UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/012,517	09/12/2012	8036988	253.005	5785

34111 7590 09/11/2013

Maxey Law Offices, PLLC
100 Second Avenue South
Suite 401 North
St. Petersburg, FL 33701

EXAMINER	
HOTALING, JOHN M	
ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
09/11/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

BUCHANAN, INGERSOLL & ROONEY PC

POST OFFICE BOX 1404

ALEXANDRIA, VA 22313-1404

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/012,517*.

PATENT NO. *8036988*.

ART UNIT *3992*.

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Office Action in Ex Parte Reexamination	Control No. 90/012,517	Patent Under Reexamination 8036988	
	Examiner JOHN HOTALING	Art Unit 3992	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

a. ☒ Responsive to the communication(s) filed on *6/7/2013* .
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

b. ☐ This action is made FINAL.

c. ☐ A statement under 37 CFR 1.530 has not been received from the patent owner.

A shortened statutory period for response to this action is set to expire *2* month(s) from the mailing date of this letter. Failure to respond within the period for response will result in termination of the proceeding and issuance of an *ex parte* reexamination certificate in accordance with this action. 37 CFR 1.550(d). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).** If the period for response specified above is less than thirty (30) days, a response within the statutory minimum of thirty (30) days will be considered timely.

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. ☐ Notice of References Cited by Examiner, PTO-892.
2. ☐ Information Disclosure Statement, PTO/SB/08.
3. ☐ Interview Summary, PTO-474.
4. ☐ _____.

Part II SUMMARY OF ACTION

1a. ☒ Claims *1-38* are subject to reexamination.
1b. ☐ Claims _____ are not subject to reexamination.
2. ☐ Claims _____ have been canceled in the present reexamination proceeding.
3. ☐ Claims _____ are patentable and/or confirmed.
4. ☒ Claims *1-38* are rejected.
5. ☐ Claims _____ are objected to.
6. ☐ The drawings, filed on _____ are acceptable.
7. ☐ The proposed drawing correction, filed on _____ has been (7a) ☐ approved (7b) ☐ disapproved.
8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the certified copies have
   1 ☐ been received.
   2 ☐ not been received.
   3 ☐ been filed in Application No. _____ .
   4 ☐ been filed in reexamination Control No. _____.
   5 ☐ been received by the International Bureau in PCT application No. _____.
   * See the attached detailed Office action for a list of the certified copies not received.
9. ☐ Since the proceeding appears to be in condition for issuance of an *ex parte* reexamination certificate except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte* Quayle, 1935 C.D. 11, 453 O.G. 213.
10. ☐ Other: _____

cc: Requester (if third party requester)

DETAILED ACTION

Summary of the Proceeding to date

Reexamination was requested on 9/12/2012 and was denied on 12/06/2012.

The Third Party Requestor submitted a petition requesting a review of the order denying request for ex parte reexamination. In response to the petition the denial was reviewed and the petition was granted. The reexamination of claims 1-38 of the 8,036,988 was ordered since Cohen raises a substantial new question of patentability as to claims 1-38 was set forth in the petition decision. For the same reasons, the third party requester's allegation that claims 11 and 12 are obvious over Cohen in view of Musmanno raises a substantial new question of patentability.

Patents and Printed Publication Cited in the Request

1. Cohen, U.S. Patent No. 6,422,462
2. Musmanno et al., U.S. Patent No. 5,826,243
3. Franklin et al., U.S. Patent No. 5,883,810
4. Joao et al., U.S. Patent No. 5,903,830
5. Yanagihara et al., U.S. Patent Application 2001/0011249

Cohen and Musmanno et al are available as prior art against the ‘988 patent.

Grounds of Rejection

The following grounds of rejection are set forth:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-10 and 13-38 are rejected under 35 U.S.C. 102(b) as being anticipated by Cohen U.S. Patent 6,442,462.

i. Claim 1

a) "A method of performing secure credit card purchases, said method comprising:"

Cohen discloses that "[i]t is an object of the present invention to provide improved credit cards and methods for credit card transactions" and that "[i]t is a further object of the present invention to provide methods and apparatus for secure transmission of credit card information" (Cohen, col. 1, l1.48-62). Accordingly, Cohen anticipates secure credit card purchases.

b) "contacting a custodial authorizing entity having custodial responsibility of account parameters of a customer's account that is used to make credit card purchases"

Cohen discloses "a user dial[ing] into her credit card company" (Cohen, col. 3, l1.42-44). It is inherent in the art that a credit card company has custodial responsibility of a customer's account used to make credit card purchases. Accordingly, a user dialing into her credit card company is anticipatory of contacting a custodial authorizing entity as claimed.

c) "supplying said custodial authorizing entity with at least account identification data of said customer's account"

Cohen discloses that the user "provid[es] the ordinary credit card number and verification data" to her credit card company (Cohen, col. 3, ll. 42-45). This supplies the credit card company, the custodial authorizing entity, with account identification data of the customer's account. Accordingly, Cohen anticipates the supplying manipulative step of claim 1.

d) "defining at least one payment category to include at least limiting a number of transactions to one or more merchants"

Cohen discloses that the card can "be customized for only particular uses or groups of uses," which would constitute payment categories as claimed by the '988 Patent (Cohen, col. 7, l1.66-67). In addition, some of the uses that the card can be customized for include the card only being valid "for use for that particular type of charge (computer or hardware stores...[or] for use in a particular store itself or a particular chain of stores" (Cohen, col. 8, l1.25-34). Therefore, the customized use can include limiting a number of transactions to one or more merchants.

e) "said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants"

Cohen discloses that a card "could be issued to the user which is only valid for use for that particular type of charge" (Cohen, col. 8, ll. 25-28). A customized use card with a customized use for only that particular type of charge would result in a card with a merchant limitation (e.g., only those merchants of that type) prior to any particular merchant (e.g., a specific merchant of that type) being identified. Additionally, Cohen states that the card could even be customized for use in a particular store itself or a

particular chain of stores (Cohen, col. 8, ll. 32-34). This is including one or more merchants in a payment category, a particular chain of stores, prior to any particular merchant being identified.

f) "designating said payment category"

Cohen discloses that "...a user can indicate in advance of purchase...what the single use or the customized credit card number is to be used for" (Cohen, col. 3, ll. 49-52). This is in effect a designation of a customized use, which is anticipatory of designating a payment category as is recited in claim 1 of the '988 Patent.

g) "generating a transaction code by a processing computer of said custodial authorizing entity"

Cohen discloses "credit cards or credit card numbers are generated" by the credit card company (Cohen, col. 2, l1.35-36). The disposable or customized credit card numbers can be indistinguishable from ordinary credit card numbers such that "both users and vendors are encouraged to use the credit card in the same manner as regular credit cards" (Cohen, col. 3, ll. 6-9).

h) "said transaction code reflecting at least the limits of said designated payment category to make a purchase within said designated payment category"

The customized or disposable credit card numbers of Cohen, like the transaction code of the '988 Patent, may have a "single or a limited range use," where the single or customized use corresponds to the single or customized use previously indicated (Cohen, col. 3, ll. 47-48). Accordingly, the customized credit card number reflects the limits of the payment category, in that the card number can only be used for the designated customized use.

i) "communicating said transaction code to a merchant to consummate a purchase with defined purchase parameters"

Cohen discloses that "...the user transmits his or her credit card information to the vendor. That vendor then verifies the transaction..." (Cohen, col. 5, ll. 36-37). It is inherent in the art that the process of a vendor verifying a transaction includes requesting authorization for the transaction from the issuer of the credit card used in the transaction, and that authorization requests include transaction details (e.g., defined purchase parameters). Accordingly, transmission of the credit card information to the vendor for verification anticipates the communicating step as recited in claim 1 of the '988 Patent.

j) "verifying that said defined purchase parameters are within said designated payment category"

Cohen discloses that the vendor "then verifies the transaction" such that the card "is only valid for use for that particular type of charge...such that if the [user] tries to use it for anything else...the charge will be declined" (Cohen, col. 8, ll. 25-32). This constitutes "verifying the defined purchase parameters being within the payment category," such that if the transaction details are not within the customized use associated with the card, the charge will be declined. Accordingly, Cohen anticipates the verifying step recited in claim 1.

k) "providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said designated payment category and to authorize payment required to complete the purchase"

Cohen discloses that, as part of the verification/authorization of the transaction "...the credit card company notes the identity of the vendor, authorizes the transaction (if

the credit card number is valid and the purchaser has sufficient funds available), and forwards the authorization code to the vendor" (Cohen, col. 5, ll. 45-49). Accordingly, as stated above, the authorization of the transaction confirms that the purchase parameters are within the customized use, and the forward of the authorization code to the vendor authorizes the payment required to complete the transaction. Therefore, Cohen anticipates this recitation of claim 1.

ii. Claim 2

"The method of claim 1 further comprising the step of designating at least one of said one or more merchants subsequent to generating said transaction code"

Cohen discloses "...the user transmit[ting] his or her credit card information to the vendor," which would thereby designated the vendor as one of the one or more merchants subsequent to the generation of the credit card number. Col. 3, ll. 49-52..

iii. Claims 3 and 20

"wherein said step of communicating the transaction code to a merchant to consummate said purchase within defined purchase parameters further comprises designation of said merchant as one of said one or more merchants"

Claim 3 includes the above recitation and is dependent from claim 1. Claim 20 includes the same recitation, but is instead dependent from claim 19. Cohen discloses generating a customized credit card number, which may then be submitted to the vendor (Cohen, col. 5, l1.36- 37).

iv. Claim 4

"wherein said step of generating said transaction code further comprises said customer obtaining said transaction code"

Cohen discloses "... a user.., is provided with a disposable or customized number..." (Cohen, col. 3, ll. 43-45). The user being provided with the customized credit card number is the same as the customer obtaining the transaction code. Accordingly, Cohen anticipates claim 4 of the '988 Patent.

v. Claim 5

"generating a transaction code which reflects at least one of a plurality of said payment categories"

Cohen discloses that the disposable or customized card number "can also be customized for only particular uses or groups of uses" (Cohen, col. 7, ll. 66-67). Accordingly, the customized number would reflect at least one of a group of customized uses.

vi. Claim 6

"defining at least one payment category to include amount parameters for a cost of one or more purchases"

Cohen discloses that "[a] customized credit card could be issues to the user which is only valid...to the credit limit decided by the issuer or [user]..." (Cohen, col. 8, l1.25-30). The provided credit limit signifies amount parameters for a cost that may be included as at least one of the customized uses that may be designated.

vii. Claim 7

"defining at least one payment category to include time parameters during which the purchase can be completed"

Cohen discloses that "...each of the disposable credit cards can be given an expiration date...[t]hus, if the credit card is not used within the time limit, it expires"

(Cohen, col. 6, ll.4-7). Accordingly, Cohen discloses time parameters during which the purchase can be completed.

viii. Claim 8

"defining at least one payment category to include limiting said transaction code to a single transaction for a purchase within a predetermined period of time"

Similar to claim 7, above, claim 8 recites a purchase within a predetermined period of time, but additionally limits the transaction code to a single transaction. Likewise, Cohen discloses that a card may "be valid for a specific predetermined amount of time" (Cohen, col., 7, ll. 61-62). In addition, Cohen also discloses that the card may be used for a single transaction, stating that "[w]ith respect to the disposable card, the user is instructed that, after use of the number once, the number may not be used again" (Cohen, col. 3, ll.60-62). Accordingly, Cohen's disposable card valid for a specific predetermined period of time anticipates claim 8 of the '988 Patent.

ix. Claim 9

"defining at least one payment category to include limiting purchases to a single transaction at a maximum amount for purchase within a predetermined period of time"

As discussed above, Cohen discloses that a disposable card number could be used for a single transaction, which may also only be valid up to a specific credit limit. Additionally, as also discussed above, Cohen discloses that the card may also only be valid for a specific predetermined amount of time. Furthermore, Cohen directly discloses this specific recitation, stating that "[t]he card could be valid only for purchase on that particular day, to a certain designated purchase limit, and even, if desired only in a certain store..." (Cohen, col. 8, ll. 43-45).

x. Claim 10

"defining at least one payment category to include limiting purchases to at least one payment category to at least two purchases at a maximum total amount for items purchased within a predetermined period of time"

Claim 10 includes the same recitation of claim 9, but is directed towards "at least two purchases" at a maximum total amount, rather than the "single transaction" recited in claim 9.

Cohen discloses throughout that a disposable card number may be used for a single use, while a customized card number may be used for customized use, which can include multiple transactions of multiple types, or from "groups of stores or types of stores, or types of purchases or items" (Cohen, col. 8, ll. 43-47). Accordingly, Cohen anticipates the recitation of claim 10 of the '988 Patent.

xii. Claim 13

"defining at least one payment category to include using said transaction code for a repeating transaction at a fixed amount payable to each of an unspecified number of time intervals"

Claim 13 includes a recitation identical to that of claim 12, except that the number of time intervals recited in claim 13 is unspecified. As discussed above, Cohen discloses that "the card can have a user customized range of dates or series of dates" for fixed amounts. (Cohen, col. 7, ll. 44-46). When the series of dates is customized to have no end but rather be a series of repeating dates (e.g., every Wednesday, the first of every month, etc.) as is disclosed in Cohen, then the credit card number would be used for a repeating transaction at an unspecified number of time intervals. Accordingly, Cohen anticipates claim 13 of the '988 Patent.

xiii. Claims 14, 26, and 34

"defining at least one payment category to include limiting a repeating transaction to a maximum dollar amount"

Claims 14, 26, and 34 each include the above recitation and are dependent from claims 1, 21, and 22, respectively. As discussed previously with respect to claims 11-13, Cohen discloses a repeating transaction as well as a designated purchase limit. In addition, Cohen discloses that "combinations of dates of transactions, types of transactions, amounts for individual and/or total transactions, etc. on a single card, or on multiple cards, can be set as well" (Cohen, col. 10, ll. 31-35). Accordingly, Cohen discloses the combination of groups of uses, which includes limiting a repeating transaction to a maximum dollar amount.

xiv. Claims 15, 27, and 35

"defining at least one payment category to include limiting purchases to a limited time interval during which a purchase is permitted"

Claims 15, 27, and 35 each include the above recitation, and are dependent from claims 1, 21, and 22, respectively.

As discussed above with respect to claim 7, Cohen discloses that "...each of the disposable credit cards can be given an expiration date...[t]hus, if the credit card is not used within the time limit, it expires" (Cohen, col. 6, ll. 4-7). And specifically, Cohen also discloses that the card "...could also be valid for a specific predetermined amount of time" (Cohen, col. 7, ll. 61-62). Accordingly, Cohen anticipates the claimed limited time interval during which a purchase is permitted.

xv. Claims 16, 28, and 36

"communicating said transaction code to the customer at the location of the merchant for use in person"

Claims 16, 28, and 36 each include the above recitation and are dependent from claims 1, 21, and 22, respectively.

Like the '988 Patent, Cohen discloses that the disposable or customized credit card number are ideally suited for Internet or other network-based financial transactions, but may also be used in person. Along these lines, Cohen discloses that there may be a physical manifestation of the card, that may be provided to the vendor such that "[t]he vendor could read the number of the disposable or customized card, could scan the number with a bar code scanner, could read a magnetic strip on the disposable card, or so forth" (Cohen, col. 4, ll. 31-35). Accordingly, Cohen discloses that the transaction code may be communicated to the customer at the location of the merchant for use in person.

xvi. Claims 17 and 19

a) "A method of performing secure credit card purchases, said method comprising the steps of:"

As pointed out above with respect to claim 1, Cohen discloses that "[i]t is an object of the present invention to provide improved credit cards and methods for credit card transactions" and that "[i]t is a further object of the present invention to provide methods and apparatus for secure transmission of credit card information" (Cohen, col. 1, ll. 48-62). Accordingly, Cohen anticipates secure credit card purchases.

b) "identifying a pre-established account that is used to make credit card purchases"

Cohen discloses that the user "provid[es] the ordinary credit card number and verification data" to her credit card company (Cohen, col. 3, ll.42-45). It is inherent in the art and disclosed by Cohen that providing the ordinary credit card number and verification data to a credit card company is for the purpose of identifying a pre-established account used to make purchase with provided same credit card.

c) "selecting a pre-determined payment category which limits its a nature, of a series of subsequent purchases to one or more merchants"

As stated with respect to claim 1, Cohen discloses that the card can "be customized for only particular uses or groups of uses," which would constitute payment categories as claimed by the '988 Patent (Cohen, col. 7, ll. 66-67). In addition, some of the uses that the card can be customized for include the card only being valid "for use for that particular type of charge (computer or hardware stores...[or] for use in a particular store itself or a particular chain of stores" (Cohen, col. 8, ll. 25-34). Therefore, the customized use can include limiting a number of transactions to one or more merchants. As also discussed previously, Cohen also discloses that the customized uses may include limited use for both a series of subsequent purchase or a single subsequent purchase.

d) "said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants"

Cohen discloses that a card "could be issued to the user which is only valid for use for that particular type of charge" (Cohen, col. 8, ll.25-28) (emphasis added). A customized use card with a customized use for only that particular type of charge would

result in a card with a merchant limitation (e.g., only those merchants of that type) prior to any particular merchant (e.g., a specific merchant of that type) being identified.

e) "generating a transaction code by a processing computer of a custodial authorizing entity of said pre-established account"

As discussed with respect to claim 1, Cohen discloses "credit cards or credit card numbers are generated" by the credit card company (Cohen, col. 2, ll.35-36). The disposable or customized credit card numbers can be indistinguishable from ordinary credit card numbers such that "both users and vendors are encouraged to use the credit card in the same manner as regular credit cards" (Cohen, col. 3, ll. 6-9).

f) "said transaction code associated with at least said pre- established account and the limits of said selected payment category"

The '988 Patent states that "the transaction code is pre-coded to be indicative of a specific credit card account...and a designated payment category" (col. 6, ll.33-35). Similarly, The customized or disposable credit card numbers of Cohen, like the transaction code of the '988 Patent, may have a "single or a limited range use," where the single or customized use corresponds to the single or customized use previously indicated (Cohen, col. 3, ll. 47-48). In addition, Cohen also discloses that "...the credit card can be marked, if desired, to show both that it has been processed to charge money to the person's account...," which illustrates the association of the customized credit card with the specific credit card account (Cohen, col. 4, ll. 36-38).

g) "different from said pre-established account"

Cohen discloses that "[n]o vendor would ever.., receive or have access to the user's permanent credit card number. Rather, the vendor would receive a disposable

credit card number from the user's supply" (Cohen, col. 4, ll. 26- 31). Accordingly, Cohen discloses that the disposable or customized credit card number is different from the account number of the user's pre-established account.

h) "communicating said transaction code to said merchant consummate a purchase within defined purchase parameters"

Cohen discloses that "...the user transmits his or her credit card information to the vendor. That vendor then verifies the transaction..." (Cohen, col. 5, ll. 36-37). The process of a vendor verifying a transaction includes requesting authorization for the transaction from the issuer of the credit card used in the transaction, and that authorization requests include transaction details (e.g., defined purchase parameters).

i) "verifying that said defined purchase parameters correspond to said selected payment category"

As discussed previously with respect to claim 1's identical recitation, Cohen discloses that the vendor "then verifies the transaction" such that the card "is only valid for use for that particular type of charge...such that if the [user] tries to use it for anything else...the charge will be declined" (Cohen, col. 8, ll.25-32). This constitutes "verifying the defined purchase parameters being within the payment category," such that if the transaction details are not within the customized use associated with the card, the charge will be declined.

j) "providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said selected payment category and to authorize payment required to complete the purchase"

As discussed with respect to this recitation included in claim 1, Cohen discloses that, as part of the verification/authorization of the transaction "...the credit card

company notes the identity of the vendor, authorizes the transaction (if the credit card number is valid and the purchaser has sufficient funds available), and forwards the authorization code to the vendor" (Cohen, col. 5, ll.45-49). Accordingly, as stated above, the authorization of the transaction confirms that the purchase parameters are within the customized use, and the forward of the authorization code to the vendor authorizes the payment required to complete the transaction. Therefore, Cohen anticipates this recitation of claim 17.

k) "associating the purchase with said pre-established account"

Cohen discloses, as discussed above, that "...the credit card can be marked, if desired, to show both that it has been processed to charge money to the person's account..." (Cohen, col. 4, ll.36-38). By showing that the transaction has been processed, and that money has been charged to the person's account, the transaction is therefore associated with the charge on the person's account and is therefore associated with the pre-established account. Accordingly, Cohen anticipates this recitation.

Claim 19 is almost identical to claim 17, except for two recitations. First, in claim 19, the "selecting a predetermined payment category" step recites a single subsequent purchase instead of the series of subsequent purchases recited in claim 17. As discussed above, Cohen discloses disposable card numbers for a single transaction.

Second, claim 19 also includes the recitation "designating a merchant as one of said one or more merchants." As discussed previously with respect to claims 2, 3, and 20, Cohen discloses that a merchant may be designated by the customer "transmit[ting]

his or her credit card information to the vendor," which anticipates this recitation (Cohen, col. 5, ll.36-37).

Based upon the foregoing, it is apparent that Cohen discloses the method for performing secure credit card purchases as recited in claims 17 and 19 of the '988 Patent.

xvii. Claim 18

"said step of verifying that said defined purchase parameters correspond to said selected payment category further identifies said merchant as one of said one or more merchants"

Cohen discloses that "[u]pon use of the card, the information regarding the transaction is transmitted to the credit card company, as is known in the art" (Cohen, col. 13, ln. 66 - col. 14, ln. 1). It is inherent in the art that merchant identification is included in the transaction details transmitted to the credit card company. Accordingly, during the verification of the transaction details, the merchant is identified as one of the one or more merchants based on the included merchant identification. Accordingly, Cohen anticipates claim 18 of the '988 Patent.

xviii. Claims 21 and 22

The recitations of claim 22 are identical to the recitations of claim 21, except that where claim 21 recites "a single merchant," claim 22 recites "one or more merchants."

a) "A method for implementing a system for performing secure credit card purchases, the method comprising:"

As pointed out above with respect to claims 1 and 17, Cohen discloses that "[i]t is an object of the present invention to provide improved credit cards and methods for

credit card transactions" and that "[i]t is a further object of the present invention to provide methods and apparatus for secure transmission of credit card information" (Cohen, col. 1, ll. 48-62). Accordingly, Cohen anticipates secure credit card purchases.

b) "receiving account information from an account holder identifying an account that is used to make credit card purchases"

As stated previously, Cohen discloses that the user "provid[es] the ordinary credit card number and verification data" to her credit card company (Cohen, col. 3, ll. 42-45). This constitutes account information that is received from the user (the account holder). It is inherent in the art that providing the ordinary credit card number and verification data to a credit card company is for the purpose of identifying a pre-established account used to make purchase with provided same credit card. Accordingly, Cohen anticipates this recitation.

c) "receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant"

As stated above, this recitation as included in claim 22, is directed to limiting transactions to "one or more merchants" rather than the "a single merchant" recited in claim 21. Cohen discloses that "[a] user dials into her credit card company before making a transaction, and...is provided with a disposable or customized number" where the user "...can indicate in advance of purchase...what the single use or the customized credit card number is to be used for" (Cohen, col. 3, ll. 49-52). As discussed above, the single or customized use may include types of charges, a particular merchant, multiple merchants, etc. Accordingly, Cohen discloses a request from an account holder for a

customized credit card number to make a purchase that limits transactions to either a single merchant or one or more merchants as the case may be.

d) "said single merchant limitation being included in said payment category prior to any particular merchant being identified as said single merchant"

Cohen discloses that a card "could be issued to the user which is only valid for use for that particular type of charge" (Cohen, col. 8, ll. 25-28). A customized use card with a customized use for only that particular type of charge would result in a card with a merchant limitation (e.g., only those merchants of that type) prior to any particular merchant (e.g., a specific merchant of that type) being identified. Additionally, Cohen states that the card could even be customized for use in a particular store itself or a particular chain of stores (Cohen, col. 8, ll. 32-34). This is including one or more merchants in a payment category, a particular chain of stores, prior to any particular merchant being identified.

e) "generating a transaction code utilizing a processing computer of a custodial authorizing entity, said transaction code associated with said account"

As discussed with respect to claims 1 and 17, Cohen discloses "credit cards or credit card numbers are generated" by the credit card company (Cohen, col. 2, ll.35-36). The disposable or customized credit card numbers can be indistinguishable from ordinary credit card numbers such that "both users and vendors are encouraged to use

the credit card in the same manner as regular credit cards" (Cohen, col. 3, ll.6-9). In addition, as discussed previously regarding claim 17, Cohen also discloses that "...the credit card can be marked, if desired, to show both that it has been processed to charge money to the person's account...," which illustrates the association of the customized credit card with the specific credit card account (Cohen, col. 4, ll. 36-38).

f) "reflecting at least the limits of said payment category, to make a purchase within said payment category"

As discussed above, the customized or disposable credit card numbers of Cohen, like the transaction code of the '988 Patent, may have a "single or a limited range use," where the single or customized use corresponds to the single or customized use previously indicated (Cohen, col. 3, ll.47-48). Accordingly, this means that the customized card number reflects at least the limits of the customized use for making a purchase within the customized use.

g) "communicating said transaction code to said account holder"

Cohen discloses that, upon dialing in to the credit card company, the account holder "... is provided with a disposable or customized number..." (Cohen, col. 3, ll.43-45). Accordingly, this anticipates communicating the disposable or customized number to the account holder.

h) "receiving a request to authorize payment for a purchase using said transaction code"

Cohen discloses "receiving the request for verification" from the vendor using the customized credit card (Cohen, col. 5, ll. 35-49). This request for verification, which is

inherent in the art, is the same as the request to authorize payment. Accordingly, Cohen anticipates this recitation.

i) "authorizing payment for said purchase if said purchase is within said payment category"

As discussed previously with respect to the "verifying" step of claims 1 and 17, Cohen discloses that, as part of the verification/authorization of the transaction "...the credit card company notes the identity of the vendor, authorizes the transaction (if the credit card number is valid and the purchaser has sufficient funds available), and forwards the authorization code to the vendor" (Cohen, col. 5, ll. 45-49). Accordingly, as stated above, the authorization of the transaction confirms that the purchase parameters are within the customized use, and the forward of the authorization code to the vendor authorizes the payment required to complete the transaction.

xix. Claims 23 and 31

"wherein the step of receiving account information from the account holder identifying an account that is used to make credit card purchases further comprises receiving information identifying a credit card account"

Claims 23 and 31 each contain this recitation, and are directed to claims 21 and 22, respectively.

As stated above with respect to claims 21 and 22, Cohen discloses the user dialing into her credit card company and providing "the ordinary credit card number and verification data" that constitutes information identifying a credit card account (Cohen, col. 3, l1.42-45). Accordingly, Cohen anticipates this recitation.

xx. Claims 24 and 32

"wherein the step of generating a transaction code utilizing a processing computer of a custodial authorizing entity further comprises generating a transaction code which reflects at least one of a plurality of predetermined payment categories"

Claims 24 and 32 each contain this recitation, and are directed to claims 21 and 22, respectively. Like discussed above, Cohen discloses generating a disposable or customized credit card number that "can also be customized only for particular uses or groups of uses" (Cohen, col. 7, ll.66-67). As the card number is customized for at least one of the plurality of uses, it therefore reflects at least one of the plurality of predetermined payment categories.

xxi. Claims 25 and 33

"wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant further comprises receiving a request from said account holder for a transaction code to make a purchase within a payment category that is automatically chosen by a custodial authorizing entity"

Claims 25 and 33 each include the above recitation and are dependent from claims 21 and 22, respectively. As discussed previously, Cohen discloses receiving a request for a disposable or customized credit card number from a user to make a purchase within a payment category. It is inherent that, based on the user "indicat[ing] in advance of purchase...what the single use or the customized credit card number is to be used for" the credit card company would automatically chose the corresponding payment category. Because the payment categories, and authorization of cards as being within those payment categories, are managed by the credit card company, it is well known in the art that the credit card company would automatically choose the corresponding payment category (e.g., based on the information indicated by the user).

xxii. Claims 29 and 37

"wherein said step of receiving a request to authorize payment for a purchase using said transaction code further identifies said single merchant"

Claims 29 and 37 each contain this recitation, and are directed to claims 21 and 22, respectively. As stated above with respect to the "receiving a request" step of claims 21, and 22, Cohen discloses that "[u]pon use of the card, the information regarding the transaction is transmitted to the credit card company, as is known in the art" where it is known in the art that transaction details included as part of the authorization request include merchant identification that identifies a merchant (Cohen, col. 13, ln. 66 - col. 14, ln. 1). In further support, Cohen also discloses that, as part of the authorization process, "...the credit card company notes the identity of the vendor..." and thus identifies the merchant (Cohen, col. 5, ll.45-49).

xxiii. Claims 30 and 38

"wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant further comprises receiving a request from said account holder for a transaction code to make a purchase within a predetermined payment category that is further limited in accordance with transaction details provided by said account holder"

Claims 30 and 38 each contain this recitation, and are directed to claims 21 and 22, respectively.

Cohen discloses that as part of the request for a customized number "...a user can indicate in advance of purchase...what the single use or the customized credit card number is to be used for" (Cohen, col. 3, ll. 49-52). The customized number can be further limited as the "user could even identify the general or specific type and amount

of transaction in advance," which constitutes transaction details provided by the user (Cohen, col. 5, ll. 23-25). Therefore, Cohen discloses the methods for performing and for implementing a system for performing secure credit card purchases.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 11 and 12 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Cohen.

Cohen discloses all of claim 1 as described above but lacks in disclosing a repeating transaction described in claims 11 and 12. Instead, Cohen discloses defining a payment category (e.g., customized uses) to include using the credit card number for at least two purchases with a designated purchase limit (e.g., fixed amount payable). In addition to this, Cohen also discloses that "the card can have a user customized range of dates or series of dates" (Cohen, col. 7, ll. 44-46). The customized range or series of dates could be used to effect a repeating transaction, by the customized series of dates being a repeatable series. Likewise, a limit placed on the series could result in a fixed number of time intervals. Cohen additionally states in Col.8 ll.35-36 that any of the features in the present application can also be combined. This would include

customized time periods and customized amounts. It is notoriously well known that the art that making car or mortgage payments involves multiple equal payments at a number of time intervals. It would have been obvious to one of ordinary skill in the art to provide such a payment category in the method described in Cohen because periodic payments in car and mortgage payments are so prevalent and notorious in the art that one of ordinary skill in the art would have expected and therefore would have found obvious making equal payments at specified times for these types of payments. The desirability for making equal payments would have been readily apparent from the increased convenience of predictability that equal payments provide. Therefore including a payment category for a repeating transaction in the method described in Cohen would have been obvious to one of ordinary skill in the art. See KSR, 127 S.Ct. at 1741. The inclusion of a payment category for a repeating transaction to the payment categories already provided in Cohen is merely a predictable variation that yields a predictable result. Id. at 1739-40.

Reexamination

In order to ensure full consideration of any amendments, affidavits or declarations, or other documents as evidence of patentability, such documents must be submitted in response to this Office action. Submissions after the next Office action, which is intended to be a final action, will be governed by the requirements of 37 CFR 1.116, after final rejection and 37 CFR 41.33 after appeal, which will be strictly enforced.

Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Additionally, 35 U.S.C. 305 requires that reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.550(a)). Extension of time in *ex parte* reexamination proceedings are provided for in 37 CFR 1.550(c).

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a), to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving Patent No. 8,036,988 throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

In any reexamination proceeding under this chapter, the patent owner will be permitted to propose any amendment to his patent and a new claim or claims thereto, in order to distinguish the invention as claimed from the prior art cited under the provisions of section 301 of this title, or in response to a decision adverse to the patentability of a claim of a patent. See 35 U.S.C. 305. For this reason, patent owner is notified that any amendment to a claim not involved in the reexamination proceeding may not be entered, and if entered, will bring that claim into the reexamination proceeding. See 37 CFR 1.104. Patent owner is also notified that any proposed amendment to the specification and/or claims in this reexamination proceeding must comply with 37 C.F.R. 1.530(d)-(j), must be formally presented pursuant to 37 C.F.R. 1.52(a) and (b), and must contain any fees required by 37 C.F.R. 1.20(c). See MPEP § 2250(IV) for examples to

assist in the preparation of proper proposed amendments in reexamination proceedings.

After the filing of a request for reexamination by a third party requester, any document filed by either the patent owner or the third party requested must be served on the other party (or parties where two or more third party requested proceedings are merged) in the reexamination proceeding in the manner provided in 37 C.F.R. 1.248. See 37 C.F.R. 1.550(0.

Regarding IDS submissions MPEP 2256 recites the following: "Where patents, publications, and other such items of information are submitted by a party (patent owner or requester) in compliance with the requirements of the rules, the requisite degree of consideration to be given to such information will be normally limited by the degree to which the party filing the information citation has explained the content and relevance of the information." Accordingly, the IDS submissions have been considered by the Examiner only with the scope required by MPEP 2256. In certain instances, the Examiner has lined through references because they do not meet the requirements of being a Patent or Printed Publication (e.g. court papers and other evidence that is not NPL). However, these references have been made of record in the proceeding and have been considered.

All correspondence relating to this *ex parte* reexamination proceeding should be directed:

By Mail to: Mail Stop *Ex Parte* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand to: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at https://efs.uspto.gov/efile/myportal/efs-registered. EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Any inquiry concerning this communication should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

Signed:

/John M Hotaling II/
Primary Examiner
AU 3992

Conferees:

//Jalatee Worjloh/
Primary Examiner, Art Unit 3992
/Alexander J Kosowski/
Supervisory Patent Examiner, Art Unit 3992

Reexamination	**Application/Control No.** 90012517	**Applicant(s)/Patent Under Reexamination** 8036988
	Certificate Date	**Certificate Number**

Requester Correspondence Address: ☐ **Patent Owner** ☒ **Third Party**
BUCHANAN, INGERSOLL & ROONEY PC POST OFFICE BOX 1404 ALEXANDRIA, VA 22313-1404

LITIGATION REVIEW ☒	/JMH/ (examiner initials)	09/05/2013 (date)
Case Name		Director Initials
D'agostino V Mastercard Inc et al 1:13cv738 (open)		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	**NUMBER**

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90012517	8036988
	Examiner	Art Unit
	JOHN HOTALING	3992

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
patent 8036988 prosecution history reviewed	9/4/2013	JH

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/012,517	09/12/2012	8036988	253.005	5785

34111 7590 06/07/2013

Maxey Law Offices, PLLC
15500 Roosevelt Blvd.
SUITE 305
CLEARWATER, FL 33760

EXAMINER	
CARLSON, JEFFREY D	
ART UNIT	**PAPER NUMBER**
3992	
MAIL DATE	**DELIVERY MODE**
06/07/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

Date: JUN 0 7 2013

CENTRAL REEXAMINATION UNIT

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. : 90012517
PATENT NO. : 8036988
ART UNIT : 3993

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified ex parte reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the ex parte reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Maxey Law Offices, PLLC
15500 Roosevelt Blvd.
SUITE 305
CLEARWATER, FL 33760

(For Patent Owner)

MAILED

JUN 0 7 2013

CENTRAL REEXAMINATION UNIT

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

(For Third Party Requester)

In re: D'Agostino
Ex Parte Reexamination Proceeding
Control No.: 90/012,517
Deposited: September 12, 2012
For: U.S. Patent No.: 8,036,988

DECISION ON PETITION
UNDER 37 CFR §§ 1.181

This is a decision on the petition filed by the third party requester on January 7, 2013, entitled "PETITION FOR REVIEW UNDER 37 CFR § 1.181" [hereinafter "the petition"]. Petitioner seeks review of the Order Denying Request for *Ex Parte* Reexamination mailed December 6, 2012.

The petition is before the Director of the Central Reexamination Unit.

The petition is granted.

REVIEW OF RELEVANT FACTS

- U.S. Patent No. 8,036,988 ["the '988 patent"] issued on October 11, 2011.
- A request for *ex parte* reexamination of claims 1-38 of the '988 patent was filed September 12, 2012 ["the Request"] and assigned control no. 90/012,517.
- An order denying the request for reexamination was issued on December 6, 2012.
- On January 7, 2012, the third party requester timely filed the instant petition for reconsideration of the denial of the request.

DECISION

Standard of Review

37 CFR § 1.515(c) provides for the filing of a petition under 37 CFR § 1.181 to review an examiner's determination refusing to order *ex parte* reexamination. The CRU Director's review on petition is *de novo*. Therefore, the review will determine whether the examiner's refusal to order reexamination was correct, and will not necessarily indicate agreement or disagreement with every aspect of the examiner's rationale for denying the request.

The Legal Standard for Ordering Reexamination

A review of 35 U.S.C. §§ 302 and 303 reveals that, by statute, *ex parte* reexamination of a United States Patent is only authorized when a consideration of prior art consisting of patents or printed publications establishes that a substantial new question of patentability exists with respect to one or more claims of that patent. 35 U.S.C. § 302 requires that a request for *ex parte* reexamination be based upon prior art as set forth in 35 U.S.C. § 301, that is, prior art consisting of patents or printed publications, while 37 CFR § 1.510(b)(1) requires that a request for *ex parte* reexamination include "a statement pointing out each substantial new question of patentability based on the cited patents and printed publications." A substantial question of patentability (SNQ) is raised by a cited patent or printed publication when there is a substantial likelihood that a reasonable examiner would consider the prior art patent or printed publication important in deciding whether or not the claim is patentable. If the prior art patents and printed publications relied upon in the request raise a substantial question of patentability, then a "substantial new

question of patentability" is present, unless the same question of patentability has already been decided by a final court holding of invalidity after all appeals, or by the Office in an earlier examination or in a reexamination of a patent. If a substantial new question of patentability is found to be raised, an order granting *ex parte* reexamination of the patent is issued.

Summary of the Prior Prosecution with Respect to the '988 Patent

The '988 patent is drawn to a system and method of performing secure credit card transaction. Generally, in the prior art, a consumer wishing to make a purchase by credit card would provide details such as their credit card number and expiration date to complete the transaction. This leads to potential security issues, particularly in the case of phone or internet based purchases, as it is impossible for the card holder to know how securely her account information has been protected from fraud. The '988 patent provides a solution by using a transaction code. The card holder first supplies her credit card information to an authorizing entity (i.e. the card issuer or bank), who verifies the status and identity of the holder and generates the transaction code. The transaction code can also reflect a payment category which limits the transaction. For example, the transaction code might limit a transaction to occurring during a particular time period, to a particular or maximum payment amount, or to a particular merchant. In any case, the card holder can provide the transaction code to the merchant rather than the card information, and the merchant communicates with the authorizing entity to verify the code and make payment arrangements. Thus, rather than giving account information to each merchant, the consumer only gives her information to the authorizing entity, an entity who has already been entrusted with such information.

In the application which became the '988 patent, the claims were originally rejected for double patenting over two parent patents and as obvious over a combination references to Franklin [U.S. 6,000,832, hereinafter "Franklin'832] and Yanagihara.[1] The applicant filed a response on March 21, 2011, including terminal disclaimers to remove the double patenting rejections and arguing that the references do not read on all of the limitations of the claims. It argued that Franklin '832 requires that a particular merchant for a transaction be known and identified to generate the transaction code as the code is merchant specific, but in the claimed invention the merchant is not identified prior to generation of the code. The examiner found the arguments persuasive and issued a Notice of Allowance, stating as reasons for allowance "the uniquely patentable feature of: "defining at least one payment category to include at least limiting a number of transaction to one or more merchants, said one or more merchants limitations being including in said payment category prior to any particular merchant being identified as one of said one or more merchants" in a method of performing secure credit card purchase." Notice of Allowance mailed Apr. 29, 2011 at p. 2 (emphasis deleted). Accordingly, references having such features would have been important to a reasonable examiner considering the patentability of the claims.

[1] This is not the same Franklin mentioned below and cited in the Request; it is the same Yanagihara.

Analysis of the Request for Reexamination and the Denial of the Request

The third party requester in the Request proposes that a substantial new question of patentability is raised as follows (See Request p. i):

A. Claims 1-38 are anticipated by Cohen.[2]
B. Claims 11 and 12 are obvious over Cohen in view of Musmanno.
C. Claims 1-8, 15, 19-24, 27, 29-32, 35, and 37-38 are anticipated by Franklin.
D. Claims 16, 25, 28, 33, and 36 are obvious over Franklin.
E. Claims 17 and 18 are obvious over Franklin in view of Joao.
F. Claims 9-14, 26, and 34 are obvious over Franklin in view of Yanagihara.

In the Order the examiner determined that none of these combinations of references raised a substantial new question of patentability with respect to the claims of the '988 patent. The third party requester ["Petitioner"] in the petition seeks review of the examiner's determinations. Note that Petitioner only argues that the examiner erred in his determination as to Cohen, therefore only Proposals A and B are under consideration in this decision. While Proposal B was not specifically addressed in the petition, it was denied by the examiner for the same reasons as Proposal A therefore it can be considered that Petitioner believes the examiner erred as to that proposal as well.

Cohen is drawn to an apparatus and method for improved credit card transactions, where the credit cards are provided with only a one time use, or some other limited use. Col. 2 ll. 35-62. Similar to the '988 patent, the credit card account holder can obtain from the credit card company a customized number to be used for a limited range of transactions, and can indicate in advance what the number is to be used for. Col. 3 ll. 41-55. The card holder can then communicate the number to the merchant to complete a transaction, and the card company will authorize it if applicable or deny it if used for something different than the customized use—for example if it is to be used for airline travel but the number is used for a different type of transaction. Col. 5 ll. 35-39; Col. 7 ll. 66 – Col. 8 ll. 5. Examples of customized limitations of the card are time limits, purchase amounts, particular merchants, locations, individuals, or industries.

The third party requester alleges that Cohen anticipates all of the claims of the '988 patent. As to the key feature deemed missing during the previous examination, the requester gave two arguments. First, it argued that the term "limiting a number of transactions to one or more merchants" as well as doing so "prior to any particular merchant being identified" is not a

[2] See Request p. ii for citations of the references.

limitation at all, because it is limited to any number of merchants, so it is not really limiting. Request pp. 5-6; 25-27. It also argues that Cohen describes these features. *Id.* at 26-27.

As to the argument that the claim term is not a limitation, the Director disagrees because the claim requires there to be some limitation of the number. That is, the claim requires the positive step of making a limit, even if that limit were of any number of merchants. In other words, if a device were silent as to what merchants are able to accept transactions, it would not meet the claim language. If a device explicitly attempts to limit the merchants somehow it could meet the claim language. In that case, even if the limit is very broad, the step of limiting exists. The claim does not care how the number of merchants is limited, so long as there is some limit. Requester simply asks us to ignore this claim language, but it is not reasonable to simply assume the claim language has no meaning. This is particularly so because this is the very reason why the claims were allowed previously. When considering whether there is a new question of patentability, one cannot assume that the very reason the claim was allowed has no patentable weight.

The third party requester has also argued that Cohen does provide a limit on the number of merchants and providing such limit before a particular merchant is identified. For example, it is argued that in Cohen one can limit the transactions only to a particular type of merchant, such as computer stores. Request p. 26 (citing Cohen col. 8 ll. 25-34); see also Cohen col. 8 ll. 43-45 (card can be limited to use at certain types of stores, such as clothing stores). If this were the case, the payment category would limit the number of merchants—to, for example, only clothing stores. At the same time, limiting to "clothing stores" does not identify any one particular merchant. Accordingly, it would appear that Cohen does include "defining a payment category to include at least limiting a number of transactions to one or more merchants, said one or more merchants limitation being included in said payment category prior to any particular merchant being identified" as claimed. This is the material which was deemed missing during the original prosecution.

In light of these teachings, as well as the third party's application of Cohen to all of claims 1-38 as set forth in the Request, a reasonable examiner would have considered Cohen important in considering the patentability of all claims 1-38. These teachings are not cumulative to any written discussion on the record of the teachings of the prior art, were not previously considered nor addressed during a prior examination, and the same question was not the subject of a final holding of invalidity in the Federal Courts. Cohen raises a substantial new question of patentability as to claims 1-38.

For the same reasons, the third party requester's allegation that claims 11 and 12 are obvious over Cohen in view of Musmanno raises a substantial new question of patentability. Musmanno is provided only for teaching the features of these dependent claims. Request pp. 50-51. The third party applies the art to the claims and gives a reason to combine the references, and such

reasons appear reasonable. This combination would therefore have been important to a reasonable examiner in determining the patentability of these claims for the same reason that Cohen alone was important as to parent claim 1.

The examiner in the Order denied the request because he disagreed with the requester's argument that the key claim term is non-limiting, and also because he found Cohen's relevant teachings are cumulative to those of the old Franklin '832 reference. Order mailed Dec. 6, 2012 at pp. 6-8. As discussed above, the Director generally agrees with the examiner that the claim terms are limiting, but the Director does not agree that Cohen is cumulative to Franklin '832.

The examiner found that Cohen's restrictions are drawn to specific merchants and particular stores. Thus, the examiner determined that Cohen must necessarily specify the identities of those merchants when defining the payment category. The examiner equates this teaching, as well as the type of charge teaching, to the merchant ID and goods ID of Franklin '832 col. 2 ll. 29-32. The Director disagrees because, as discussed above, Cohen does not necessarily limit transactions to any specific merchant or particular store—if Cohen provides a limit of "clothing stores" then there is necessarily a limit on number of stores, as not all stores are clothing stores. At the same time there is no limit or specific identification of any specific store. Cohen therefore limits a number of transactions to one or more merchants, those of a specific industry, while not identifying and particular merchant. Limiting by industry does not necessarily identify a particular merchant, so there is not necessarily something like the merchant ID of Franklin '832.

The examiner also appears to state this is cumulative to the "goods ID" of Franklin '832. The Director does not agree, because there is no indication that "goods ID" has anything to do with identification of a type of store. That is, even if the type of goods are identified (i.e. clothes) this is not the same thing as providing a limit to a subset of stores as is done in Cohen (i.e. clothing stores). Cohen provides both teachings while Franklin '832 does not. Cohen is therefore more relevant to the claims and provides a new technical teaching not present in Franklin '832. Cohen raises a substantial new question of patentability with respect to claims 1-38 alone, and with respect to claims 11 and 12 when combined with Musmanno.

Accordingly, the petition filed January 7, 2013 is granted. The request for reexamination filed September 12, 2012 is granted with respect to the substantial new questions of patentability based on Cohen.

CONCLUSION

1. Based on a *de novo* review of the record as a whole, the petition is granted. The request for *ex parte* reexamination of claims 1-38 of the '988 patent is granted. All claims 1-38 will be reexamined.

2. This decision addresses only the proposals based on the Cohen reference. The examiner's denials of the proposals based on the Franklin reference are not disturbed.

3. Review of this decision is permitted only as explained in Clarification on the Procedure for Seeking Review of a Finding of a Substantial New Question of Patentability in *Ex Parte* Reexamination Proceeding, 75 Fed. Reg. 36,357 (June 25, 2010).

4. Patent owner has a time period of TWO MONTHS from the mailing date of this decision to file an optional patent owner's statement in accordance with 37 CFR § 1.530(b). The third party requester has a time period of TWO MONTHS from the date of service of a timely filed patent owner statement to file a reply to the statement under 37 CFR § 1.535. If patent owner does not file a statement, no reply by the requester is permitted. See the Order for correspondence information.

5. Telephone inquiries related to this decision should be directed to Alexander Kosowski, Supervisory Patent Reexamination Specialist, at (571) 272-3744, or in his absence to the undersigned at (571) 272-0700.

Irem Yucel
Director, Central Reexamination Unit

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	John D'Agostino	Patent No:	8,036,988
Serial No.:	90/012,517	Granted:	10/11/2011
Filed:	09/12/2012	Docket No.	253.005
Confirmation No.:	5785		

For: **System and Method for Performing Secure Credit Card Transactions**

STATEMENT REGARDING PRIOR OR CONCURRENT PROCEEDINGS (37 C.F.R. § 1.565)

Mail Stop Ex Parte Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

U.S. Patent No. 8,036,988 is presently asserted in concurrent or past proceedings in the following United States District Courts.

Date	Lawsuit	Status
4/26/2013	*John D'Agostino v.Mastercard Inc.*, *et al*, 1:2013cv00738, District of Delaware.	Pending

Respectfully submitted,
Maxey Law Offices, PLLC

Date: May 2, 2013

/Stephen Lewellyn/

Stephen Lewellyn
Registration No. 51,942
15500 Roosevelt Blvd., Suite 305
Clearwater, Florida 33760
Tel: 727-230-4949

CERTIFICATE OF SERVICE

It is hereby certified by the undersigned that a true copy of the Statement Regarding Prior or Concurrent Proceedings, filed May 2, 2013, was sent via email to:

Charles F. Wieland III
Buchanan Ingersoll & Rooney, P.C.
1737 King Street, Suite 500
Alexandria, VA 22314
Charles.wieland@bipc.com

For the Patentee,

Date: May 2, 2013

/Stephen Lewellyn/

Stephen Lewellyn
Registration No. 51,942
15500 Roosevelt Blvd., Suite 305
Clearwater, Florida 33760
Tel: 727-230-4949

Electronic Acknowledgement Receipt

EFS ID:	15672964
Application Number:	90012517
International Application Number:	
Confirmation Number:	5785
Title of Invention:	SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES
First Named Inventor/Applicant Name:	8036988
Customer Number:	34111
Filer:	Stephen James Lewellyn
Filer Authorized By:	
Attorney Docket Number:	253.005
Receipt Date:	02-MAY-2013
Filing Date:	12-SEP-2012
Time Stamp:	12:39:58
Application Type:	Reexam (Patent Owner)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		253005_proceedings_statement_05022013.pdf	162846 101516bb71bba7a4b5abe899399876baefbe6857	yes	2

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Notice of concurrent proceeding(s)	1	1
	Reexam Certificate of Service	2	2
Warnings:			
Information:			
	Total Files Size (in bytes):	162846	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Litigation Search Report CRU 3999

Reexam Control No. 90/012,517

TO: JEFFREY CARLSON **Location: CRU** **Art Unit: 3992** **Date: 05/02/2013**	**From: MANUEL SALDANA** **Location: CRU 3999** **MDE 5D14** **Phone: (571) 272-7740** **MANUEL.SALDANA@uspto.gov**

Search Notes

Litigation was found for US Patent Number: **8,036,988**

1) I performed a KeyCite Search in Westlaw, which retrieves all history on the patent including any litigation.

2) I performed a search on the patent in Lexis CourtLink for any open dockets or closed cases.

3) I performed a search in Lexis in the Federal Courts and Administrative Materials databases for any cases found.

4) I performed a search in Lexis in the IP Journal and Periodicals database for any articles on the patent.

5) I performed a search in Lexis in the news databases for any articles about the patent or any articles about litigation on this patent.

Westlaw.

Date of Printing: May 03, 2013

KEYCITE

C US PAT 8036988 SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD TRANSACTIONS, (Oct 11, 2011)

History

Direct History

=> 1 **SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD TRANSACTIONS,** US PAT 8036988 (U.S. PTO Utility Oct 11, 2011)

Patent Family

2 METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES OF GOODS OR SERVICES THROUGH REMOTE COMMERCIAL TRANSACTIONS E.G. INTERNET, INVOLVES PROVIDING AUTHORIZATION FOR PURCHASE SO AS TO CONFIRM WHETHER PURCHASE PARAMETERS ARE WITHIN CATEGORY, Derwent World Patents Legal 2011-D08434

Patent Status Files

.. Certificate of Correction, (OG DATE: Mar 05, 2013)

.. Request for Re-Examination, (OG DATE: Nov 27, 2012)

Docket Summaries

5 D' AGOSTINO v. MASTERCARD INC. ET AL, (D.DEL. Apr 26, 2013) (NO. 1:13CV00738), (35 USC 271 PATENT INFRINGEMENT)

Prior Art (Coverage Begins 1976)

C 6 ACCESS SECURITY CONTROL, US PAT 4599509 (U.S. PTO Utility 1986)

C 7 ACCESS SECURITY CONTROL, US PAT 4395628 (U.S. PTO Utility 1983)

C 8 ANONYMOUS CREDIT CARD TRANSACTIONS, US PAT 5420926Assignee: AT&T Corp., (U.S. PTO Utility 1995)

C 9 ANTI-FRAUD VERIFICATION SYSTEM USING A DATA CARD, US PAT 5457747Assignee: Drexler Technology Corporation, (U.S. PTO Utility 1995)

C 10 APPARATUS AND METHOD FOR ROUTING ENCRYPTED TRANSACTION CARD IDENTIFYING DATA THROUGH A PUBLIC TELEPHONE NETWORK, US PAT 6598031Assignee: EDI Secure LLLP, (U.S. PTO Utility 2003)

C 11 APPARATUS AND METHODS FOR IMPROVED CREDIT CARDS AND CREDIT CARD TRANSACTIONS, US PAT 6422462 (U.S. PTO Utility 2002)

C 12 APPARATUS AND SYSTEM FOR MANAGING A CARD NUMBER, US PAT 5893907 (U.S. PTO Utility 1999)

C 13 APPARATUS FOR CHECKING THE USER OF A CARD IN CARD-ACTUATED MACHINES, US PAT 4048475Assignee: Omron Tateisi Electronics Company, (U.S. PTO Utility 1977)

C 14 APPARATUS FOR GENERATING ENCRYPTION/DECRYPTION LOOK-UP TABLES USING A SESSION KEY, US PAT 5832087Assignee: Chantilley Corporation Limited, (U.S. PTO Utility 1998)

C 15 APPARATUS FOR KEY DISTRIBUTION IN AN ENCRYPTION SYSTEM, US PAT 5768381Assignee: Chantilley Corporation Limited, (U.S. PTO Utility 1998)

C 16 APPARATUS, SYSTEM AND METHOD FOR CREATING CREDIT VOUCHERS USABLE AT POINT OF PURCHASE STATIONS, US PAT 5010485Assignee: JBH Ventures, (U.S. PTO Utility 1991)

C 17 AUTHENTICATION SYSTEM USING ONE-TIME PASSWORDS, US PAT 5592553Assignee: International Business Machines, (U.S. PTO Utility 1997)

C 18 AUTOMATED BANKING SYSTEM FOR DISPENSING MONEY ORDERS, WIRE TRANSFER AND BILL PAYMENT, US PAT 6012048Assignee: Capital Security Systems, Inc., (U.S. PTO Utility 2000)

C 19 AUTOMATED, CLASSIFIED EXPENDITURE DATA CARD RECORDING SYSTEM, US PAT 5748908 (U.S. PTO Utility 1998)

C 20 AUTOMATED INTERACTIVE CLASSIFIED AD SYSTEM FOR THE INTERNET, US PAT 6253188Assignee: Thomson Newspapers, Inc., (U.S. PTO Utility 2001)

C 21 AUTOMATED PURCHASING CONTROL SYSTEM, US PAT 5621201Assignee: Visa International, (U.S. PTO Utility 1997)

C 22 AUTOMATED PURCHASING CONTROL SYSTEM, US PAT 5500513Assignee: Visa International, (U.S. PTO Utility 1996)

C 23 AUTOMATIC BANKING SYSTEM, US PAT 4423316Assignee: Omron Tateisi Electronics Co., (U.S. PTO Utility 1983)

C 24 BUSINESS-TO-BUSINESS COMMERCE USING FINANCIAL TRANSACTION NUMBERS, US PAT APP 20030018567Assignee: Orbis Patents Ltd., (U.S. PTO Application 2003)

C 25 CARD CHARGING SYSTEMS, US PAT 6375084Assignee: Transmo Limited, (U.S. PTO Utility 2002)

C 26 CARD VALIDATION, METHOD AND SYSTEM, US PAT 4016405Assignee: Diebold, Incorporated, (U.S. PTO Utility 1977)

C 27 CARDLESS PAYMENT SYSTEM, US PAT 6341724Assignee: First USA Bank, NA, (U.S. PTO Utility 2002)

C 28 CARDLESS PAYMENT SYSTEM, US PAT 6227447Assignee: First USA Bank, NA, (U.S. PTO Utility 2001)

C 29 CATEGORIZATION OF PURCHASED ITEMS FOR EACH TRANSACTION BY A SMART CARD, US PAT 5559313Assignee: Lucent Technologies Inc., (U.S. PTO Utility 1996)

H 30 CENTRALIZED CONSUMER CASH VALUE ACCUMULATION SYSTEM FOR MULTIPLE

MERCHANTS, US PAT RE36116 (U.S. PTO Reissue 1999)

C 31 CENTRALIZED CONSUMER CASH VALUE ACCUMULATION SYSTEM FOR MULTIPLE MERCHANTS, US PAT 5287268 (U.S. PTO Utility 1994)

C 32 CENTRALIZED CONSUMER CASH VALUE ACCUMULATION SYSTEM FOR MULTIPLE MERCHANTS, US PAT 5202826 (U.S. PTO Utility 1993)

C 33 CENTRALIZED CONSUMER CASH VALUE ACCUMULATION SYSTEM FOR MULTIPLE MERCHANTS, US PAT 4941090 (U.S. PTO Utility 1990)

C 34 CENTRALIZED CONSUMER CASH VALVE ACCUMULATION SYSTEM FOR MULTIPLE MERCHANTS, US PAT 5117355 (U.S. PTO Utility 1992)

C 35 CHARITABLE CONTRIBUTION CENTRALIZATION SYSTEM AND APPARATUS, US PAT 5555497 (U.S. PTO Utility 1996)

C 36 CHILDREN'S CREDIT OR DEBIT CARD SYSTEM, US PAT 5953710 (U.S. PTO Utility 1999)

C 37 CODING FORMULA FOR VERIFYING CHECKS AND CREDIT CARDS, US PAT 5754653 (U.S. PTO Utility 1998)

C 38 COMPUTERIZED PAYMENT SYSTEM FOR PURCHASING GOODS AND SERVICES ON THE INTERNET, US PAT 5757917Assignee: First Virtual Holdings Incorporated, (U.S. PTO Utility 1998)

C 39 COMPUTERIZED PURCHASING SYSTEM AND METHOD FOR MEDIATING PURCHASE TRANSACTIONS OVER AN INTERACTIVE NETWORK, US PAT 5878141Assignee: Microsoft Corporation, (U.S. PTO Utility 1999)

C 40 COMPUTERIZED SYSTEM FOR MAKING PAYMENTS AND AUTHENTICATING TRANSACTIONS OVER THE INTERNET, US PAT 5826241Assignee: First Virtual Holdings Incorporated, (U.S. PTO Utility 1998)

C 41 COMPUTING AND INDICATING DEVICE, US PAT 4856062 (U.S. PTO Utility 1989)

C 42 CONSUMER ORIENTED SMART CARD SYSTEM AND AUTHENTICATION TECHNIQUES, US PAT 5193114 (U.S. PTO Utility 1993)

C 43 CONTEXTUAL DATA REPRESENTATION AND RETRIEVAL METHOD, US PAT 6470490 (U.S. PTO Utility 2002)

C 44 COUNTERFEIT-PROOF IDENTIFICATION CARD, US PAT 5694471Assignee: V-ONE Corporation, (U.S. PTO Utility 1997)

C 45 CREDIT CARD-BASED ACCOUNTING SERVICE SYSTEM FOR A NETWORK, US PAT 5583918Assignee: Fujitsu Limited, (U.S. PTO Utility 1996)

C 46 CREDIT CARD PAGER APPARATUS, US PAT 5192947 (U.S. PTO Utility 1993)

C 47 CREDIT CARD SPENDING AUTHORIZATION CONTROL SYSTEM, US PAT 5914472Assignee: AT&T Corp, (U.S. PTO Utility 1999)

C 48 CREDIT CARD SYSTEM AND METHOD, US PAT 6636833Assignee: Obis Patents Ltd., (U.S. PTO Utility 2003)

C 49 CREDIT CARD SYSTEM AND METHOD, US PAT APP 20030028481Assignee: Orbis Patents, Ltd., (U.S. PTO Application 2003)

C 50 CREDIT CARD SYSTEM AND METHOD OF ISSUING CREDIT CARD USING SUCH A SYSTEM, US PAT 5883452Assignee: Nippon Shinpan Co., Ltd., (U.S. PTO Utility 1999)

C 51 CREDIT CARD SYSTEM AND METHOD OF USING CREDIT CARD WITH SUCH CREDIT CARD SYSTEM, US PAT 5777306Assignee: Nippon Shinpan Co., Ltd., (U.S. PTO Utility 1998)

C 52 CREDIT/CHARGE CARD SYSTEM ENABLING PURCHASERS TO CONTRIBUTE TO SELECTED CHARITIES, US PAT 5466919 (U.S. PTO Utility 1995)

C 53 CRYPTOGRAPHIC METHOD FOR UPDATING FINANCIAL RECORDS, US PAT 5231666Assignee: International Business Machines, (U.S. PTO Utility 1993)

C 54 CURRENCY TRANSFER SYSTEM AND METHOD, US PAT 5326960 (U.S. PTO Utility 1994)

C 55 CURRENCY TRANSFER SYSTEM AND METHOD USING FIXED LIMIT CARDS, US PAT 5350906 (U.S. PTO Utility 1994)

▷ 56 DATA PROCESSING METHOD OF CONFIGURING AND MONITORING A SATELLITE SPENDING CARD LINKED TO A HOST CREDIT CARD, US PAT 5864830 (U.S. PTO Utility 1999)

C 57 DIGITAL ACTIVE ADVERTISING, US PAT 6195649Assignee: Open Market, Inc., (U.S. PTO Utility 2001)

C 58 DIGITAL ACTIVE ADVERTISING, US PAT 5724424Assignee: Open Market, Inc., (U.S. PTO Utility 1998)

C 59 DIGITAL MONEY WITH USAGE-CONTROL, US PAT APP 20020152158Assignee: INTERNATIONAL BUSINESS MACHINES, (U.S. PTO Application 2002)

C 60 DIRECT TELEPHONE DIAL ORDERING SERVICE, US PAT 5023904Assignee: Science Dynamics Corporation, (U.S. PTO Utility 1991)

C 61 ELECTRONIC CASHLESS TRANSACTION SYSTEM, US PAT 5428684Assignee: Fujitsu Limited, (U.S. PTO Utility 1995)

C 62 ELECTRONIC COMMERCE USING A SECURE COURIER SYSTEM, US PAT 5671279Assignee: Netscape Communications Corporation, (U.S. PTO Utility 1997)

C 63 ELECTRONIC FUNDS TRANSFER INSTRUMENTS, US PAT 5677955Assignee: Financial Services Technology Consortium; The First National Bank of Boston; Bell Communications Research, Inc., (U.S. PTO Utility 1997)

C 64 ELECTRONIC FUNDS TRANSFER SYSTEM WITH MEANS FOR VERIFYING A PERSONAL IDENTIFICATION NUMBER WITHOUT PRE- ESTABLISHED SECRET KEYS, US PAT 4797920Assignee: MasterCard International, Inc., (U.S. PTO Utility 1989)

C 65 ELECTRONIC MONEY CARD, ELECTRONIC MONEY RECEIVING/PAYING MACHINE, AND ELECTRONIC MONEY CARD EDITING DEVICE., US PAT APP 20010011249 (U.S. PTO Application 2001)

C 66 ELECTRONIC ONLINE COMMERCE CARD WITH CUSTOMER GENERATED TRANSACTION PROXY NUMBER FOR ONLINE TRANSACTIONS, US PAT 6000832Assignee: Microsoft Corporation, (U.S. PTO Utility 1999)

C 67 ELECTRONIC ONLINE COMMERCE CARD WITH TRANSACTIONPROXY NUMBER FOR ONLINE TRANSACTIONS, US PAT 5883810Assignee: Microsoft Corporation, (U.S. PTO Utility 1999)

C 68 ELECTRONIC PAYMENT SYSTEM EMPLOYING LIMITED-USE ACCOUNT NUMBER, US PAT 6339766Assignee: TransactionSecure, (U.S. PTO Utility 2002)
C 69 ENHANCED SECURITY FOR A SECURE TOKEN CODE, US PAT 5485519Assignee: Security Dynamics Technologies, Inc., (U.S. PTO Utility 1996)
C 70 FINANCIAL CARDS, US PAT APP 20030216997 (U.S. PTO Application 2003)
C 71 FINANCIAL TRANSACTION SYSTEM, US PAT 5822737 (U.S. PTO Utility 1998)
C 72 FINANCIAL TRANSACTION SYSTEM, US PAT 4988849Assignee: Hitachi, Ltd., (U.S. PTO Utility 1991)
C 73 FRAUD PROTECTION FOR CARD TRANSACTIONS, US PAT 5311594Assignee: AT&T Bell Laboratories, (U.S. PTO Utility 1994)
C 74 IDENTIFICATION VERIFICATION METHOD AND SYSTEM, US PAT 4679236 (U.S. PTO Utility 1987)
C 75 INFORMATION MANAGEMENT, RETRIEVAL AND DISPLAY SYSTEM AND ASSOCIATED METHOD, US PAT 6484166Assignee: Evresearch, Ltd., (U.S. PTO Utility 2002)
C 76 INSTANT CREDIT CARD MARKETING SYSTEM FOR RESERVATIONS FOR FUTURE SERVICES, US PAT 6144948Assignee: Walker Digital, LLC, (U.S. PTO Utility 2000)
C 77 INTEGRATED SYSTEM FOR CONTROLLING MASTER ACCOUNT AND NESTED SUB-ACCOUNT(S), US PAT 5826243Assignee: Merrill Lynch & Co., Inc., (U.S. PTO Utility 1998)
H 78 INTERNET BILLING METHOD, US PAT 5794221 (U.S. PTO Utility 1998)
C 79 MAGNETIC SMARTCARD, US PAT 5434398Assignee: Labenski, Haim, (U.S. PTO Utility 1995)
H 80 METHOD AND APPARATUS FOR ELECTRONIC COMMERCE, US PAT 5903878 (U.S. PTO Utility 1999)
C 81 METHOD AND APPARATUS FOR FUNDS AND CREDIT LINE TRANSFERS, US PAT 6267292Assignee: Walker Digital, LLC, (U.S. PTO Utility 2001)
C 82 METHOD AND APPARATUS FOR IMPROVED SECURITY USING ACCESS CODES, US PAT 5239583 (U.S. PTO Utility 1993)
C 83 METHOD AND APPARATUS FOR MARKING PARTS, US PAT 4269874Assignee: Diffracto Ltd., (U.S. PTO Utility 1981)
C 84 METHOD AND APPARATUS FOR PERSONAL VERIFICATION UTILIZING NONPREDICTABLE CODES AND BIOCHARACTERISTICS, US PAT 4998279 (U.S. PTO Utility 1991)
C 85 METHOD AND APPARATUS FOR POSITIVELY IDENTIFYING AN INDIVIDUAL, US PAT 4720860Assignee: Security Dynamics Technologies, Inc., (U.S. PTO Utility 1988)
C 86 METHOD AND APPARATUS FOR PROVIDING SECURE ACCESS TO A LIMITED ACCESS SYSTEM, US PAT 5163097Assignee: DynamicServe, Ltd., (U.S. PTO Utility 1992)
C 87 METHOD AND APPARATUS FOR RESTRICTING CREDIT CARD COMMUNICATION CALLS, US PAT 4893330Assignee: American Telephone and Telegraph Company,, (U.S. PTO Utility 1990)
C 88 METHOD AND APPARATUS FOR SECURE IDENTIFICATION AND VERIFICATION, US PAT 5097505Assignee: Securities Dynamics Technologies, Inc., (U.S. PTO Utility 1992)

C 89 METHOD AND APPARATUS FOR SECURING CREDIT CARD TRANSACTIONS, US PAT 5317636Assignee: Arris, Inc., (U.S. PTO Utility 1994)

C 90 METHOD AND DEVICE FOR GENERATING A SINGLE-USE FINANCIAL ACCOUNT NUMBER, US PAT 6163771Assignee: Walker Digital, LLC, (U.S. PTO Utility 2000)

C 91 METHOD AND SYSTEM FOR CONDUCTING SECURE PAYMENTS OVER A COMPUTER NETWORK, US PAT APP 20020116341 (U.S. PTO Application 2002)

C 92 METHOD AND SYSTEM FOR GIFT CREDIT CARD, US PAT 5984180 (U.S. PTO Utility 1999)

C 93 METHOD AND SYSTEM FOR MANAGING A DATA OBJECT SO AS TO COMPLY WITH PREDETERMINED CONDITIONS FOR USAGE, US PAT 5845281Assignee: MediaDNA, Inc., (U.S. PTO Utility 1998)

C 94 METHOD AND SYSTEM FOR PROVIDING TEMPORARY CREDIT AUTHORIZATIONS, US PAT 6456984Assignee: Qwest Communications International Inc., (U.S. PTO Utility 2002)

C 95 METHOD AND SYSTEM FOR RETRIEVING RELEVANT DOCUMENTS FROM A DATABASE, US PAT 6370525Assignee: KCSL, Inc., (U.S. PTO Utility 2002)

C 96 METHOD FOR THE BILLING OF TRANSACTIONS OVER THE INTERNET, US PAT 5905736Assignee: AT&T Corp, (U.S. PTO Utility 1999)

C 97 METHOD FOR ENCOURAGING PURCHASE OF EXECUTABLE AND NON-EXECUTABLE SOFTWARE, US PAT 5509070Assignee: SoftLock Services Inc., (U.S. PTO Utility 1996)

C 98 METHOD FOR TRANSFERRING, RECEIVING AND UTILIZING ELECTRONIC GIFT CERTIFICATES, US PAT 6240397 (U.S. PTO Utility 2001)

C 99 METHOD OF CONTROLLING PAYMENT OF DEBTS, US PAT 6298335 (U.S. PTO Utility 2001)

C 100 MOBILE COMMUNICATION METHOD, AND MOBILE TELEPHONE SWITCHING STATION CUSTOMER MANAGEMENT SYSTEM, AND MOBILE UNIT FOR IMPLEMENTING THE SAME, US PAT 6064879Assignee: Fujitsu Limited, (U.S. PTO Utility 2000)

C 101 MULTI-LANGUAGE DOCUMENT SEARCH AND RETRIEVAL SYSTEM, US PAT 6466901Assignee: Apple Computer, Inc., (U.S. PTO Utility 2002)

C 102 MULTIMEDIA ELECTRONIC WALLET WITH GENERIC CARD, US PAT 5748737 (U.S. PTO Utility 1998)

C 103 MULTIPLE COMPANY CREDIT CARD, US PAT 3376661 (U.S. PTO Utility 1968)

▶ 104 NETWORK SALES SYSTEM, US PAT 5715314Assignee: Open Market, Inc., (U.S. PTO Utility 1998)

C 105 ON-LINE SECURED FINANCIAL TRANSACTION SYSTEM THROUGH ELECTRONIC MEDIA, US PAT 5729594 (U.S. PTO Utility 1998)

C 106 ON-LINE SHOPPING SYSTEM AND THE METHOD OF PAYMENT SETTLEMENT, US PAT 5890137Assignee: Kabushiki Kaisha N.K. Kikaku, (U.S. PTO Utility 1999)

C 107 OPEN NETWORK PAYMENT SYSTEM FOR PROVIDING FOR AUTHENTICATION OF PAYMENT ORDERS BASED ON A CONFIRMATION ELECTRONIC MAIL MESSAGE, US PAT 6049785Assignee: Open Market, Inc., (U.S. PTO Utility 2000)

C 108 PACKAGE ASSEMBLY AND METHOD FOR ACTIVATING PREPAID DEBIT CARDS, US

PAT 5777305Assignee: Incomm, (U.S. PTO Utility 1998)

C 109 PAYMENT AND TRANSACTIONS IN ELECTRONIC COMMERCE SYSTEM, US PAT 6029150Assignee: Certco, LLC, (U.S. PTO Utility 2000)

C 110 PERSONAL IDENTIFICATION ENCRYPTOR AND METHOD, US PAT 5363449Assignee: Tandem Computers Incorporated, (U.S. PTO Utility 1994)

C 111 PERSONAL IDENTIFICATION SYSTEMS, US PAT 5606614Assignee: British Telecommunications public limited, (U.S. PTO Utility 1997)

C 112 PERSONAL SECURITY SYSTEM, US PAT 5361062Assignee: Security Dynamics Technologies, Inc., (U.S. PTO Utility 1994)

C 113 PERSONAL UNIVERSAL IDENTITY CARD SYSTEM FOR FAILSAFE INTERACTIVE FINANCIAL TRANSACTIONS, US PAT 4707592 (U.S. PTO Utility 1987)

C 114 PERSONAL VERIFICATION SYSTEM, US PAT 3938091Assignee: Atalla Technovations Company, (U.S. PTO Utility 1976)

C 115 PIN VENDING DISPENSER, US PAT 5868236Assignee: Rademacher, Darrell G., (U.S. PTO Utility 1999)

C 116 PORTABLE PIN CARD, US PAT 5130519Assignee: Bush, George; Ross, Estelle, (U.S. PTO Utility 1992)

C 117 POSITIVE IDENTIFICATION DISPLAY DEVICE AND SCANNER FOR LOW COST COLLECTION AND DISPLAY OF GRAPHIC AND TEXT DATA IN A SECURE MANNER, US PAT 6202055Assignee: Image Data, LLC, (U.S. PTO Utility 2001)

▻ 118 PRE-PAID CARD SYSTEM AND METHOD, US PAT 5721768Assignee: Call Processing, Inc., (U.S. PTO Utility 1998)

C 119 PRE-PAID CARD SYSTEM AND METHOD, US PAT 5577109Assignee: Call Processing, Inc., (U.S. PTO Utility 1996)

C 120 PREPAYMENT METERING SYSTEM, US PAT 4629874Assignee: The De La Rue Company PLC, (U.S. PTO Utility 1986)

C 121 PREPAYMENT WRISTBAND AND COMPUTER DEBIT SYSTEM, US PAT 6352205Assignee: Busch Entertainment Corporation, (U.S. PTO Utility 2002)

C 122 PROGRAMMABLE CREDIT CARD, US PAT 5585787 (U.S. PTO Utility 1996)

C 123 PROGRAMMABLE TRANSACTION CARD, US PAT 5955961 (U.S. PTO Utility 1999)

C 124 PROVIDING VERIFICATION INFORMATION FOR A TRANSACTION, US PAT 5826245 (U.S. PTO Utility 1998)

C 125 PSEUDO-RANDOM SEQUENCE GENERATORS, US PAT 5323338Assignee: Enfranchise Sixty Limited, (U.S. PTO Utility 1994)

C 126 PUBLIC NETWORK MERCHANDISING SYSTEM, US PAT 5825881Assignee: Allsoft Distributing Inc., (U.S. PTO Utility 1998)

C 127 PURCHASE MANAGEMENT SYSTEM AND METHOD, US PAT 6014650 (U.S. PTO Utility 2000)

C 128 RECEPTION MODE CONTROL IN RADIO RECEIVERS FOR RECEIVING BOTH VSB AND QAM DIGITAL TELEVISION SIGNALS, US PAT 5959699Assignee: SamSung Electronics Co., Ltd., (U.S. PTO Utility 1999)

C 129 RECOGNITION APPARATUS AND METHOD FOR SECURITY SYSTEMS, US PAT 5093861Assignee: Cardkey Systems, Inc., (U.S. PTO Utility 1992)

C 130 RESTRICTED PURPOSE, COMMERCIAL, MONETARY REGULATION METHOD, US PAT 4725719Assignee: First City National Bank of Austin, (U.S. PTO Utility 1988)

C 131 RETAIL METHOD OVER A WIDE AREA NETWORK, US PAT 5899980Assignee: Trivnet Ltd., (U.S. PTO Utility 1999)

C 132 SECURE COMMUNICATIONS SYSTEM FOR REMOTELY LOCATED COMPUTERS, US PAT 5196840Assignee: International Business Machines, (U.S. PTO Utility 1993)

C 133 SECURE CREDIT CARD, US PAT 4667087Assignee: Quintana, Max A.; King, Robert E.; Morgan, Bernard L.; Lennon, Alton Y., (U.S. PTO Utility 1987)

C 134 SECURE CREDIT CARD WHICH PREVENTS UNAUTHORIZED TRANSACTIONS, US PAT 5478994 (U.S. PTO Utility 1995)

C 135 SECURE CREDIT/DEBIT CARD AUTHORIZATION, US PAT 5485510Assignee: AT&T Corp., (U.S. PTO Utility 1996)

C 136 SECURE METHOD FOR COMMUNICATING CREDIT CARD DATA WHEN PLACING AN ORDER ON A NON- SECURE NETWORK, US PAT 5727163Assignee: Amazon.Com, Inc., (U.S. PTO Utility 1998)

C 137 SECURE NETWORKED TRANSACTION SYSTEM, US PAT APP 20020077837 (U.S. PTO Application 2002)

C 138 SECURE SYSTEM FOR ELECTRONIC SELLING, US PAT 5799285 (U.S. PTO Utility 1998)

C 139 SECURED DISPOSABLE DEBIT CARD CALLING SYSTEM AND METHOD, US PAT 5504808 (U.S. PTO Utility 1996)

C 140 SIGNATURE CAPTURING PRINTER AND DATA CARD TERMINAL, US PAT 5479530Assignee: Microbilt Corporation, (U.S. PTO Utility 1995)

C 141 SMART CARD WITH MULTIPLE CHARGE ACCOUNTS AND PRODUCT ITEM TABLES DESIGNATING THE ACCOUNT TO DEBIT, US PAT 5649118Assignee: Lucent Technologies Inc., (U.S. PTO Utility 1997)

C 142 SYSTEM AND METHOD FOR BILLING FOR TRANSACTIONS CONDUCTED OVER THE INTERNET FROM WITHIN AN INTRANET, US PAT 5845267Assignee: AT&T Corp, (U.S. PTO Utility 1998)

C 143 SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES, US PAT 7840486 (U.S. PTO Utility 2010)

C 144 SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES, US PAT APP 20060031161 (U.S. PTO Application 2006)

C 145 SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES, US PAT 6324526 (U.S. PTO Utility 2001)

C 146 SYSTEM AND METHOD FOR PERFORMING SECURE USER ACCOUNT PURCHASES, US PAT APP 20020120587 (U.S. PTO Application 2002)

C 147 SYSTEM AND METHOD FOR PRE-AUTHORIZATION OF INDIVIDUAL ACCOUNT REMOTE TRANSACTIONS, US PAT 6226624 (U.S. PTO Utility 2001)

C 148 SYSTEM AND METHOD FOR PRE-AUTHORIZATION OF INDIVIDUAL ACCOUNT

TRANSACTIONS, US PAT 5991750Assignee: GE Capital, (U.S. PTO Utility 1999)

C 149 SYSTEM AND METHOD FOR PROVIDING OPERATOR AND CUSTOMER SERVICES, US PAT 6188761Assignee: MCI Communications Corporation, (U.S. PTO Utility 2001)

C 150 SYSTEM AND METHOD FOR PSEUDO CASH TRANSACTIONS, US PAT 5913203Assignee: Jaesent Inc., (U.S. PTO Utility 1999)

C 151 SYSTEM AND METHOD FOR REAL-TIME BUNDLED TELECOMMUNICATIONS ACCOUNT PROCESSING AND BILLING, US PAT 6885857Assignee: Verisign, Inc., (U.S. PTO Utility 2005)

C 152 SYSTEM AND METHODS TO SELECT AUTHORIZED VENDORS FOR PREPAID DEBIT CARD/CREDIT CARD, US PAT APP 20100012720 (U.S. PTO Application 2010)

C 153 SYSTEM AND PROCESS FOR ISSUING AND MANAGING FORCED REDEMPTION VOUCHERS HAVING ALIAS ACCOUNT NUMBERS, US PAT 6330544Assignee: Walker Digital, LLC, (U.S. PTO Utility 2001)

C 154 SYSTEM FOR PREVENTING FRAUDULENT USE OF CREDIT CARD, US PAT 5163098 (U.S. PTO Utility 1992)

C 155 SYSTEM FOR SECURED CREDIT CARD TRANSACTIONS ON THE INTERNET, US PAT 5956699Assignee: Jaesent Inc., (U.S. PTO Utility 1999)

C 156 SYSTEM FOR VERIFYING THE USER OF A CARD, US PAT 4023012Assignee: Omron Tateisi Electronics Co., (U.S. PTO Utility 1977)

C 157 SYSTEM INTEGRATING CREDIT CARD TRANSACTIONS INTO A FINANCIAL MANAGEMENT SYSTEM, US PAT 6343279Assignee: American Management Systems, Inc., (U.S. PTO Utility 2002)

C 158 SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR NETWORK ELECTRONIC AUTHORIZATION UTILIZING AN AUTHORIZATION INSTRUMENT, US PAT 5815657Assignee: VeriFone, Inc., (U.S. PTO Utility 1998)

C 159 SYSTEMS FOR FINANCIAL AND ELECTRONIC COMMERCE, US PAT APP 20030097331 (U.S. PTO Application 2003)

C 160 TAMPER RESISTANT SMART CARD AND METHOD OF PROTECTING DATA IN A SMART CARD, US PAT 6068192Assignee: Micron Technology, Inc., (U.S. PTO Utility 2000)

C 161 TELEPHONE DEBIT CARD DISPENSER AND METHOD, US PAT 5696908Assignee: Southeast Phonecard, Inc., (U.S. PTO Utility 1997)

C 162 TOKENLESS BIOMETRIC ATM ACCESS SYSTEM, US PAT 6154879Assignee: SmartTouch, Inc., (U.S. PTO Utility 2000)

C 163 TRANSACTION AUTHENTICATION USING A CENTRALLY GENERATED TRANSACTION IDENTIFIER, US PAT 5343529 (U.S. PTO Utility 1994)

C 164 TRANSACTION DEVICE, EQUIPMENT AND METHOD FOR PROTECTING ACCOUNT NUMBERS AND THEIR ASSOCIATED PERSONAL IDENTIFICATION NUMBERS, US PAT 5627355 (U.S. PTO Utility 1997)

C 165 TRANSACTION SECURITY APPARATUS AND METHOD, US PAT 5903830 (U.S. PTO Utility 1999)

C 166 TRANSACTION SECURITY SYSTEM USING TIME VARIANT PARAMETER, US PAT

4747050Assignee: International Business Machines, (U.S. PTO Utility 1988)

C 167 UNIVERSAL ELECTRONIC TRANSACTION CARD INCLUDING RECEIPT STORAGE AND SYSTEM AND METHODS OF CONDUCTING ELECTRONIC TRANSACTIONS, US PAT 5590038 (U.S. PTO Utility 1996)

C 168 USER-SPECIFIED CREDIT CARD SYSTEM, US PAT 6029890 (U.S. PTO Utility 2000)

C 169 VIRTUAL CALLING CARD SYSTEM, US PAT 5479494Assignee: AT&T Corp., (U.S. PTO Utility 1995)

C 170 WIRELESS TELEPHONY FOR COLLECTING TOLLS, CONDUCTING FINANCIAL TRANSACTIONS, AND AUTHORIZING OTHER ACTIVITIES, US PAT 5991749 (U.S. PTO Utility 1999)

Click a docket number below to view a docket.

Patent Search Results

Edit Search

Results: 1 cases and their patents, totaling 1 items.

Re-run Search

This search was run on 5/3/2013

Update Docket(s) Email Docket(s)

Printer Friendly List
Email List
Customize List

Items 1 to 1 of 1

	Patent	Class	Subclass	Description	Court (All)	Docket Number	Filed	Date Retrieved
☐	8,036,988	705	44	D' Agostino V. Mastercard Inc. Et Al	US-DIS-DED	1:13cv738	4/26/2013	4/29/2013

Items 1 to 1 of 1

Update Docket(s) Email Docket(s)

Printer Friendly List
Email List
Customize List

US District Court Civil Docket

U.S. District - Delaware
(Wilmington)

1:13cv738

D' Agostino v. Mastercard Inc. et al

This case was retrieved from the court on Monday, April 29, 2013

Date Filed:	**04/26/2013**	**Class Code:**	**OPEN**
Assigned To:	**Unassigned Judge**	**Closed:**	**No**
Referred To:		**Statute:**	**35:271**
Nature of suit:	**Patent (830)**	**Jury Demand:**	**Plaintiff**
Cause:	**Patent Infringement**	**Demand Amount:**	**$0**
Lead Docket:	**None**	**NOS Description:**	**Patent**
Other Docket:	**None**		
Jurisdiction:	**Federal Question**		

Litigants	Attorneys
John D' Agostino Plaintiff	George Pazuniak LEAD ATTORNEY;ATTORNEY TO BE NOTICED Pazuniak Law Office 1201 North Orange Street 7th Floor, Suite 7114 Wilmington, DE 19801-1186 USA (302) 478-4230 Email:Gp@del-Iplaw.Com
Mastercard Inc. Defendant	
Mastercard International Incorporated Defendant	
Orbiscom Ltd. Defendant	
Orbiscom Inc. Defendant	
Citigroup Inc. Defendant	
Discover Financial Services Defendant	
Xerxes Engineering Llc Defendant	

Date	#	Proceeding Text

04/26/2013	1	COMPLAINT FOR PATENT INFRINGEMENT filed with Jury Demand against Citigroup Inc., Discover Financial Services, MasterCard International Incorporated, Mastercard Inc., Orbiscom Inc., Orbiscom Ltd., Xerxes Engineering LLC - Magistrate Consent Notice to Pltf. (Filing fee $ 350, receipt number 0311-1278561.) - filed by John D' Agostino. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Civil Cover Sheet)(jeb,) (Entered: 04/29/2013)
04/26/2013	2	Notice, Consent and Referral forms re: U.S. Magistrate Judge jurisdiction (jeb,) (Entered: 04/29/2013)
04/26/2013	3	Report to the Commissioner of Patents and Trademarks for Patent/Trademark Number(s) 8,036,988; 7,840,486;. (jeb,) (Entered: 04/29/2013)
04/29/2013	--	Summons Issued with Magistrate Consent Notice attached as to Citigroup Inc. on 4/29/2013; Discover Financial Services on 4/29/2013; MasterCard International Incorporated on 4/29/2013; Mastercard Inc. on 4/29/2013; Orbiscom Inc. on 4/29/2013; Orbiscom Ltd. on 4/29/2013; Xerxes Engineering LLC on 4/29/2013. Requesting party or attorney should pick up issued summons at the Help Desk, Room 4209, or call 302-573-6170 and ask the Clerk to mail the summons to them. (jeb,) (Entered: 04/29/2013)
05/01/2013	--	Case Assigned to Judge Gregory M. Sleet. Please include the initials of the Judge (GMS) after the case number on all documents filed. (rjb) (Entered: 05/01/2013)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Reexamination of	)	**MAIL STOP *EX PARTE* REEXAM**
John D'AGOSTINO	)	Examiner: SHRESTHA, Bijendra K.
Patent No.: 8,036,988	)	Control No.: 90/012,517
Issued: October 11, 2011	)	Group Art Unit: 3992
For: SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES	)	Confirmation No.: 5785

PETITION FOR REVIEW UNDER 37 CFR § 1.181

ATTN: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The undersigned ("Requester") requests review of the Order Denying Request for *Ex Parte* Reexamination in the above-identified application of December 6, 2012. The undersigned respectfully submits that the denial of the Request for Ex Parte Reexamination of claims 1 through 38 of the above-captioned patent (the "'988 Patent"), is based on an overlooked aspect of the applied art and the Order presents an improper interpretation of the claims. A substantial new question of patentability is raised both in the Request of September 12, 2012 and the Order for at least the following reasons.

Reasons for Review

Establishing a Substantial New Question of Patentability

As stated at page 3 of the Order, during the prosecution history of the '988 Patent, Mr. D'Agostino argued that the prior art, under which the present claims at issue were then rejected, required "that a particular merchant for a specific transaction to be known and identified to generate the transaction code," but that the "claimed method does not identify a merchant prior to the generation of the transaction code." In light of these remarks, the claims were allowed for the recitation of "defining at least one payment category to include at least limiting a number of transactions to one or more merchants, said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants." (As mentioned in the Order, the prior art in the underlying patent application, Franklin, was characterized as "designating" a single merchant by attaching transaction details including the merchant identity when generating a transaction code, whereas the transaction code of the '988 Patent does not - though it is not clear to the undersigned how this recitation added to the '988 Patent claims supports this distinction because the payment category of Franklin that requires the transaction details be submitted is defined before a merchant is identified.)

The above recitation specifies, in light of the statement by Mr. D'Agostino, that a payment category be defined to limit a number of transactions to "one or more merchants," with the limitation being included in the category without any particular merchant being identified. As demonstrated below, this aspect relied upon for allowance is found in Cohen, discussed below.

Cohen Raises a Substantial New Question of Patentability

Cohen raises a substantial new question of patentability as to the claims under both the Requester's broadest reasonable interpretation, and the improper, narrow interpretation offered in the Order (as explained below).

The Request is incorporated by reference herein, but fo rht econvenience of the Office, an abbreviated version of Appendix A, claim chart for Claim 1, is anticipated by Cohen is reproduced below:

'988 Patent Claims	Disclosure in Cohen (6,422,462)
1. A method of performing secure credit card purchases, said method comprising:	"It is an object of the present invention to provide improved credit cards and methods for credit card transactions…[i]t is a further object of the present invention to provide methods and apparatus for secure transmission of credit card information" (Cohen, col. 1, ll. 48-62).
a) contacting a custodial authorizing entity having custodial responsibility of account parameters of a customer's account that is used to make credit card purchases;	"…a user dials into her credit card company…" (Cohen, col. 3, ll. 42-44).
b) supplying said custodial authorizing entity with at least account identification data of said customer's account;	"…a user dials into her credit card company…and after providing the ordinary credit card number and verification data…" (Cohen, col. 3, ll. 42-45).
c) defining at least one payment category to include at least limiting a number of transactions to one or more merchants,	"The card can also be customized for only particular uses or groups of uses" (Cohen, col. 7, ll. 66-67). "A customized credit card could be issued to the user which is only valid for use for

	that particular type of charge (computer hardware or software stores)…[or] for use in a particular store itself or a particular chain of stores" (Cohen, col. 8, ll. 25-34).
said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants;	"A customized credit card could be issued to the user which is only valid for use for that particular *type* of charge (computer hardware or software stores)…" (Cohen, col. 8, ll. 25-28) (emphasis added).
d) designating said payment category;	"…a user can indicate in advance of purchase…what the single use or the customized credit card number is to be used for" (Cohen, col. 3, ll. 49-52).
e) generating a transaction code by a processing computer of said custodial authorizing entity,	"A user dials into her credit card company before making a transaction, and…is provided with a disposable or customized number" (Cohen, col. 3, ll. 41-45). "These credit cards or credit card numbers are generated…" (Cohen, col. 2, ll. 35-36).
said transaction code reflecting at least the limits of said designated payment category to make a purchase within said designated payment category;	"A customized credit card could be issued to the user which is only valid for use for that particular type of charge" (Cohen, col. 8, ll. 25-27). "A customized credit card…is only valid for use for that particular type of charge…such that if the employee tries to use it for anything else…the charge will be declined" (Cohen, col. 8, ll. 25-32)
f) communicating said transaction code to a merchant to consummate a purchase with defined purchase parameters;	"…the user transmits his or her credit card information to the vendor. That vendor then verifies the transaction…" (Cohen, col. 5, ll. 36-37).
g) verifying that said defined purchase parameters are within said	"That vendor then verifies the transaction…" (Cohen, col. 5, ln. 37).

designated payment category; and	"A customized credit card…is only valid for use for that particular type of charge…such that if the employee tries to use it for anything else…the charge will be declined" (Cohen, col. 8, ll. 25-32)
h) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said designated payment category and to authorize payment required to complete the purchase.	"…the credit card company notes the identity of the vendor, authorizes the transaction (if the credit card number is valid and the purchaser has sufficient funds available), and forwards the authorization code to the vendor" (Cohen, col. 5, ll. 45-49).

The Order suggests Step c) is not met by Cohen, but in this discussion actually points to the language that meets this claim recitation. Specifically, at page 7 the Order cites to the Request where it is stated that Cohen discloses that transactions may be limited to, among other criteria, a *specific merchant or industry*. In fact, the Order even emphasizes the limitation along with other criteria disclosed by Cohen by underlining each of the criteria cited in the Request to the relevant portions of Cohen, but seems to overlook that that these "use" limitations meet the claim recitations. Specifically, the Order states:

> Requester points to Cohen's transaction restrictions as a basis for raising a substantial new question of patentability. However the restrictions noted not only are the same types of restrictions found by the Examiner in Franklin '832, they fail to address the claim language identified for patentability.
>
> Requester notes that Cohen's pre-arranged restrictions may include:
>
> "Examples of the customized uses for which a disposable or customized number can be indicated may include a time limit (col. 6, ln. 7), a specified sequence (col. 4, ln. 13), specific merchant or industry (col. 8, ll. 2-14), specific individuals or groups of individuals (col. 8, ll. 15-16), a specific merchant or merchants (col. 8, ll. 33-34), purchase amount (col. 8, ln. 44), geographic area (col. 8, ll. 58-59), security level (col. 10, ln. 5), etc. These various customized uses can also be used in combination, such as a customized number to be used on specific dates, for specific amounts, etc. (col. 10, ll. 24-35)" [request, page 13].
>
> "for use in a particular store itself or a particular chain of stores" [request, page 26].
>
> "only valid for that particular type of charge" [request, page 26].

Yes, some similar restrictions are found in Franklin (the prior art applied in the prosecution of the '988 Patent that was found by the ex parte examiner to disclose only pre-identification of the merchant), but Cohen does address the claim language.

The Order first acknowledges that "Cohen's restriction to 'specific merchant'(s) and "particular store"(s) would cover the claim language of restriction to "one or more merchants" as part of the category restriction" but then erroneously concludes:

> However, such a category restriction clearly cannot be defined "prior to any particular merchant being identified" as claim 1 requires. Cohen's "specific merchant"(s) or "particular store"(s) necessarily requires prior specifying of those merchant identities.

This is clearly not true when referring to restricting the transactions to a "specific industry". Though not specifically identified in Cohen or the '988 Patent, transactions can be limited to an industry by the use of merchant category codes (MCCs) that are conveyed with an transaction authorization request in currently used transaction processing systems. Cohen makes reference to this type of code by reference to "types

of charges" in passages such as: "For example, the card could be customized so that it is only good for airline reservations, such that if the employee tries to use it for any other type of charge, the charge will be declined, regardless of the amount of the transaction involved." Col. 8, lines 2-6.

As such, Cohen clearly discloses that transactions may be limited to a "specific industry" without identifying any specific or particular merchants. Cohen clearly meets the recitation of "defining at least one payment category to include at least limiting a number of transactions to one or more merchants, said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants."

As stated above and as overlooked in the Order, Cohen discloses that transactions may be limited to an industry "prior to any particular merchant being identified as one of said one or more merchants." Limiting to an industry would result in transactions being limited to "one or more merchants," those merchants in the specified industry, without any particular merchants being identified. As such, Cohen discloses the above recitation of the '988 Patent, where a payment category may be defined including limiting a number of transactions to one or more merchants (merchants in a specific industry) without identifying a particular merchant.

At page 3 of the Order, the Examiner stated that the claims of the '988 Patent were allowed due to the recitation of "defining at least one payment category to include at least limiting a number of transactions to one or more merchants, said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants. This is exactly what

Cohen discloses and establishes and is exactly what the ex parte examiner thought was absent from the prior art when allowing the claims under review. Accordingly, Cohen raises a substantial new question of patentability for this reason and the reasons provided in the initial Request.

Furthermore, Cohen raises the substantial new question of patentability under either interpretation of the above recitation of the claims at issue in the '988 Patent. Under the Examiner's interpretation that improperly narrows the scope of the claims, the recitation includes an extra limitation that the "one or more merchants" is restricted to a "finite number of merchants" where no particular merchant is identified at the time of the defining the category restriction. However, as stated above, Cohen discloses that transactions may be limited to an industry. One skilled in the art would understand that a specific industry would include a finite number of merchants. As such, the limiting of a number of transactions to an industry would result in limiting the number of transactions to those one or more merchants included in that industry, without identifying a particular merchant. Therefore, even under the interpretation set forth in the Order, Cohen still discloses the recitation of the claims at issue in the '988 Patent.

The Order Improperly Narrows the Scope of the Claims

The Order improperly interpreted the claims of the '988 Patent by reading in an extra limitation into the claims' scope. The Order interpreted the recitation of "defining at least one payment category to include at least limiting a number of transactions to one or more merchants" to further limit the recitation "one or more merchants" to "a finite number of merchants," which is, of course, improper. This is further explained below. On one hand, a substantial new question of patentability is present even under this interpretation, but on the other hand, the undersigned did not want this interpretation go unchallenged on the record.

As discussed in more detail in the Request, the limiting of the number of transactions to "one or more merchants" is, in practical effect, a non-limitation because a negative number of merchants or zero merchants would not make sense in the context of the claims. The term "one or more merchants" encompasses either a single merchant, two merchants, three merchants, one thousand merchants (such as might be present in a large industry), or even up to an infinite number of merchants, and the entire phrase encompasses limiting a number of transactions to any and all merchants, provided that no particular merchant is identified before defining the category.

In short, defining a payment category to limit a number of transactions to "one or more merchants" does not require that the number of merchants be finite.

At page 5 in the Order, it is alleged that such an interpretation is "unreasonable" and "over-broad" and that "one of ordinary skill in the art would find this to teach transactions to be restricted to a certain quantity of merchants." However, the Requester respectfully submits that the claims do not contain such a limitation.

Specifically, "one or more merchants" does not present an upper limit on the number of merchants. This is the phrase's plain meaning and how it would be understood by those skilled in the art. *See* MPEP § 2111.01.

Accordingly, the Order improperly narrows the scope of the claims by reading in an extra limitation to the claims, stating that the limiting of the number of transactions to "one or more merchants" must be of a "certain quantity of merchants." In fact, the Order goes so far as to assert, at page 5, that "the words in the claim require a restriction defined as a *finite number of merchants*" (emphasis added). This is clearly in error. Further, the Order fails to provide any support for such an assertion, but instead cites to the specification, col. 8, lines 18-34, which also does not identify any particular upper range. This cited passage states, *inter alia*:

> The payment category may also include a multi-transaction authorization wherein more than one purchase may be made from **one or a plurality of different merchants**, each of which may or may not be identified by the customer and pre-coded in association with the transaction code, and wherein a total cost of the plurality of purchases may not exceed a maximum limit amount. (Emphasis added)

Furthermore, as discussed above, one of skilled in the art would not understand the claim to require any such restriction, but instead, require only general limitation as to the merchants and not necessarily that a finite number of merchant is required. Thus, the Order did not provide the claims with their broadest reasonable interpretation.

Conclusion

In light of the foregoing, the Requester respectfully submits that Cohen's disclosure of the above recitation of the '988 patent raises a substantial new question of

patentability, and therefore respectfully submits that the *ex parte* request for reexamination of the '988 patent be granted for the reasons set forth herein and in the Request of September 12, 2012.

The undersigned does not believe any fee is required with the filing of this Petition. However, if a fee is required, then such fee is authorized to be charged to Deposit Account 02-4800.

Should any questions or residual issues arise, the Commissioner is invited to contact the undersigned at the number provided below. Prompt and favorable consideration of this Petition for Review is respectfully requested.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: Monday, January 7, 2013

By: _____
Charles F. Wieland III
Registration No. 33,096

Customer No. 21839
703 836 6620

Electronic Acknowledgement Receipt

EFS ID:	14632845
Application Number:	90012517
International Application Number:	
Confirmation Number:	5785
Title of Invention:	SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES
First Named Inventor/Applicant Name:	8036988
Customer Number:	34111
Filer:	Charles F. Wieland III/Christine Becker
Filer Authorized By:	Charles F. Wieland III
Attorney Docket Number:	253.005
Receipt Date:	07-JAN-2013
Filing Date:	12-SEP-2012
Time Stamp:	16:13:06
Application Type:	Reexam (Third Party)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Petition for Review of Reexam Denial	029_PetitionforReview.pdf	674041 93cbe7c294a9e9fd2a50b4365e86c508049779c2	no	11

Warnings:	
Information:	

Total Files Size (in bytes):	674041

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Reexamination of	**MAIL STOP *EX PARTE* REEXAM**
John D'AGOSTINO	Examiner: SHRESTHA, Bijendra K.
Patent No.: 8,036,988	Control No.: 90/012,517
Issued: October 11, 2011	Group Art Unit: 3992
For: SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES	Confirmation No.: 5785

CERTIFICATE OF SERVICE

ATTN: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

It is hereby certified by the undersigned that a true copy of the PETITION FOR REVIEW UNDER 37 CFR § 1.181 filed January 7, 2013, was mailed via courier to:

Stephen J. Lewellyn, Esq.
Maxey Law Offices, PLLC
15500 Roosevelt Boulevard, Suite 305
Clearwater, Florida 33760

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: January 7, 2013

By: _____
Charles F. Wieland III
Registration No. 33096

Customer No. 21839
703 836 6620

Electronic Acknowledgement Receipt

EFS ID:	14634375
Application Number:	90012517
International Application Number:	
Confirmation Number:	5785
Title of Invention:	SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES
First Named Inventor/Applicant Name:	8036988
Customer Number:	34111
Filer:	Charles F. Wieland III/Christine Becker
Filer Authorized By:	Charles F. Wieland III
Attorney Docket Number:	253.005
Receipt Date:	07-JAN-2013
Filing Date:	12-SEP-2012
Time Stamp:	17:10:15
Application Type:	Reexam (Third Party)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam Certificate of Service	029_CertificateofService.pdf	396703 8ca9b75518564ffcd741ce6e0217bb774ab477ec	no	1

Warnings:	
Information:	

Total Files Size (in bytes):	396703

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/012,517	09/12/2012	8036988	0076412-000029	5785

34111 7590 12/06/2012

Maxey Law Offices, PLLC
15500 Roosevelt Blvd.
SUITE 305
CLEARWATER, FL 33760

EXAMINER	
CARLSON, JEFFREY D	
ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
12/06/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

BUCHANAN, INGERSOLL & ROONEY PC

POST OFFICE BOX 1404

ALEXANDRIA, VA 22313-1404

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/012,517*.

PATENT NO. *8036988*.

ART UNIT *3992*.

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Order Granting / Denying Request For Ex Parte Reexamination	**Control No.** 90/012,517	**Patent Under Reexamination** 8036988
	Examiner JEFFREY CARLSON	**Art Unit** 3992

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The request for *ex parte* reexamination filed *12 September 2012* has been considered and a determination has been made. An identification of the claims, the references relied upon, and the rationale supporting the determination are attached.

Attachments: a)☐ PTO-892, b)☐ PTO/SB/08, c)☒ Other: *PTO-1449*

1. ☐ The request for *ex parte* reexamination is GRANTED.

RESPONSE TIMES ARE SET AS FOLLOWS:

For Patent Owner's Statement (Optional): TWO MONTHS from the mailing date of this communication (37 CFR 1.530 (b)). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).**

For Requester's Reply (optional): TWO MONTHS from the **date of service** of any timely filed Patent Owner's Statement (37 CFR 1.535). **NO EXTENSION OF THIS TIME PERIOD IS PERMITTED.** If Patent Owner does not file a timely statement under 37 CFR 1.530(b), then no reply by requester is permitted.

2. ☒ The request for *ex parte* reexamination is DENIED.

This decision is not appealable (35 U.S.C. 303(c)). Requester may seek review by petition to the Commissioner under 37 CFR 1.181 within ONE MONTH from the mailing date of this communication (37 CFR 1.515(c)). **EXTENSION OF TIME TO FILE SUCH A PETITION UNDER 37 CFR 1.181 ARE AVAILABLE ONLY BY PETITION TO SUSPEND OR WAIVE THE REGULATIONS UNDER 37 CFR 1.183.**

In due course, a refund under 37 CFR 1.26 (c) will be made to requester:

a) ☐ by Treasury check or,

b) ☒ by credit to Deposit Account No. *02-4800*, or

c) ☐ by credit to a credit card account, unless otherwise notified (35 U.S.C. 303(c)).

/Jeffrey D. Carlson/ Primary Examiner, Art Unit 3992		

cc:Requester (if third party requester)

DECISION DENYING EX PARTE REEXAMINATION

No substantial new question of patentability affecting claims 1-38 of US Patent 8,036,988 is raised by the present request for ex parte reexamination and the prior art cited therein for the reasons set forth below.

Issue Not Within Scope of Inter Partes Reexamination

It is noted that an issue not within the scope of reexamination proceedings has been raised. On pages 3, 6, 7 of the request, requester discusses 35 USC 112. These issues will not be considered in a reexamination proceeding. 37 CFR 1.906(c). While this issue is not within the scope of reexamination, the patentee is advised that it may be desirable to consider filing a reissue application provided that the patentee believes one or more claims to be partially or wholly inoperative or invalid.

Prior art cited in the Request

The instant request filed 9/12/2012 indicates that the requester considers that a substantial new question of patentability is raised as to claims 1-38 of US Patent 8,036,988 by the following prior art references:

- "Cohen" [US 6,422,462]
- "Musmanno" [US 5,826,243]
- "Franklin '810" [US 5,883,810]
- "Joao" [US 5,903,830]
- "Yanagihara" [US 2001/0011249]

Prosecution History

10/12/2010: 12/902,399 was filed with claims 1-20.

12/7/2010: Claims 21-22 were added via a preliminary amendment.

1/14/2011: Claims 1-22 were rejected as obvious over Franklin '832 [US 6,000,832] in view of Yanagihara [US 2001/0011249]. Examiner made the following remarks about Franklin '832:

> "(see column 9, lines 52-55; where code specific to a merchant is generated by the software supplied by the issuing bank installed on customer computer as described in column 2, lines 18-37; Examiner notes merchant ID code generated by the computer hides the identity of the merchant)"

Claims 1-22 were also given a Double Patenting rejection over US Patent 7,840,486 and US Patent 6,324,526.

3/21/2011: Applicant argued that:

> "Contrary to the Office's contention, Franklin '832 requires that a particular merchant for a specific transaction to be known and identified to generate the transaction code by entering transaction-specific data into a MAC coding unit for generating a transaction account number that is specific to the identified merchant (column 9, lines 48-64). Whereas, the Applicant's claimed method does not identify a merchant prior to the generation of the transaction code."

Applicant also filed a terminal disclaimer.

4/29/2011: Claims 1-22 were allowed with the following reasons for allowance:

> "With regards to claim 1, the prior art of records, alone or combined, does neither anticipate nor render obvious, inter alia, as a whole, the uniquely patentable feature of :" defining at least one payment category to include at least limiting a number of transactions to one or more merchants, said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants" in a method of performing secure credit card purchase."

7/26/2011: Dependent claims 23-38 were proposed after allowance.

8/18/2011: Dependent claims 23-38 were approved for entry after allowance.

Discussion Regarding Substantial New Questions of Patentability

The presence or absence of "a substantial new question of patentability" determines whether or not reexamination is ordered. If the prior art patents and printed publications raise a

substantial question of patentability of at least one claim of the patent, then a substantial new question of patentability is present, unless the same question of patentability has already been decided by (A) a final holding of invalidity, after all appeals, or (B) by the Office in a previous examination or pending reexamination of the patent. A "previous examination" of the patent is: (A) the original examination of the application which matured into the patent; (B) the examination of the patent in a reissue application that has resulted in a reissue of the patent; or (C) the examination of the patent in an earlier pending or concluded reexamination.

The requested patent, US Patent 8,036,988

US Patent 8,036,988 describes the security problem of a consumer having to transmit his credit card account information to a third-party merchant:

> "Unfortunately, however, even with such encryption techniques, the account information must usually still ultimately be transmitted to a third party who did not previously have access to that information previously" [US Patent 8,036,988, col 2: lines 30-34]

Claim 1 is representative:

1. A method of performing secure credit card purchases, said method comprising:

a) contacting a custodial authorizing entity having custodial responsibility of account parameters of a customer's account that is used to make credit card purchases;

b) supplying said custodial authorizing entity with at least account identification data of said customer's account;

c) defining at least one payment category to include at least limiting a number of transactions to one or more merchants, said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants;

d) designating said payment category;

e) generating a transaction code by a processing computer of said custodial authorizing entity, said transaction code reflecting at least the limits of said designated payment category to make a purchase within said designated payment category;

f) communicating said transaction code to a merchant to consummate a purchase with defined purchase parameters;

g) verifying that said defined purchase parameters are within said designated payment category; and

h) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said designated payment category and to authorize payment required to complete the purchase.

Requester interprets the above-highlighted claim language:

"does not present a meaningful limitations in the claims" [request, page 4].

"[the claimed] transactions are 'limited' to any possible number of merchants [due to the 'one or more merchants' phrase], which is not a limitation at all. Thus, the recited claim limitation becomes non-limiting." [request, page 5].

Requester takes an unreasonable, overly-broad position regarding this claim scope, ignoring the plain meaning of the words. The claim requires a payment category to be defined, such category being used in the latter parts of the claim as a way to authorize the subsequent transaction(s) and confirm the transaction as within the category restriction(s). The particular category restriction set forth is one "limiting a number of transactions to one or more merchants" and this is done "prior to any particular merchant being identified as one of said one or more merchants". This appears to be consistent with the teachings in the specification:

"The payment category may also include a multi-transaction authorization wherein more than one purchase may be made from one or a plurality of different merchants, each of which may or may not be identified by the customer and pre-coded in association with the transaction code…and/or…can **designate that only one merchant, whether designated or not**, can use the transaction code." [US Patent 8,036,988, 8:18-34]

One of ordinary skill would find this to teach transactions to be restricted to a certain quantity of merchants, whereby the identity of merchant(s) could either be pre-identified or the identity of merchant(s) could be unspecified. Looking to the claim language, the words in the claim require a restriction defined as a finite number of merchants with the further requirement that the merchant(s) NOT be identified at the time of defining the category restriction.

Examiner allowed the claim language over Franklin '832 even though it was pointed out by Examiner [by citing to column 2 lines 18-37] that Franklin '832's temporary transaction code was restricted according to "transaction-specific data (e.g., transaction amount, merchant ID, goods ID, time, transaction date, etc.)" [Franklin '832 at 2:29-32].

Cohen

Cohen was not relied upon or described by the Examiner in 12/902,399 which matured into the instant Patent requested for reexamination, US Patent 8,036,988. Cohen was applied as prior art in 90/007,481 (all claims being canceled via reexamination) which was a reexamination of US Patent 6,324,526 which is a related case in the chain of continuity for the instant Patent. However, the claim language at issue in this instant Request was not present in reexamination 90/007,481.

Cohen also seeks to solve the problem of credit card fraud and teaches that restrictions can be associated with one-time use card numbers:

> "These credit cards or credit card numbers are generated for a one time, single transaction basis, after which they are disposed of, or thrown away. The numbers can be used by a user over the Internet or any other communications system, whether open or secure, to effect a single transaction. After a one time use of the credit card number, the number is deactivated by the issuing credit card company such that it is no longer available for use" [Cohen 2:35-43].
>
> "allowed to activate a disposable or customized card for a single or a limited range use" [Cohen 3:47-48].

Requester provides claim construction:

> " 'limiting a number of transactions to one or more merchants' is, in effect, non-limiting due to its recitation of 'one or more merchants.' Taking the broadest reasonable interpretation, the recitation is simply directed towards the defining of at least one payment category." [request, page 25].
>
> "As stated above, the 'one or more merchants' limitation' is in effect a non-limitation. Therefore, this recitation, which includes the 'one or more merchants limitation' in said

payment category prior to identifying any particular merchant, also becomes a non-limitation" [request, page 26].

As described by the examiner previously, Broadest Reasonable Interpretation of the claim language doesn't allow application of prior art that merely restricts a transaction code to any type of transaction category; the restriction must be a limiting to one or more merchants, but prior to the merchant(s) being identified.

Requester points to Cohen's transaction restrictions as a basis for raising a substantial new question of patentability. However the restrictions noted not only are the same types of restrictions found by the Examiner in Franklin '832, they fail to address the claim language identified for patentability.

Requester notes that Cohen's pre-arranged restrictions may include:

"Examples of the customized uses for which a disposable or customized number can be indicated may include a time limit (col. 6, ln. 7), a specified sequence (col. 4, ln. 13), specific merchant or industry (col. 8, ll. 2-14), specific individuals or groups of individuals (col. 8, ll. 15-16), a specific merchant or merchants (col. 8, ll. 33-34), purchase amount (col. 8, ln. 44), geographic area (col. 8, ll. 58-59), security level (col. 10, ln. 5), etc. These various customized uses can also be used in combination, such as a customized number to be used on specific dates, for specific amounts, etc. (col. 10, ll. 24-35)" [request, page 13].

"for use in a particular store itself or a particular chain of stores" [request, page 26].

"only valid for that particular type of charge" [request, page 26].

Cohen's restriction to "specific merchant"(s) and "particular store"(s) would cover the claim language of restricting the transaction to "one or more merchants" as part of the category restriction. However, such a category restriction clearly cannot be defined "prior to any particular merchant being identified" as claim 1 requires. Cohen's "specific merchant"(s) or "particular store"(s) necessarily requires prior specifying of those merchant identities.

Cohen's "type of charge" as argued by requester provides a restriction of the type of purchased item, but does not define a limit on the number of merchants as required by the claims.

Lastly, the "specific merchant"/"particular store" and "type of charge" restrictions of Cohen argued by requester are merely cumulative to Franklin '832's merchant ID and goods ID as addressed in the patent prosecution [by citing to Franklin '832, see 2:29-32].

The other independent claims 17, 19, 21, 22 have similar language to claim 1 and therefore, Cohen fails to raise a substantial new question of patentability for any of claims 1-38.

Musmanno

Requester relies upon Musmanno to address dependent claim features in claims 11, 12 and does not assert where Musmanno would teach the critical features relied upon for patentability and deemed herein as missing from Cohen. Therefore, Musmanno alone or in combination with Cohen fails to raise a substantial new question of patentability for any of claims 1-38.

Franklin '810

Franklin [US 5,883,810] was not relied upon or described by the Examiner in 12/902,399 which matured into the instant Patent requested for reexamination, US Patent 8,036,988. A different Franklin reference [US 6,000,832] was used in art rejections in the prosecution history of US Patent 8,036,988. This "old" Franklin '832 reference shares inventors, assignee and filing date with "new" Franklin '810 reference.

Franklin '810 also seeks to solve the problem of credit card fraud and teaches that restrictions can be associated with temporary use card/transaction numbers:

> "The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number." [Franklin '810, abstract].

Requester provides claim construction:

> "limiting a number of transactions to one or more merchants" is, in effect, non-limiting due to its recitation of "one or more merchants." Taking the broadest reasonable interpretation, the recitation is simply directed towards the defining of at least one payment category" [request, page 53].
>
> "the "one or more merchants limitation" is in effect a non-limitation. Therefore, this recitation, which includes the "one or more merchants limitation" in said payment category prior to identifying any particular merchant, also becomes a non-limitation" [request, page 54].

As described by the examiner previously, Broadest Reasonable Interpretation of the claim language doesn't allow application of prior art that merely restricts a transaction code to any type of transaction category; the restriction must be a limiting to one or more merchants, but prior to the merchant(s) being identified.

Requester points to Franklin '810 transaction restrictions as a basis for raising a substantial new question of patentability. However the restrictions noted not only are the same types of restrictions found by the Examiner in Franklin '832, they fail to address the claim language identified for patentability.

Requester points to features of Franklin '810:

> "Franklin's temporary transaction number can also be linked to extra transaction information to further increase the security. For example, the transaction number might be tied to a specific purchase amount, to a particular merchant 10, or be given an expiration term such that the number becomes invalid after the term expires (col. 2, ll. 48-55)." [request, pages 16-17].
>
> "Franklin discloses the temporary transaction number capable of being "linked to extra transaction information to ensure that the number is used only for one specific transaction" (Franklin, col. 2, 11.48-50). The extra transaction information may include, for instance, a "specific purchase amount," a merchant 10, or a short expiration term on the transaction number (Franklin, col. 2, ll. 50-55). Accordingly, the extra transaction information of Franklin, which may specify a type of transaction (e.g., based on a specific purchase amount), anticipates the payment category" [request, pages 53-54].
>
> "a payment category may be defined (e.g., for a specific purchase amount) without a particular merchant being identified. Accordingly, Franklin anticipates this recitation of claim 1" [request, page 54].

Franklin 810's restriction to "particular merchant" would cover the claim language of restricting the transaction to "one or more merchants" as part of the category restriction. However, such a category restriction clearly cannot be defined "prior to any particular merchant being identified" as claim 1 requires. Franklin 810's "particular merchant" necessarily requires prior specifying of the merchant identity.

Franklin 810's "specific purchase amount" (with no merchant restriction) as a restriction category as argued by requester provides a restriction of the purchase amount, but does not define a limit on the number of merchants as required by the claims.

Lastly, the "particular merchant" and "specific purchase amount" restrictions of Franklin '810 argued by requester are merely cumulative to Franklin '832's "merchant ID" and "transaction amount" as addressed in the patent prosecution [by citing to Franklin '832, see 2:29-32].

The other independent claims 17, 19, 21, 22 have similar language to claim 1 and therefore, Franklin '810 fails to raise a substantial new question of patentability for any of claims 1-38.

Joao

Requester relies upon Joao to address claim features in claims 17, 18 and does not assert where Joao would teach the critical features relied upon for patentability and deemed herein as missing from Franklin '810. Therefore, Joao alone or in combination with Franklin '810 fails to raise a substantial new question of patentability for any of claims 1-38.

Yanagihara

Requester relies upon Yanagihara to address dependent claim features in claims 9-14, 26, 34 and does not assert where Yanagihara would teach the critical features relied upon for

patentability and deemed herein as missing from Franklin '810. Therefore, Yanagihara alone or in combination with Franklin '810 fails to raise a substantial new question of patentability for any of claims 1-38.

Scope of Reexamination

Claims 1-38 will not be reexamined.

Conclusion

Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Additionally, 35 U.S.C. 305 requires that reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.550(a)). Extension of time in ex parte reexamination proceedings are provided for in 37 CFR 1.550(c).

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a), to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the patent requested for reexamination throughout the course of this reexamination proceeding. Likewise, if present, the third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

All correspondence relating to this ex parte reexamination proceeding should be directed:

By Mail to: Mail Stop *Ex Parte* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450

Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at:

https://efs.uspto.gov/efile/myportal/efs-registered

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Any inquiry concerning this communication should be directed to **the Central Reexamination Unit** at telephone number **517-272-7705.**

/Jeffrey D. Carlson/
Primary Examiner, Art Unit 3992

Conferees:

/C. Michelle Tarae/
Primary Examiner, Art Unit 3992

/Fred Ferris/
Acting SPE, Art Unit 3992

Search Notes	Application/Control No.	Applicant(s)/Patent under Reexamination	
	90/012,517	8036988	
	Examiner	Art Unit	
	JEFFREY CARLSON	3992	

SEARCHED			
Class	Subclass	Date	Examiner

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
reviewied of patented file's prosecution historyfile history for	11/29/2012	JDC

Reexamination	**Application/Control No.** 90/012,517	**Applicant(s)/Patent Under Reexamination** 8036988
	Certificate Date	**Certificate Number**

Requester Correspondence Address: ☐ **Patent Owner** ☒ **Third Party**

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

LITIGATION REVIEW ☒	**jdc** (examiner initials)	(date)
Case Name		Director Initials
none found		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	**NUMBER**
1.	
2.	
3.	
4.	

Substitute for form 1449/PTO & 1449B/PTO

FIRST

INFORMATION DISCLOSURE

(use as many sheets as necessary)

Complete if Known

In Re Reexamination Application of:	John D'Agostino
Patent No./Issued:	8,036,988 / October 11, 2011
Reexam Control No.:	
Examiner/Group Art Unit:	
Confirmation No.:	
Attorney Docket No.	0076412-000029

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Document Number-Kind Code	Issue/Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
/jdc/	US-6,422,462	07-23-2002	COHEN	
/jdc/	US-5,883,810	03-16-1999	FRANKLIN et al.	
/jdc/	US-5,903,830	05-11-1999	JOAO et al.	
/jdc/	US-5,826,243	10-20-1998	MUSMANNO et al.	
/jdc/	US-2001/0011249	08-02-2001	YANAGIHARA et al.	
/jdc/	US-6,324,526	11-27-2001	D'AGOSTINO	
/jdc/	US-7,840,486	11-23-2010	D'AGOSTINO	

[1]Enter Office that issued the document, by the two-letter code.

FOREIGN PATENT DOCUMENTS

Examiner Initials	Foreign Patent Document: Country Code[1], Number, Kind Code	Publication Date (MM-DD-YYYY)	Name of Patentee or Applicant of Cited Document	STATUS: Translation	Partial Translation	Eng. Lang. Summary	Search Report	IPER	Abstract	Cited in Spec. / Pg. No(s).	

[1]Enter Office that issued the document, by the two-letter code.

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.

Examiner Signature	/Jeffrey Carlson/	Date Considered	12/03/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with M.P.E.P. § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/012,517	09/12/2012	8036988	0076412-000029	5785

34111 7590 10/10/2012

Maxey Law Offices, PLLC
15500 Roosevelt Blvd.
SUITE 305
CLEARWATER, FL 33760

EXAMINER	
CARLSON, JEFFREY D	
ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
10/10/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

Date:

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. : 90012517
PATENT NO. : 8036988
ART UNIT : 3993

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified ex parte reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the ex parte reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Ex Parte Reexamination Interview Summary – Pilot Program for Waiver of Patent Owner's Statement	**Control No.** 90/012,517	**Patent For Which Reexamination is Requested** 8,036,988
	Examiner ANDRES KASHNIKOW	**Art Unit** 3993

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

All participants (USPTO official and patent owner):

(1) MANUEL SALDANA, CRU (3)

(2) STEPHEN LEWELLYN, REG. NO. 51,942 (4)

Date of Telephonic Interview: 09/26/12.

The USPTO official requested waiver of the patent owner's statement pursuant to the pilot program for waiver of patent owner's statement in *ex parte* reexamination proceedings.*

☐ The patent owner **agreed** to waive its right to file a patent owner's statement under 35 U.S.C. 304 in the event reexamination is ordered for the above-identified patent.

☒ The patent owner **did not agree** to waive its right to file a patent owner's statement under 35 U.S.C. 304 at this time.

The patent owner is not required to file a written statement of this telephone communication under 37 CFR 1.560(b) or otherwise. However, any disagreement as to this interview summary must be brought to the immediate attention of the USPTO, and no later than one month from the mailing date of this interview summary. Extensions of time are governed by 37 CFR 1.550(c).

*For more information regarding this pilot program, see *Pilot Program for Waiver of Patent Owner's Statement in Ex Parte Reexamination Proceedings*, 75 *Fed. Reg.* 47269 (August 5, 2010), available on the USPTO Web site at http://www.uspto.gov/patents/law/notices/2010.jsp.

☐ USPTO personnel were unable to reach the patent owner.

The patent owner may contact the USPTO personnel at the telephone number provided below if the patent owner decides to waive the right to file a patent owner's statement under 35 U.S.C. 304.

/MANUEL SALDANA/ 571-272-7740
Signature and telephone number of the USPTO official who contacted or attempted to contact the patent owner.

cc: Requester (if third party requester)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
90/012,517	09/12/2012	8036988

CONFIRMATION NO. 5785

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

REEXAMINATION REQUEST NOTICE

OC000000056771114

Date Mailed: 09/26/2012

NOTICE OF REEXAMINATION REQUEST FILING DATE

(Third Party Requester)

Requester is hereby notified that the filing date of the request for reexamination is 09/12/2012, the date that the filing requirements of 37 CFR § 1.510 were received.

A decision on the request for reexamination will be mailed within three months from the filing date of the request for reexamination. (See 37 CFR 1.515(a)).

A copy of the Notice is being sent to the person identified by the requester as the patent owner. Further patent owner correspondence will be the latest attorney or agent of record in the patent file. (See 37 CFR 1.33). Any paper filed should include a reference to the present request for reexamination (by Reexamination Control Number).

cc: Patent Owner
34111
Maxey Law Offices, PLLC
15500 Roosevelt Blvd.
SUITE 305
CLEARWATER, FL 33760

/rbell/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
90/012,517	09/12/2012	8036988

CONFIRMATION NO. 5785

REEXAM ASSIGNMENT NOTICE

34111
Maxey Law Offices, PLLC
15500 Roosevelt Blvd.
SUITE 305
CLEARWATER, FL 33760

OC000000056771115

Date Mailed: 09/26/2012

NOTICE OF ASSIGNMENT OF REEXAMINATION REQUEST

The above-identified request for reexamination has been assigned to Art Unit 3993. All future correspondence to the proceeding should be identified by the control number listed above and directed to the assigned Art Unit.

A copy of this Notice is being sent to the latest attorney or agent of record in the patent file or to all owners of record. (See 37 CFR 1.33(c)). If the addressee is not, or does not represent, the current owner, he or she is required to forward all communications regarding this proceeding to the current owner(s). An attorney or agent receiving this communication who does not represent the current owner(s) may wish to seek to withdraw pursuant to 37 CFR 1.36 in order to avoid receiving future communications. If the address of the current owner(s) is unknown, this communication should be returned within the request to withdraw pursuant to Section 1.36.

cc: Third Party Requester(if any)
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

/rbell/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900

REEXAMINATION TITLE REPORT (AKA PATENT ASSIGNMENT ABSTRACT OF TITLE)

TYPE OF REEXAMINATION: XX EX PARTE *INTER PARTES*

REEXAM CONTROL NO.: 90/012,517

SERIAL NUMBER : 12/902,399 FILING DATE 09/12/12

PATENT NUMBER: 8,036,988 ISSUE DATE 10/11/2011

FIRST *THREE* INVENTORS' NAMES: John D'Agostino

ET. AL : Y XX N

CONTINUITY DATA (IF ANY) :

XX_THIS IS (OR) A _XX_CON __DIV __CIP __ A ___ PROVISIONAL APPLICATION: ___ OF SERIAL NUMBER: 09436280 FILED ON: 11/08/99 STATUS: _XX__PATENTED WITH PATENT NUMBER: 6342290 OR ___PENDING, OR ___ ABANDONED (*EXPIRED* FOR PROVISIONALS).

_WHICH IS A _ CON, ___DIV, CIP, ___PROVISIONAL, OR ___OTHER, OF SERIAL NUMBER: FILED ON: STATUS: ___PATENTED, WITH PATENT NUMBER: AND SERIAL NUMBER, FILED: PENDING, OR ABANDONED.

__WHICH IS A __ CON, DIV, CIP A PROVISIONAL APPLICATION ___OTHER OF SERIAL NUMBER: FILED ON: .STATUS: __ PATENTED WITH PATENT NUMBER: OR___PENDING, OR ABANDONED.

_WHICH IS A __ CON, DIV, CIP, ___PROVISIONAL, OR ___OTHER, OF SERIAL NUMBER: FILED ON: STATUS: __ PATENTED, WITH PATENT NUMBER: AND SERIAL NUMBER FILED PENDING, OR ABANDONED.

__WHICH IS A CON, __ DIV, CIP, A PROVISIONAL APPLICATION ___OTHER OF SERIAL NUMBER: FILED ON: STATUS: __ PATENTED WITH PATENT NUMBER: OR___PENDING, OR ABANDONED.

__WHICH IS A CON, DIV, CIP A PROVISIONAL APPLICATION ___OTHER OF SERIAL NUMBER: FILED ON . STATUS: PATENTED WITH PATENT NUMBER: OR___PENDING, OR ABANDONED

__WHICH IS A CON, DIV, CIP A PROVISIONAL APPLICATION ___OTHER OF SERIAL NUMBER: FILED ON . STATUS: PATENTED WITH PATENT NUMBER: OR___PENDING, OR ABANDONED

__WHICH IS A CON, DIV, CIP A PROVISIONAL APPLICATION ___OTHER OF SERIAL NUMBER: FILED ON. STATUS: PATENTED WITH PATENT NUMBER: OR___PENDING, OR ABANDONED (*EXPIRED* FOR PROVISIONALS).

__WHICH IS A CIP OF SERIAL NUMBER FILED ON. STATUS: PATENTED, WITH PATENT NUMBER ABANDONED.

ET. AL.

ASSIGNMENT RECORD DATA

THE ASSIGNMENT RECORDS REVEAL THAT THE TITLE REPORT APPEARS TO BE VESTED IN:

XX INVENTOR(S): Sarasota, FL (US)

___AS ENDORSED:

___AS THE RECORD STANDS, THE PATENT WHEN GRANTED WILL ISSUE IN THE NAME OF THE INVENTOR(S)

___LEGAL REPRESENTATIVE:

___SECURITY ASSIGNMENT/LICENSEE(PLEASE NOTE THAT THE OWNERSHIP OF THE PATENT IS STILL REFLECTED IN THE *ASSIGNOR*. THE *ASSIGNEE* IN THIS CASE CANNOT OWN THE PATENT. (SEE ACCOMPANYING PAGES, IF ANY.)

___WHEN THE ASSIGNMENT IS RECORDED, THE PATENT SHOULD BELONG TO:

___OTHER: REEL NO: FRAME NO.: DATE RECORDED: // COMPANY NAME: CITY AND STATE OR COUNTRY: .

___NOTES/COMMENTS: Please see section 306 of the Manual of Patent Examining Procedure regarding the *Assignment of a Division, Continuation, Substitute, and Continuation-in-Part in Relation to Parent Application.*

EXAMINED UP TO AND INCLUDING THIS CERTIFICATE DATED AND SIGNED: 09/25/12

LEGAL INSTRUMENTS EXMR., OFFICE OF PATENT LEGAL ADMIN., CENTRAL REEXAMINATION UNIT

TO ANY PRINTERS: THE REEXAMINATION TITLE REPORT DOES NOT HAVE TO HAVE THE STREET ADDRESS OF THE OWNER(S). IF THERE IS ANY INQUIRY, PLEASE NOTIFY THE PERSON ABOVE.

Litigation Search Report CRU 3999

Reexam Control No. 90/012,517

TO: ANDRES KASHNIKOW **Location: CRU** **Art Unit: 3993** **Date: 09/23/2012**	**From: MANUEL SALDANA** **Location: CRU 3999** **MDE 5D14** **Phone: (571) 272-7740** **MANUEL.SALDANA@uspto.gov**

Search Notes

Litigation was NOT found for US Patent Number: 8,036,988

1) I performed a KeyCite Search in Westlaw, which retrieves all history on the patent including any litigation.

2) I performed a search on the patent in Lexis CourtLink for any open dockets or closed cases.

3) I performed a search in Lexis in the Federal Courts and Administrative Materials databases for any cases found.

4) I performed a search in Lexis in the IP Journal and Periodicals database for any articles on the patent.

5) I performed a search in Lexis in the news databases for any articles about the patent or any articles about litigation on this patent.

Westlaw.

Date of Printing: Sep 23, 2012

KEYCITE

C US PAT 8036988 SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD TRANSACTIONS, (Oct 11, 2011)

History

Direct History

=> 1 **SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD TRANSACTIONS,** US PAT 8036988 (U.S. PTO Utility Oct 11, 2011)

Prior Art (Coverage Begins 1976)

C 2 ACCESS SECURITY CONTROL, US PAT 4599509 (U.S. PTO Utility 1986)

C 3 ACCESS SECURITY CONTROL, US PAT 4395628 (U.S. PTO Utility 1983)

C 4 ANONYMOUS CREDIT CARD TRANSACTIONS, US PAT 5420926Assignee: AT&T Corp., (U.S. PTO Utility 1995)

C 5 ANTI-FRAUD VERIFICATION SYSTEM USING A DATA CARD, US PAT 5457747Assignee: Drexler Technology Corporation, (U.S. PTO Utility 1995)

C 6 APPARATUS AND METHOD FOR ROUTING ENCRYPTED TRANSACTION CARD IDENTIFYING DATA THROUGH A PUBLIC TELEPHONE NETWORK, US PAT 6598031Assignee: EDI Secure LLLP, (U.S. PTO Utility 2003)

C 7 APPARATUS AND METHODS FOR IMPROVED CREDIT CARDS AND CREDIT CARD TRANSACTIONS, US PAT 6422462 (U.S. PTO Utility 2002)

C 8 APPARATUS AND SYSTEM FOR MANAGING A CARD NUMBER, US PAT 5893907 (U.S. PTO Utility 1999)

C 9 APPARATUS FOR CHECKING THE USER OF A CARD IN CARD-ACTUATED MACHINES, US PAT 4048475Assignee: Omron Tateisi Electronics Company, (U.S. PTO Utility 1977)

C 10 APPARATUS FOR GENERATING ENCRYPTION/DECRYPTION LOOK-UP TABLES USING A SESSION KEY, US PAT 5832087Assignee: Chantilley Corporation Limited, (U.S. PTO Utility 1998)

C 11 APPARATUS FOR KEY DISTRIBUTION IN AN ENCRYPTION SYSTEM, US PAT 5768381Assignee: Chantilley Corporation Limited, (U.S. PTO Utility 1998)

C 12 APPARATUS, SYSTEM AND METHOD FOR CREATING CREDIT VOUCHERS USABLE AT POINT OF PURCHASE STATIONS, US PAT 5010485Assignee: JBH Ventures, (U.S. PTO Utility 1991)

C 13 AUTHENTICATION SYSTEM USING ONE-TIME PASSWORDS, US PAT 5592553Assignee: International Business Machines, (U.S. PTO Utility 1997)

C 14 AUTOMATED BANKING SYSTEM FOR DISPENSING MONEY ORDERS, WIRE TRANSFER AND BILL PAYMENT, US PAT 6012048Assignee: Capital Security Systems, Inc., (U.S. PTO Utility 2000)

C 15 AUTOMATED, CLASSIFIED EXPENDITURE DATA CARD RECORDING SYSTEM, US PAT 5748908 (U.S. PTO Utility 1998)

C 16 AUTOMATED INTERACTIVE CLASSIFIED AD SYSTEM FOR THE INTERNET, US PAT 6253188Assignee: Thomson Newspapers, Inc., (U.S. PTO Utility 2001)

C 17 AUTOMATED PURCHASING CONTROL SYSTEM, US PAT 5621201Assignee: Visa International, (U.S. PTO Utility 1997)

C 18 AUTOMATED PURCHASING CONTROL SYSTEM, US PAT 5500513Assignee: Visa International, (U.S. PTO Utility 1996)

C 19 AUTOMATIC BANKING SYSTEM, US PAT 4423316Assignee: Omron Tateisi Electronics Co., (U.S. PTO Utility 1983)

C 20 BUSINESS-TO-BUSINESS COMMERCE USING FINANCIAL TRANSACTION NUMBERS, US PAT APP 20030018567Assignee: Orbis Patents Ltd., (U.S. PTO Application 2003)

C 21 CARD CHARGING SYSTEMS, US PAT 6375084Assignee: Transmo Limited, (U.S. PTO Utility 2002)

C 22 CARD VALIDATION, METHOD AND SYSTEM, US PAT 4016405Assignee: Diebold, Incorporated, (U.S. PTO Utility 1977)

C 23 CARDLESS PAYMENT SYSTEM, US PAT 6341724Assignee: First USA Bank, NA, (U.S. PTO Utility 2002)

C 24 CARDLESS PAYMENT SYSTEM, US PAT 6227447Assignee: First USA Bank, NA, (U.S. PTO Utility 2001)

C 25 CATEGORIZATION OF PURCHASED ITEMS FOR EACH TRANSACTION BY A SMART CARD, US PAT 5559313Assignee: Lucent Technologies Inc., (U.S. PTO Utility 1996)

H 26 CENTRALIZED CONSUMER CASH VALUE ACCUMULATION SYSTEM FOR MULTIPLE MERCHANTS, US PAT RE36116 (U.S. PTO Reissue 1999)

C 27 CENTRALIZED CONSUMER CASH VALUE ACCUMULATION SYSTEM FOR MULTIPLE MERCHANTS, US PAT 5287268 (U.S. PTO Utility 1994)

C 28 CENTRALIZED CONSUMER CASH VALUE ACCUMULATION SYSTEM FOR MULTIPLE MERCHANTS, US PAT 5202826 (U.S. PTO Utility 1993)

C 29 CENTRALIZED CONSUMER CASH VALUE ACCUMULATION SYSTEM FOR MULTIPLE MERCHANTS, US PAT 4941090 (U.S. PTO Utility 1990)

C 30 CENTRALIZED CONSUMER CASH VALVE ACCUMULATION SYSTEM FOR MULTIPLE MERCHANTS, US PAT 5117355 (U.S. PTO Utility 1992)

C 31 CHARITABLE CONTRIBUTION CENTRALIZATION SYSTEM AND APPARATUS, US PAT 5555497 (U.S. PTO Utility 1996)

C 32 CHILDREN'S CREDIT OR DEBIT CARD SYSTEM, US PAT 5953710 (U.S. PTO Utility 1999)

C 33 CODING FORMULA FOR VERIFYING CHECKS AND CREDIT CARDS, US PAT 5754653 (U.S. PTO Utility 1998)

34 COMPUTERIZED PAYMENT SYSTEM FOR PURCHASING GOODS AND SERVICES ON THE INTERNET, US PAT 5757917Assignee: First Virtual Holdings Incorporated, (U.S. PTO Utility 1998)

35 COMPUTERIZED PURCHASING SYSTEM AND METHOD FOR MEDIATING PURCHASE TRANSACTIONS OVER AN INTERACTIVE NETWORK, US PAT 5878141Assignee: Microsoft Corporation, (U.S. PTO Utility 1999)

36 COMPUTERIZED SYSTEM FOR MAKING PAYMENTS AND AUTHENTICATING TRANSACTIONS OVER THE INTERNET, US PAT 5826241Assignee: First Virtual Holdings Incorporated, (U.S. PTO Utility 1998)

37 COMPUTING AND INDICATING DEVICE, US PAT 4856062 (U.S. PTO Utility 1989)

38 CONSUMER ORIENTED SMART CARD SYSTEM AND AUTHENTICATION TECHNIQUES, US PAT 5193114 (U.S. PTO Utility 1993)

39 CONTEXTUAL DATA REPRESENTATION AND RETRIEVAL METHOD, US PAT 6470490 (U.S. PTO Utility 2002)

40 COUNTERFEIT-PROOF IDENTIFICATION CARD, US PAT 5694471Assignee: V-ONE Corporation, (U.S. PTO Utility 1997)

41 CREDIT CARD-BASED ACCOUNTING SERVICE SYSTEM FOR A NETWORK, US PAT 5583918Assignee: Fujitsu Limited, (U.S. PTO Utility 1996)

42 CREDIT CARD PAGER APPARATUS, US PAT 5192947 (U.S. PTO Utility 1993)

43 CREDIT CARD SPENDING AUTHORIZATION CONTROL SYSTEM, US PAT 5914472Assignee: AT&T Corp, (U.S. PTO Utility 1999)

44 CREDIT CARD SYSTEM AND METHOD, US PAT 6636833Assignee: Obis Patents Ltd., (U.S. PTO Utility 2003)

45 CREDIT CARD SYSTEM AND METHOD, US PAT APP 20030028481Assignee: Orbis Patents, Ltd., (U.S. PTO Application 2003)

46 CREDIT CARD SYSTEM AND METHOD OF ISSUING CREDIT CARD USING SUCH A SYSTEM, US PAT 5883452Assignee: Nippon Shinpan Co., Ltd., (U.S. PTO Utility 1999)

47 CREDIT CARD SYSTEM AND METHOD OF USING CREDIT CARD WITH SUCH CREDIT CARD SYSTEM, US PAT 5777306Assignee: Nippon Shinpan Co., Ltd., (U.S. PTO Utility 1998)

48 CREDIT/CHARGE CARD SYSTEM ENABLING PURCHASERS TO CONTRIBUTE TO SELECTED CHARITIES, US PAT 5466919 (U.S. PTO Utility 1995)

49 CRYPTOGRAPHIC METHOD FOR UPDATING FINANCIAL RECORDS, US PAT 5231666Assignee: International Business Machines, (U.S. PTO Utility 1993)

50 CURRENCY TRANSFER SYSTEM AND METHOD, US PAT 5326960 (U.S. PTO Utility 1994)

51 CURRENCY TRANSFER SYSTEM AND METHOD USING FIXED LIMIT CARDS, US PAT 5350906 (U.S. PTO Utility 1994)

52 DATA PROCESSING METHOD OF CONFIGURING AND MONITORING A SATELLITE SPENDING CARD LINKED TO A HOST CREDIT CARD, US PAT 5864830 (U.S. PTO Utility 1999)

C 53 DIGITAL ACTIVE ADVERTISING, US PAT 6195649Assignee: Open Market, Inc., (U.S. PTO Utility 2001)
C 54 DIGITAL ACTIVE ADVERTISING, US PAT 5724424Assignee: Open Market, Inc., (U.S. PTO Utility 1998)
C 55 DIGITAL MONEY WITH USAGE-CONTROL, US PAT APP 20020152158Assignee: INTERNATIONAL BUSINESS MACHINES, (U.S. PTO Application 2002)
C 56 DIRECT TELEPHONE DIAL ORDERING SERVICE, US PAT 5023904Assignee: Science Dynamics Corporation, (U.S. PTO Utility 1991)
C 57 ELECTRONIC CASHLESS TRANSACTION SYSTEM, US PAT 5428684Assignee: Fujitsu Limited, (U.S. PTO Utility 1995)
C 58 ELECTRONIC COMMERCE USING A SECURE COURIER SYSTEM, US PAT 5671279Assignee: Netscape Communications Corporation, (U.S. PTO Utility 1997)
C 59 ELECTRONIC FUNDS TRANSFER INSTRUMENTS, US PAT 5677955Assignee: Financial Services Technology Consortium; The First National Bank of Boston; Bell Communications Research, Inc., (U.S. PTO Utility 1997)
C 60 ELECTRONIC FUNDS TRANSFER SYSTEM WITH MEANS FOR VERIFYING A PERSONAL IDENTIFICATION NUMBER WITHOUT PRE- ESTABLISHED SECRET KEYS, US PAT 4797920Assignee: MasterCard International, Inc., (U.S. PTO Utility 1989)
C 61 ELECTRONIC MONEY CARD, ELECTRONIC MONEY RECEIVING/PAYING MACHINE, AND ELECTRONIC MONEY CARD EDITING DEVICE., US PAT APP 20010011249 (U.S. PTO Application 2001)
C 62 ELECTRONIC ONLINE COMMERCE CARD WITH CUSTOMER GENERATED TRANSACTION PROXY NUMBER FOR ONLINE TRANSACTIONS, US PAT 6000832Assignee: Microsoft Corporation, (U.S. PTO Utility 1999)
C 63 ELECTRONIC ONLINE COMMERCE CARD WITH TRANSACTIONPROXY NUMBER FOR ONLINE TRANSACTIONS, US PAT 5883810Assignee: Microsoft Corporation, (U.S. PTO Utility 1999)
C 64 ELECTRONIC PAYMENT SYSTEM EMPLOYING LIMITED-USE ACCOUNT NUMBER, US PAT 6339766Assignee: TransactionSecure, (U.S. PTO Utility 2002)
C 65 ENHANCED SECURITY FOR A SECURE TOKEN CODE, US PAT 5485519Assignee: Security Dynamics Technologies, Inc., (U.S. PTO Utility 1996)
C 66 FINANCIAL CARDS, US PAT APP 20030216997 (U.S. PTO Application 2003)
▶ 67 FINANCIAL TRANSACTION SYSTEM, US PAT 5822737 (U.S. PTO Utility 1998)
C 68 FINANCIAL TRANSACTION SYSTEM, US PAT 4988849Assignee: Hitachi, Ltd., (U.S. PTO Utility 1991)
C 69 FRAUD PROTECTION FOR CARD TRANSACTIONS, US PAT 5311594Assignee: AT&T Bell Laboratories, (U.S. PTO Utility 1994)
C 70 IDENTIFICATION VERIFICATION METHOD AND SYSTEM, US PAT 4679236 (U.S. PTO Utility 1987)
C 71 INFORMATION MANAGEMENT, RETRIEVAL AND DISPLAY SYSTEM AND ASSOCIATED METHOD, US PAT 6484166Assignee: Evresearch, Ltd., (U.S. PTO Utility 2002)

C 72 INSTANT CREDIT CARD MARKETING SYSTEM FOR RESERVATIONS FOR FUTURE SERVICES, US PAT 6144948Assignee: Walker Digital, LLC, (U.S. PTO Utility 2000)

C 73 INTEGRATED SYSTEM FOR CONTROLLING MASTER ACCOUNT AND NESTED SUB-ACCOUNT(S), US PAT 5826243Assignee: Merrill Lynch & Co., Inc., (U.S. PTO Utility 1998)

H 74 INTERNET BILLING METHOD, US PAT 5794221 (U.S. PTO Utility 1998)

C 75 MAGNETIC SMARTCARD, US PAT 5434398Assignee: Labenski, Haim, (U.S. PTO Utility 1995)

H 76 METHOD AND APPARATUS FOR ELECTRONIC COMMERCE, US PAT 5903878 (U.S. PTO Utility 1999)

C 77 METHOD AND APPARATUS FOR FUNDS AND CREDIT LINE TRANSFERS, US PAT 6267292Assignee: Walker Digital, LLC, (U.S. PTO Utility 2001)

C 78 METHOD AND APPARATUS FOR IMPROVED SECURITY USING ACCESS CODES, US PAT 5239583 (U.S. PTO Utility 1993)

C 79 METHOD AND APPARATUS FOR MARKING PARTS, US PAT 4269874Assignee: Diffracto Ltd., (U.S. PTO Utility 1981)

C 80 METHOD AND APPARATUS FOR PERSONAL VERIFICATION UTILIZING NONPREDICTABLE CODES AND BIOCHARACTERISTICS, US PAT 4998279 (U.S. PTO Utility 1991)

C 81 METHOD AND APPARATUS FOR POSITIVELY IDENTIFYING AN INDIVIDUAL, US PAT 4720860Assignee: Security Dynamics Technologies, Inc., (U.S. PTO Utility 1988)

C 82 METHOD AND APPARATUS FOR PROVIDING SECURE ACCESS TO A LIMITED ACCESS SYSTEM, US PAT 5163097Assignee: DynamicServe, Ltd., (U.S. PTO Utility 1992)

C 83 METHOD AND APPARATUS FOR RESTRICTING CREDIT CARD COMMUNICATION CALLS, US PAT 4893330Assignee: American Telephone and Telegraph Company,, (U.S. PTO Utility 1990)

C 84 METHOD AND APPARATUS FOR SECURE IDENTIFICATION AND VERIFICATION, US PAT 5097505Assignee: Securities Dynamics Technologies, Inc., (U.S. PTO Utility 1992)

C 85 METHOD AND APPARATUS FOR SECURING CREDIT CARD TRANSACTIONS, US PAT 5317636Assignee: Arris, Inc., (U.S. PTO Utility 1994)

C 86 METHOD AND DEVICE FOR GENERATING A SINGLE-USE FINANCIAL ACCOUNT NUMBER, US PAT 6163771Assignee: Walker Digital, LLC, (U.S. PTO Utility 2000)

C 87 METHOD AND SYSTEM FOR CONDUCTING SECURE PAYMENTS OVER A COMPUTER NETWORK, US PAT APP 20020116341 (U.S. PTO Application 2002)

C 88 METHOD AND SYSTEM FOR GIFT CREDIT CARD, US PAT 5984180 (U.S. PTO Utility 1999)

C 89 METHOD AND SYSTEM FOR MANAGING A DATA OBJECT SO AS TO COMPLY WITH PREDETERMINED CONDITIONS FOR USAGE, US PAT 5845281Assignee: MediaDNA, Inc., (U.S. PTO Utility 1998)

C 90 METHOD AND SYSTEM FOR PROVIDING TEMPORARY CREDIT AUTHORIZATIONS, US PAT 6456984Assignee: Qwest Communications International Inc., (U.S. PTO Utility 2002)

C 91 METHOD AND SYSTEM FOR RETRIEVING RELEVANT DOCUMENTS FROM A DATABASE, US PAT 6370525Assignee: KCSL, Inc., (U.S. PTO Utility 2002)

C 92 METHOD FOR THE BILLING OF TRANSACTIONS OVER THE INTERNET, US PAT 5905736Assignee: AT&T Corp, (U.S. PTO Utility 1999)

C 93 METHOD FOR ENCOURAGING PURCHASE OF EXECUTABLE AND NON-EXECUTABLE SOFTWARE, US PAT 5509070Assignee: SoftLock Services Inc., (U.S. PTO Utility 1996)

C 94 METHOD FOR TRANSFERRING, RECEIVING AND UTILIZING ELECTRONIC GIFT CERTIFICATES, US PAT 6240397 (U.S. PTO Utility 2001)

C 95 METHOD OF CONTROLLING PAYMENT OF DEBTS, US PAT 6298335 (U.S. PTO Utility 2001)

C 96 MOBILE COMMUNICATION METHOD, AND MOBILE TELEPHONE SWITCHING STATION CUSTOMER MANAGEMENT SYSTEM, AND MOBILE UNIT FOR IMPLEMENTING THE SAME, US PAT 6064879Assignee: Fujitsu Limited, (U.S. PTO Utility 2000)

C 97 MULTI-LANGUAGE DOCUMENT SEARCH AND RETRIEVAL SYSTEM, US PAT 6466901Assignee: Apple Computer, Inc., (U.S. PTO Utility 2002)

C 98 MULTIMEDIA ELECTRONIC WALLET WITH GENERIC CARD, US PAT 5748737 (U.S. PTO Utility 1998)

C 99 MULTIPLE COMPANY CREDIT CARD, US PAT 3376661 (U.S. PTO Utility 1968)

H 100 NETWORK SALES SYSTEM, US PAT 5715314Assignee: Open Market, Inc., (U.S. PTO Utility 1998)

C 101 ON-LINE SECURED FINANCIAL TRANSACTION SYSTEM THROUGH ELECTRONIC MEDIA, US PAT 5729594 (U.S. PTO Utility 1998)

C 102 ON-LINE SHOPPING SYSTEM AND THE METHOD OF PAYMENT SETTLEMENT, US PAT 5890137Assignee: Kabushiki Kaisha N.K. Kikaku, (U.S. PTO Utility 1999)

C 103 OPEN NETWORK PAYMENT SYSTEM FOR PROVIDING FOR AUTHENTICATION OF PAYMENT ORDERS BASED ON A CONFIRMATION ELECTRONIC MAIL MESSAGE, US PAT 6049785Assignee: Open Market, Inc., (U.S. PTO Utility 2000)

C 104 PACKAGE ASSEMBLY AND METHOD FOR ACTIVATING PREPAID DEBIT CARDS, US PAT 5777305Assignee: Incomm, (U.S. PTO Utility 1998)

C 105 PAYMENT AND TRANSACTIONS IN ELECTRONIC COMMERCE SYSTEM, US PAT 6029150Assignee: Certco, LLC, (U.S. PTO Utility 2000)

C 106 PERSONAL IDENTIFICATION ENCRYPTOR AND METHOD, US PAT 5363449Assignee: Tandem Computers Incorporated, (U.S. PTO Utility 1994)

C 107 PERSONAL IDENTIFICATION SYSTEMS, US PAT 5606614Assignee: British Telecommunications public limited, (U.S. PTO Utility 1997)

C 108 PERSONAL SECURITY SYSTEM, US PAT 5361062Assignee: Security Dynamics Technologies, Inc., (U.S. PTO Utility 1994)

C 109 PERSONAL UNIVERSAL IDENTITY CARD SYSTEM FOR FAILSAFE INTERACTIVE FINANCIAL TRANSACTIONS, US PAT 4707592 (U.S. PTO Utility 1987)

C 110 PERSONAL VERIFICATION SYSTEM, US PAT 3938091Assignee: Atalla Technovations Company, (U.S. PTO Utility 1976)

C 111 PIN VENDING DISPENSER, US PAT 5868236Assignee: Rademacher, Darrell G., (U.S. PTO Utility 1999)
C 112 PORTABLE PIN CARD, US PAT 5130519Assignee: Bush, George; Ross, Estelle, (U.S. PTO Utility 1992)
C 113 POSITIVE IDENTIFICATION DISPLAY DEVICE AND SCANNER FOR LOW COST COLLECTION AND DISPLAY OF GRAPHIC AND TEXT DATA IN A SECURE MANNER, US PAT 6202055Assignee: Image Data, LLC, (U.S. PTO Utility 2001)
▷ 114 PRE-PAID CARD SYSTEM AND METHOD, US PAT 5721768Assignee: Call Processing, Inc., (U.S. PTO Utility 1998)
C 115 PRE-PAID CARD SYSTEM AND METHOD, US PAT 5577109Assignee: Call Processing, Inc., (U.S. PTO Utility 1996)
C 116 PREPAYMENT METERING SYSTEM, US PAT 4629874Assignee: The De La Rue Company PLC, (U.S. PTO Utility 1986)
C 117 PREPAYMENT WRISTBAND AND COMPUTER DEBIT SYSTEM, US PAT 6352205Assignee: Busch Entertainment Corporation, (U.S. PTO Utility 2002)
C 118 PROGRAMMABLE CREDIT CARD, US PAT 5585787 (U.S. PTO Utility 1996)
C 119 PROGRAMMABLE TRANSACTION CARD, US PAT 5955961 (U.S. PTO Utility 1999)
C 120 PROVIDING VERIFICATION INFORMATION FOR A TRANSACTION, US PAT 5826245 (U.S. PTO Utility 1998)
C 121 PSEUDO-RANDOM SEQUENCE GENERATORS, US PAT 5323338Assignee: Enfranchise Sixty Limited, (U.S. PTO Utility 1994)
C 122 PUBLIC NETWORK MERCHANDISING SYSTEM, US PAT 5825881Assignee: Allsoft Distributing Inc., (U.S. PTO Utility 1998)
C 123 PURCHASE MANAGEMENT SYSTEM AND METHOD, US PAT 6014650 (U.S. PTO Utility 2000)
C 124 RECEPTION MODE CONTROL IN RADIO RECEIVERS FOR RECEIVING BOTH VSB AND QAM DIGITAL TELEVISION SIGNALS, US PAT 5959699Assignee: SamSung Electronics Co., Ltd., (U.S. PTO Utility 1999)
C 125 RECOGNITION APPARATUS AND METHOD FOR SECURITY SYSTEMS, US PAT 5093861Assignee: Cardkey Systems, Inc., (U.S. PTO Utility 1992)
C 126 RESTRICTED PURPOSE, COMMERCIAL, MONETARY REGULATION METHOD, US PAT 4725719Assignee: First City National Bank of Austin, (U.S. PTO Utility 1988)
C 127 RETAIL METHOD OVER A WIDE AREA NETWORK, US PAT 5899980Assignee: Trivnet Ltd., (U.S. PTO Utility 1999)
C 128 SECURE COMMUNICATIONS SYSTEM FOR REMOTELY LOCATED COMPUTERS, US PAT 5196840Assignee: International Business Machines, (U.S. PTO Utility 1993)
C 129 SECURE CREDIT CARD, US PAT 4667087Assignee: Quintana, Max A.; King, Robert E.; Morgan, Bernard L.; Lennon, Alton Y., (U.S. PTO Utility 1987)
C 130 SECURE CREDIT CARD WHICH PREVENTS UNAUTHORIZED TRANSACTIONS, US PAT 5478994 (U.S. PTO Utility 1995)
C 131 SECURE CREDIT/DEBIT CARD AUTHORIZATION, US PAT 5485510Assignee: AT&T

Corp., (U.S. PTO Utility 1996)

C 132 SECURE METHOD FOR COMMUNICATING CREDIT CARD DATA WHEN PLACING AN ORDER ON A NON- SECURE NETWORK, US PAT 5727163Assignee: Amazon.Com, Inc., (U.S. PTO Utility 1998)

C 133 SECURE NETWORKED TRANSACTION SYSTEM, US PAT APP 20020077837 (U.S. PTO Application 2002)

C 134 SECURE SYSTEM FOR ELECTRONIC SELLING, US PAT 5799285 (U.S. PTO Utility 1998)

C 135 SECURED DISPOSABLE DEBIT CARD CALLING SYSTEM AND METHOD, US PAT 5504808 (U.S. PTO Utility 1996)

C 136 SIGNATURE CAPTURING PRINTER AND DATA CARD TERMINAL, US PAT 5479530Assignee: Microbilt Corporation, (U.S. PTO Utility 1995)

C 137 SMART CARD WITH MULTIPLE CHARGE ACCOUNTS AND PRODUCT ITEM TABLES DESIGNATING THE ACCOUNT TO DEBIT, US PAT 5649118Assignee: Lucent Technologies Inc., (U.S. PTO Utility 1997)

C 138 SYSTEM AND METHOD FOR BILLING FOR TRANSACTIONS CONDUCTED OVER THE INTERNET FROM WITHIN AN INTRANET, US PAT 5845267Assignee: AT&T Corp, (U.S. PTO Utility 1998)

C 139 SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES, US PAT 7840486 (U.S. PTO Utility 2010)

C 140 SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES, US PAT APP 20060031161 (U.S. PTO Application 2006)

C 141 SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES, US PAT 6324526 (U.S. PTO Utility 2001)

C 142 SYSTEM AND METHOD FOR PERFORMING SECURE USER ACCOUNT PURCHASES, US PAT APP 20020120587 (U.S. PTO Application 2002)

C 143 SYSTEM AND METHOD FOR PRE-AUTHORIZATION OF INDIVIDUAL ACCOUNT REMOTE TRANSACTIONS, US PAT 6226624 (U.S. PTO Utility 2001)

C 144 SYSTEM AND METHOD FOR PRE-AUTHORIZATION OF INDIVIDUAL ACCOUNT TRANSACTIONS, US PAT 5991750Assignee: GE Capital, (U.S. PTO Utility 1999)

C 145 SYSTEM AND METHOD FOR PROVIDING OPERATOR AND CUSTOMER SERVICES, US PAT 6188761Assignee: MCI Communications Corporation, (U.S. PTO Utility 2001)

C 146 SYSTEM AND METHOD FOR PSEUDO CASH TRANSACTIONS, US PAT 5913203Assignee: Jaesent Inc., (U.S. PTO Utility 1999)

C 147 SYSTEM AND METHOD FOR REAL-TIME BUNDLED TELECOMMUNICATIONS ACCOUNT PROCESSING AND BILLING, US PAT 6885857Assignee: Verisign, Inc., (U.S. PTO Utility 2005)

C 148 SYSTEM AND METHODS TO SELECT AUTHORIZED VENDORS FOR PREPAID DEBIT CARD/CREDIT CARD, US PAT APP 20100012720 (U.S. PTO Application 2010)

C 149 SYSTEM AND PROCESS FOR ISSUING AND MANAGING FORCED REDEMPTION VOUCHERS HAVING ALIAS ACCOUNT NUMBERS, US PAT 6330544Assignee: Walker Digital, LLC, (U.S. PTO Utility 2001)

C 150 SYSTEM FOR PREVENTING FRAUDULENT USE OF CREDIT CARD, US PAT 5163098 (U.S. PTO Utility 1992)

C 151 SYSTEM FOR SECURED CREDIT CARD TRANSACTIONS ON THE INTERNET, US PAT 5956699Assignee: Jaesent Inc., (U.S. PTO Utility 1999)

C 152 SYSTEM FOR VERIFYING THE USER OF A CARD, US PAT 4023012Assignee: Omron Tateisi Electronics Co., (U.S. PTO Utility 1977)

C 153 SYSTEM INTEGRATING CREDIT CARD TRANSACTIONS INTO A FINANCIAL MANAGEMENT SYSTEM, US PAT 6343279Assignee: American Management Systems, Inc., (U.S. PTO Utility 2002)

C 154 SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR NETWORK ELECTRONIC AUTHORIZATION UTILIZING AN AUTHORIZATION INSTRUMENT, US PAT 5815657Assignee: VeriFone, Inc., (U.S. PTO Utility 1998)

C 155 SYSTEMS FOR FINANCIAL AND ELECTRONIC COMMERCE, US PAT APP 20030097331 (U.S. PTO Application 2003)

C 156 TAMPER RESISTANT SMART CARD AND METHOD OF PROTECTING DATA IN A SMART CARD, US PAT 6068192Assignee: Micron Technology, Inc., (U.S. PTO Utility 2000)

C 157 TELEPHONE DEBIT CARD DISPENSER AND METHOD, US PAT 5696908Assignee: Southeast Phonecard, Inc., (U.S. PTO Utility 1997)

C 158 TOKENLESS BIOMETRIC ATM ACCESS SYSTEM, US PAT 6154879Assignee: SmartTouch, Inc., (U.S. PTO Utility 2000)

C 159 TRANSACTION AUTHENTICATION USING A CENTRALLY GENERATED TRANSACTION IDENTIFIER, US PAT 5343529 (U.S. PTO Utility 1994)

C 160 TRANSACTION DEVICE, EQUIPMENT AND METHOD FOR PROTECTING ACCOUNT NUMBERS AND THEIR ASSOCIATED PERSONAL IDENTIFICATION NUMBERS, US PAT 5627355 (U.S. PTO Utility 1997)

C 161 TRANSACTION SECURITY APPARATUS AND METHOD, US PAT 5903830 (U.S. PTO Utility 1999)

C 162 TRANSACTION SECURITY SYSTEM USING TIME VARIANT PARAMETER, US PAT 4747050Assignee: International Business Machines, (U.S. PTO Utility 1988)

C 163 UNIVERSAL ELECTRONIC TRANSACTION CARD INCLUDING RECEIPT STORAGE AND SYSTEM AND METHODS OF CONDUCTING ELECTRONIC TRANSACTIONS, US PAT 5590038 (U.S. PTO Utility 1996)

C 164 USER-SPECIFIED CREDIT CARD SYSTEM, US PAT 6029890 (U.S. PTO Utility 2000)

C 165 VIRTUAL CALLING CARD SYSTEM, US PAT 5479494Assignee: AT&T Corp., (U.S. PTO Utility 1995)

C 166 WIRELESS TELEPHONY FOR COLLECTING TOLLS, CONDUCTING FINANCIAL TRANSACTIONS, AND AUTHORIZING OTHER ACTIVITIES, US PAT 5991749 (U.S. PTO Utility 1999)

LexisNexis® CourtLink®

Patent Search 8036988 9/23/2012

No cases found.

Return to Search

(Charges for search still apply)

902399 (12) 8036988 October 11, 2011

UNITED STATES PATENT AND TRADEMARK OFFICE GRANTED PATENT

8036988

Get Drawing Sheet 1 of 2
Access PDF of Official Patent *
Order Patent File History / Wrapper from REEDFAX®
Link to Claims Section

October 11, 2011

System and method for performing secure credit card transactions

INVENTOR: D'Agostino, John - Sarasota, Florida, United States of America (US), United States of America ()

APPL-NO: 902399 (12)

FILED-DATE: October 12, 2010

GRANTED-DATE: October 11, 2011

CORE TERMS: customer, credit card, merchant, entity, custodial, remote, commercial transaction, identification, authorization, computer, verification, unauthorized, designated, prime, telephone, dollar amount, solicitation, promotional, performing, encryption, utilizing, consumer's, verified, debit, accomplishing, transmitted, consummate, internet, interval, card

ENGLISH-ABST:

A method and system of performing secure credit card purchases in the context of a remote commercial transaction, such as over the telephone, wherein only the customer, once generally deciding upon a product or service to be purchased, communicates with a custodial authorizing entity, such as a credit card company or issuing bank wherein such entity has previous knowledge of the credit card number as well as custodial control of other account parameters such as interest rate, payment history, available credit limit etc. The customer supplies the custodial authorizing entity with the account identification data such as the credit card number and a requested one of a possible plurality of predetermined payment categories which define the dollar amount for the purchase and specific, predetermined time parameters within which authorization by the custodial authorizing entity will remain in effect. The custodial authorizing entity then generates a transaction code which is communicated exclusively to the customer

wherein the customer in turn communicates only the transaction code to the merchant instead of a credit card number. The transaction code is indicative of merchant identification, credit card account identification and a designated one of the plurality of predetermined payment categories.

Source: **Legal > / . . . / > Utility, Design and Plant Patents**
Terms: **patno=8036988** (Suggest Terms for My Search)
View: KWIC
Date/Time: Sunday, September 23, 2012 - 9:42 AM EDT

In

No Documents Found

No documents were found for your search terms
"8036988 or 8,036,988"

Click "Save this search as an Alert" to schedule your search to run in the future.

- OR -
Click "Search Using Natural Language" to run your search as Natural Language search.

- OR -

Click "Edit Search" to return to the search form and modify your search.

Suggestions:

- Check for spelling errors.
- Remove some search terms.
- Use more common search terms, such as those listed in "Suggested Words and Concepts."
- Use a less restrictive date range.
- Use "OR" in between terms to search for one term or the other.

| **Save this Search as an Alert** || **Search Using Natural Language** || **Edit Search** |

In

No Documents Found

No documents were found for your search terms
"8036988 or 8,036,988"

Click "Save this search as an Alert" to schedule your search to run in the future.

- OR -
Click "Search Using Natural Language" to run your search as Natural Language search.

- OR -

Click "Edit Search" to return to the search form and modify your search.

Suggestions:

- Check for spelling errors.
- Remove some search terms.
- Use more common search terms, such as those listed in "Suggested Words and Concepts."
- Use a less restrictive date range.
- Use "OR" in between terms to search for one term or the other.

| **Save this Search as an Alert** || **Search Using Natural Language** || **Edit Search** |

In

Source: **Legal > / . . . / > News, All (English, Full Text)** i
Terms: **8036988 or 8,036,988** (Suggest Terms for My Search)

Select for FOCUS™ or Delivery

1. US Patent Issued on Oct. 11 for "System and Method for Performing Secure Credit Card Transactions" (Florida Inventor), US Fed News, October 17, 2011 Monday 9:36 AM EST, , 333 words, ALEXANDRIA, Va.

2. U.S. Patents Awarded to Inventors in Florida (Oct. 12), Targeted News Service, October 12, 2011 Wednesday 2:03 PM EST, , 1982 words, Targeted News Service Targeted News Service, Alexandria, VA.

3. Florida Inventor Develops Patent for System and Method for Performing Secure Credit Card Transactions, Targeted News Service, October 12, 2011 Wednesday 3:22 AM EST, , 348 words, Targeted News Service, Alexandria, Va.

Source: **Legal > / . . . / > News, All (English, Full Text)** i
Terms: **8036988 or 8,036,988** (Suggest Terms for My Search)
View: Cite
Date/Time: Sunday, September 23, 2012 - 9:43 AM EDT

Substitute for form 1449/PTO & 1449B/PTO

Complete if Known

FIRST

INFORMATION DISCLOSURE

(use as many sheets as necessary)

In Re Reexamination Application of:	John D'Agostino
Patent No./Issued:	8,036,988 / October 11, 2011
Reexam Control No.:	
Examiner/Group Art Unit:	
Confirmation No.:	
Attorney Docket No.	0076412-000029

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Document Number-Kind Code	Issue/Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	US-6,422,462	07-23-2002	COHEN	
	US-5,883,810	03-16-1999	FRANKLIN et al.	
	US-5,903,830	05-11-1999	JOAO et al.	
	US-5,826,243	10-20-1998	MUSMANNO et al.	
	US-2001/0011249	08-02-2001	YANAGIHARA et al.	
	US-6,324,526	11-27-2001	D'AGOSTINO	
	US-7,840,486	11-23-2010	D'AGOSTINO	

[1]Enter Office that issued the document, by the two-letter code.

FOREIGN PATENT DOCUMENTS

Examiner Initials	Foreign Patent Document: Country Code[1], Number, Kind Code	Publication Date (MM-DD-YYYY)	Name of Patentee or Applicant of Cited Document	STATUS: Translation	Partial Translation	Eng. Lang. Summary	Search Report	IPER	Abstract	Cited in Spec. / Pg. No(s).	

[1]Enter Office that issued the document, by the two-letter code.

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with M.P.E.P. § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

US006324526B1

(12) **United States Patent**
D'Agostino

(10) **Patent No.: US 6,324,526 B1**
(45) **Date of Patent: Nov. 27, 2001**

(54) **SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES**

(76) Inventor: **John D'Agostino**, 5120 NE. 27th Ter., Lighthouse Point, FL (US) 33064

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/231,745**

(22) Filed: **Jan. 15, 1999**

(51) **Int. Cl.**[7] **G06F 17/60**
(52) **U.S. Cl.** **705/44**; 235/375; 380/23
(58) **Field of Search** 705/14, 1, 39, 705/41, 44; 380/23, 25; 235/380, 375

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,671,279	9/1997	Elgamal .
5,715,314	2/1998	Payne et al. .
5,727,163	3/1998	Bezos .
5,729,594	3/1998	Klingman .
5,794,221	8/1998	Egendorf .
5,815,657	9/1998	Williams et al. .
5,822,737	10/1998	Ogram .

OTHER PUBLICATIONS

Matt Barthel, Debit–Card point of Sale Terminals, Sep. 28, 1993, American Banker, pp. 1–2.*
Bob Woods, New Dell E–commerce Guarantee Called "Weak", Aug. 1998, Newbytes News pp. 1–2.*
Anne Finnigan, The safe way to shop online, Good Housekeeping, Sep. 1998, pp. 1–2.*
Paul Demery, Attacking the smart card fortress, Credit Card Management, Sep. 1998, pp. 1–4.*
Larry Chase, Taking transactions online, Target Marketing, Oct. 1998, 1–4.*

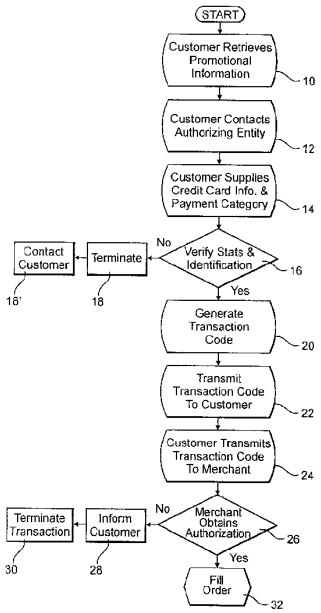
* cited by examiner

Primary Examiner—Eric W. Stamber
Assistant Examiner—Mussie Tesfamariam
(74) *Attorney, Agent, or Firm*—Malloy & Malloy, P.A.

(57) **ABSTRACT**

A method and system of performing secure credit card purchases in the context of a remote commercial transaction, such as over the telephone, wherein only the customer, once generally deciding upon a product or service to be purchased, communicates with a custodial authorizing entity, such as a credit card company or issuing bank wherein such entity has previous knowledge of the credit card number as well as custodial control of other account parameters such as interest rate, payment history, available credit limit etc. The customer supplies the custodial authorizing entity with the account identification data such as the credit card number and a requested one of a possible plurality of predetermined payment categories which define the dollar amount for the purchase and specific, predetermined time parameters within which authorization by the custodial authorizing entity will remain in effect. The custodial authorizing entity then generates a transaction code which is communicated exclusively to the customer wherein the customer in turn communicates only the transaction code to the merchant instead of a credit card number. The transaction code is indicative of merchant identification, credit card account identification and a designated one of the plurality of predetermined payment categories.

16 Claims, 2 Drawing Sheets



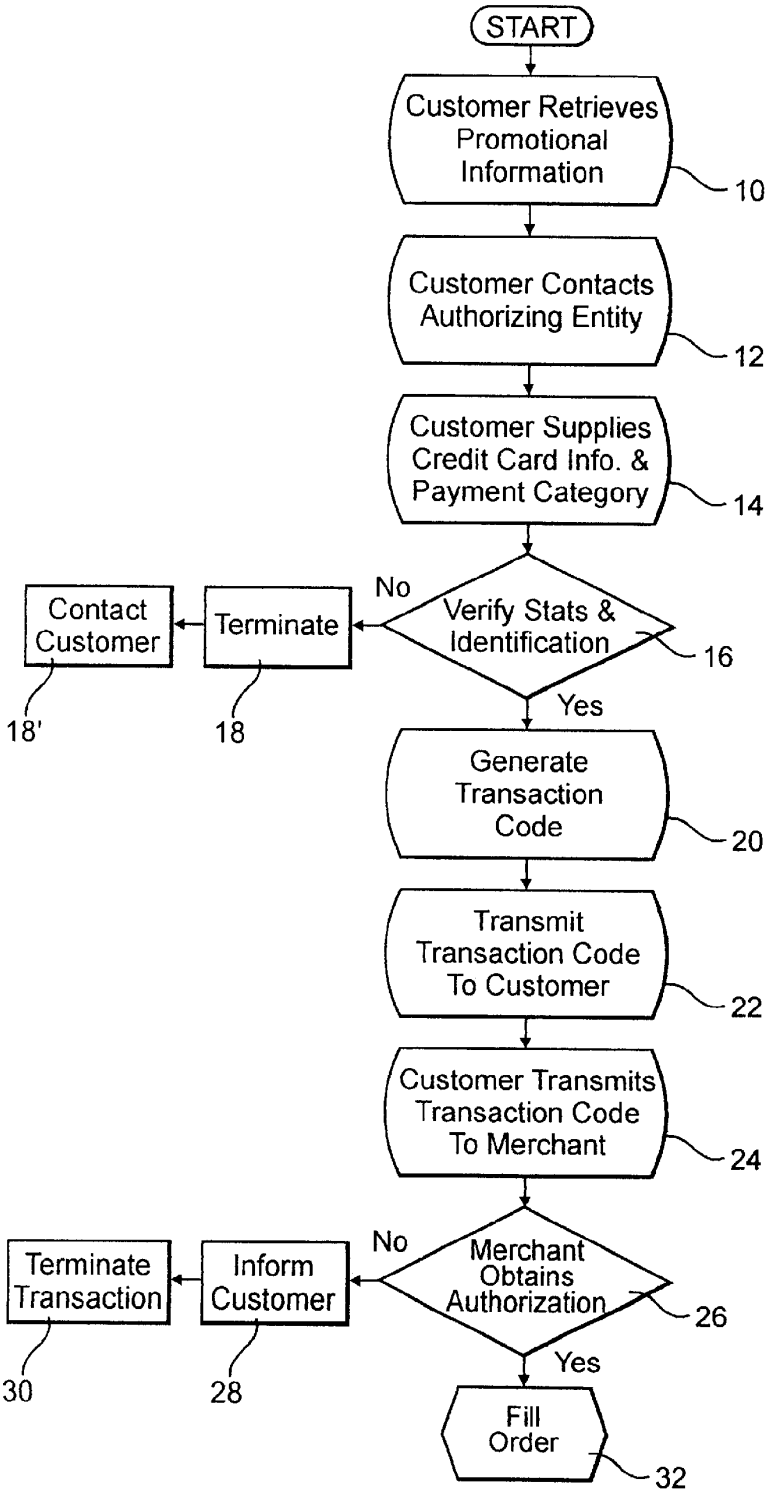

START
Customer Retrieves Promotional Information
10
Customer Contacts Authorizing Entity
12
Customer Supplies Credit Card Info. & Payment Category
14
Verify Stats & Identification
16
No
Terminate
18
Contact Customer
18'
Yes
Generate Transaction Code
20
Transmit Transaction Code To Customer
22
Customer Transmits Transaction Code To Merchant
24
Merchant Obtains Authorization
26
No
Inform Customer
28
Terminate Transaction
30
Yes
Fill Order
32

FIG. 1

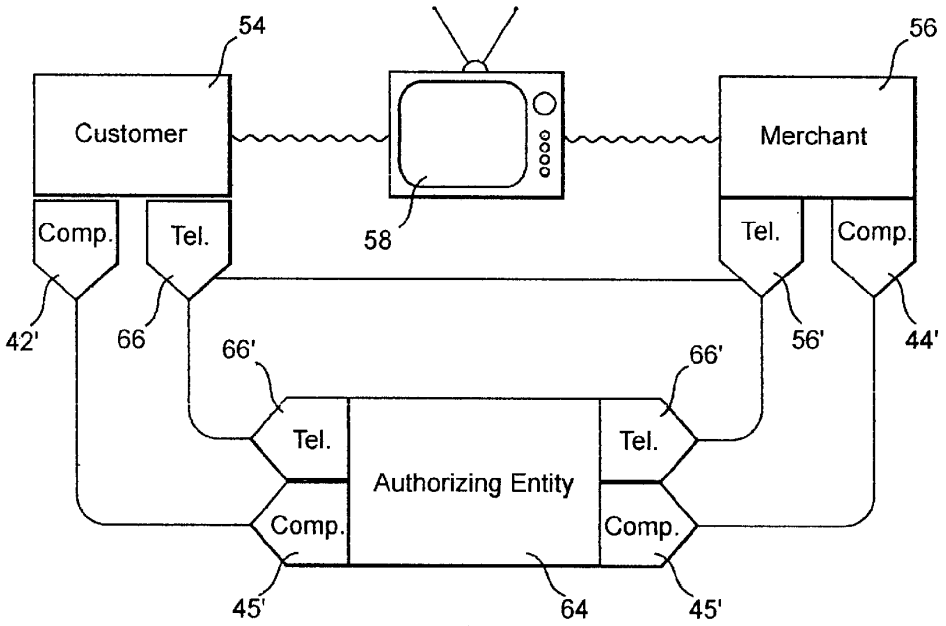

54
56
Customer
Merchant
58
Comp.
Tel.
Tel.
Comp.
42'
66
66'
66'
56'
44'
Tel.
Tel.
Authorizing Entity
Comp.
Comp.
45'
64
45'

FIG. 2

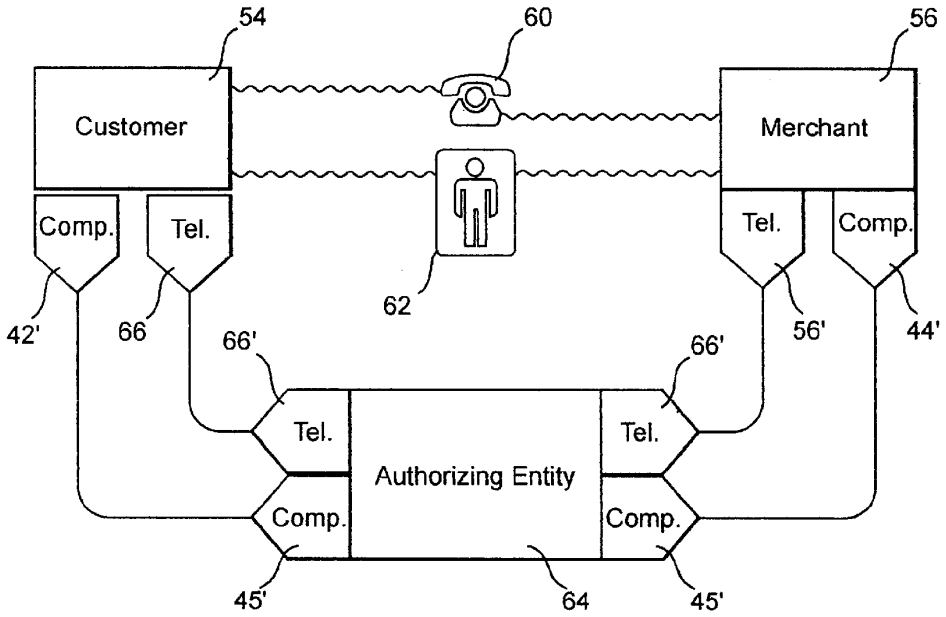

54
60
56
Customer
Merchant
Comp.
Tel.
Tel.
Comp.
62
42'
66
66'
66'
56'
44'
Tel.
Tel.
Authorizing Entity
Comp.
Comp.
45'
64
45'

FIG. 3

SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to a system and method of performing secure credit card purchases in connection with remote commercial transactions, wherein a credit card holder does not have to reveal their credit card number to a merchant or a mechanism controlled by the merchant in order to accomplish a purchase, and wherein the merchant is still assured of the necessary credit verifications and approvals prior to authorizing and/or completing a credit card transaction, thereby increasing overall security by minimizing any access to credit card numbers without having to substantially modify or deviate from existing, accepted credit card transaction practices.

2. Description of the Related Art

The utilization of credit and debit cards to conduct transactions is ever increasing. This is especially the case with remote or "mail-order" transactions wherein merchants desire to be assured of a payment prior to shipping a product. For example, recent years have seen a substantial increase in the popularity of televised shopping networks to further supplement the popularity of catalogue type sales. Moreover, the increasing use and popularity of distributed computer networks such as the internet has also contributed to the dramatic increase in the number of remote commercial transactions conducted every day.

One primary reason associated with the rapid growth of remote commercial transactions is the ability of a merchant to reach an almost limitless number of potential customers at a substantially insignificant cost and with little or no operating overhead since an actual store is not required. Additionally, such sales techniques permit customers to view the products and services in a greatly expanded marketplace, representing a great number of vendors, without extensive travel and without foregoing the privacy and convenience of their home or other predetermined computer site in some cases. Simply put, a telephone or like communication avenue is all that is needed to place the consumer in contact with the merchant and complete the transaction.

The vast increase in popularity of remote commercial transactions conducted over the telephone or internet is further facilitated by the relatively simple protocols and procedures necessary to conduct such transactions. In particular, in order to complete a valid transaction, a merchant need not physically see the customer or the credit card, but must merely accept and enter a customer's credit card account number and an expiration date thereof to obtain authorization. This same convenience, however, is the primary disadvantage and/or problem associated with conducting commerce in the manners set forth above. Specifically, there is a great reluctance on the part of the customer to transmit the credit card account information, including the credit card number, because of the proliferation of fraud, and a well recognized lack of security directed to the protection of such account information. Indeed, it has been established that security and privacy concerns are realistic due to the fact that credit card account data is easily readable or interceptable by unauthorized parties, and can be readily used for all types of remote transactions with minimal risk of being physically caught. In fact, unscrupulous individuals have many ways of gaining access to a consumer's legitimate remote transactions and thereby obtaining the credit card information. This information can be obtained from old

credit card receipts or even from the unauthorized notation and use of the information by merchants or their employees after a legitimate transaction is made. Naturally, the latter is the most difficult to prevent utilizing known methods and systems unless a consumer is willing to completely forego the use of a credit card for purchases.

In the case of computerized remote transactions, as messages, including account data or other confidential information, move across the internet, they can easily pass through numerous computers, any one of which can be utilized to copy such confidential information or data, thereby leading to a further risk of potential fraud when conducting such transactions. Presently, some companies currently seek to address such security and privacy concerns by the employment of encryption programs and techniques. To this end there is an extensive facility associated with both public and private encryption schemes being deployed in order to guard the private or secured information being transmitted across the internet or like world wide networks. Unfortunately, however, even with such encryption techniques, the account information must usually still ultimately be transmitted to a third party who did not previously have access to that information previously. Even some more sophisticated systems which seek to interpose a separate computer or encryption entity between the consumer and the merchant so as to obtain authorization and forward it to the merchant, that information must still be made available to and/or transmitted to that third party, thereby leaving open an avenue for fraud or theft. Further, such encryption techniques, even if minimally effective for computerized remote transactions, are not truly useable for other conventional types of remote transactions, or even normal in person transactions.

Based on the above, there is an obvious need in the field of art associated with remote commercial transactions for a system and method of performing secure credit card purchases of goods and services which truly reduces the risk of potential fraud and theft by eliminating outside access to a consumer's private credit card information without requiring complex encryption equipment or significantly altering the ease and convenience of current transaction techniques. Further, such a system and method should also be effective for use in conventional, "in person" transactions as well, thereby providing an added measure of security and minimizing the hazards associated with the passing on of account information by unscrupulous merchants. Also, such a system should provide limits to potential loss or liability in a manner which does not impede the transaction.

SUMMARY OF THE INVENTION

The present invention is directed towards a system and method of performing secure credit card purchases, wherein payment for goods or services purchased is efficiently accomplished while eliminating the necessity of disclosure or dissemination of a consumers specific credit card number or other account data which the customer or other individual may wish to maintain in confidence. The system and method of the present invention incorporates the advantage of consummating the purchase by the customer through the selection of any one of a plurality of predetermined payment categories. Collectively, the payment categories represent a variety of methods for accomplishing payment for a fixed transaction, a multiple transaction and/or a repeating transaction.

One embodiment of the system and method of the present invention comprises a customer receiving information,

including specific data necessary for the purchase of any given product or service. This promotional information generated by the merchant can be received by any of a plurality of conventional means including advertisements, catalogues, computer network connections, direct person to person customer and merchant contact, telephone solicitation, mail orders, television sales, etc. Once the customer has identified the product or services which he/she wishes to purchase, the customer contacts and supplies a custodial authorizing entity with the requisite information concerning both the identification of a specific credit card or debit card account and a requested payment category. Additionally, security against unauthorized use of confidential account data may also preferably include information relating to the merchant's identification and/or location.

The custodial authorizing entity is preferably defined as the entity which has or has been assigned the custodial responsibility for the financial account data of a customer's credit card account, including a previous knowledge of the credit card number and other information such as credit limits, payment history, available credit amounts and other information which will determine the status of a given credit card account in terms of authorizing a requested payment for a current purchase.

As part of the security system for accomplishing a commercial transaction utilizing credit card or debit card payment, the custodial authorizing entity includes sufficient facilities, preferably including a processing computer or like applicable hardware for the generation of an exclusive transaction code. The transaction code is to be used in substitution for the credit card number and when utilized as authorized, will issue the merchant a credit approval, and will accomplish payment for the goods or services desired in the normal fashion normally associated with a credit or debit card transaction, without the publication or dissemination of an identifying credit card number for a specific customer's account to any entity that is not already aware of that information.

Further, a feature of the transaction code is its ability to indicate any one of preferably a plurality of predetermined payment categories which may be either requested by the customer or automatically chosen by the custodial authorizing entity based on the type of account or the type of purchase or other commercial transaction involved. Each of the payment categories are reflective of a different type of payment desired or required to consummate the intended purchase. More specifically, the plurality of payment categories may include a single transaction involving a specific dollar amount for a purchase within a specific time period, such as twenty four hours, during which authorization of the purchase remains valid. Alternately, a single transaction may be involved wherein a maximum limit or a dollar amount is determined above which the purchase will become invalidated and further wherein a fixed period of time is preferably established for maintaining authorization of such purchase. Other alternatives would involve one or more of the categories coded to define multiple transactions involving a maximum dollar amount for purchases, as well as a fixed period of time for authorization of such purchases, and/or a repeating transaction wherein payments may be automatically accessed by a merchant over a predetermined or unspecified time interval (such as every thirty days) for a specific dollar amount or a maximum dollar amount limit. Also, limits solely as to a specific merchant or a given time period can be effectively established for which the transaction code is valid.

A further feature of the present invention to be described in greater details hereinafter, is the requirement that the transaction code, once received by the customer is transmitted to the merchant by the customer or a person specifically authorized by the customer. Only minimal contact by the merchant and the custodial authorizing entity is provided for purposes of the merchant verifying the validity of the transaction code utilizing a conventional process electronically or otherwise similar to the verification of a credit card number normally offered to a merchant for the purchase of goods or services. There is, therefore, no disclosure, publication or other dissemination of the specific credit card number of a given customer account beyond those entities who already know the information, and the transaction code is transmitted exclusively to the customer by the custodial authorizing entity who has the ability to better identify whether the customer is properly authorized to use the account. Moreover, the transaction code, once given out by the customer, only has a limited usefulness, thereby limiting the risk of misuse and minimizing the potential losses to be experienced by the credit card company and/or the account holder.

Accordingly, it is an object of the present invention to provide a system and attendant method for performing remote commercial transactions utilizing credit cards, which maximizes the security of the transaction and limits the potential liability to be experienced from a fraudulent transaction.

Yet another object of the present invention is to provide a secure system and method for establishing credit card purchases which eliminate the disclosure or dissemination of the actual credit card number to anyone other than a custodial authorizing entity which normally has custodial responsibilities for account information including the previously established credit card number.

It is another object of the present invention to provide a system and method of establishing secure credit card purchases through the generation of a transaction code which renders it extremely difficult or impossible to access or infiltrate a customer's credit card account by unauthorized means.

It is yet another object of the present invention to provide a secure method of completing a remote commercial transaction which eliminates the need to convey actual account information to a merchant, but which allows the merchant to conduct a normal verification of information needed to consummate a given purchase.

It is also an object of the present invention to provide a system and attendant method of accomplishing secure credit card purchases which eliminates the need to disclose or disseminate a given credit card number while providing the customer with the versatility of choosing any one of a plurality of predetermined payment categories.

It is yet another feature of the present invention to provide a system and method of accomplishing secure credit card payments having the versatility of allowing the customer to select any one of a plurality of payment categories which are indicative of a variance in the amount of a purchase as well as the time in which authorization for such payment is valid.

These and other objects, features and advantages of the present invention will become more clear when the drawings as well as the detailed description are taken into consideration.

BRIEF DESCRIPTION OF THE DRAWINGS

For a fuller understanding of the nature of the present invention, reference should be had to the following detailed description taken in connection with the accompanying drawings in which:

FIG. **1** is a schematic representation of a flow chart showing various steps involved in the performance of the system and method of the present invention for the secure credit card purchasing;

FIG. **2** is a schematic representation similar to that of FIG. **1** wherein customer to merchant contact is accomplished by conventional facilities such as television; and

FIG. **3** is a schematic representation similar that of FIG. **2** wherein customer to merchant contact is established either by phone or in person.

Like reference numerals refer to like parts throughout the several views of the drawings.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

As shown in the accompanying Figures, the present invention is directed towards a system and method for accomplishing secure credit card purchases. Moreover, these purchases can be "in person", but preferably include remote commercial transactions such as mail order, purchases over the internet, television solicitations, telephone solicitations, etc. Security is establish by virtue of the elimination of the need to disclose an active credit card number and expiration date to the merchant or any other party other than the original credit card company, issuing bank or like financial institution which already has custodial responsibilities for the financial or account data associated with a given customer's credit card account.

More specifically and with reference to FIG. **1** the system as well as an attendant method is preferably instigated by the customer viewing a product, identifying a desired amount for a transaction and/or receiving promotional information as at **10**, either in person or by any of the electronic or more conventional techniques which will be described in greater detail with reference to FIGS. **2** through **3**. Once the customer reviews the product or promotional information and has sufficient information, such as including price, product or service identification, payment requirement, etc., regarding the remote commercial transaction to be conducted, the customer contacts, either by computer, telephone or in person, a custodial authorizing entity as at **12**. The custodial authorizing entity may herein be defined as comprising that entity or institution which has or has been designated by the entity which has custodial responsibility for the financial data and security of a given credit card account of a customer. As set forth above such custodial authorizing entity can be represented by the credit card company issuing a credit card to a given customer or alternately can be represented by a bank or other financial institution serving to sponsor a credit card or debit card to the extent of processing the debits and credit associated therewith. The authorizing entity's custodial responsibilities of course includes the previous knowledge and/or storage of the credit card number serving to identify a specific customer's credit card account. Once contacted, the customer then supplies appropriate identification data to inform the custodial authorizing entity of a specific customer's credit card account as at **14**. In addition, the customer will supply the custodial authorizing entity with additional required information needed to consummate the purchase as well as ensure the security of the account in order to prevent its unauthorized use. Such additional information may preferably include the identification of the merchant or merchants involved, when such information is deemed necessary, and a requested one of a plurality of predetermined payment categories to facilitate consummation of the purchase of the products or services desired. Such predetermined plurality of payment categories will be discussed in greater detail hereinafter.

Once the appropriate information has been received from the customer as indicated at **16**, the custodial authorizing entity verifies the credit card status and account identification of the customer to determine the viability of the account in terms of dollar amount limits, payment history, available credit balance, etc. If the accessed credit card account is not in good standing, the custodial authorizing entity will permanently or temporarily terminate the transaction as at **18** and/or communicate to the customer directly as at **18'** by any applicable means for purposes of informing the customer of the unacceptable status of the accessed credit card account. If the credit card account is in good standing, based at least in part on the requested payment category, (amount of payment), the custodial authorizing entity generates a transaction code as at **20**. The transaction code is used in substitution for the specific credit card number which would normally identify a customer's credit card account and would allow access thereto by any entity having possession of the credit card number whether or not such possession was authorized or unauthorized. More specifically, the transaction code is pre-coded to be indicative of a specific credit card account, preferably a merchant or merchants identification and a designated payment category, selected from the plurality of predetermined payment categories as set forth above. Once generated, the transaction code is communicated exclusively to the authorized and verified customer by the custodial authorizing entity as at **22**, wherein the system and method of the present invention preferably restricts communication between the custodial authorizing entity and the merchant except to conduct a normal verification as will be explained.

The verified customer thereafter and preferably within a time limit to be determined by the customer and pre-coded in association with the transaction code, will directly or through an authorized representative communicate the transaction code to the merchant as at **24**. The system and method of the preferred embodiment of the present invention contemplates that only the verified customer will transmit the generated transaction code to the merchant in the case of a remote commercial transaction, thereby limiting knowledge of the transaction code to those parties having a need to know. Of course, however, as the transaction code will generally have a limited value as defined by the verified customer when obtained, the verified customer may designate an agent or other entity to act as the customer on his/her behalf, with the amount of potential liability to be experienced by such a transaction to be limited to the amount defined by the verified customer when obtaining the transaction code.

At this point the purchase is consummated at least from the customer standpoint in that the customer has previously established the acceptable status of the account. Therefore the customer feels free to disclose the transaction code to the merchant or merchants instead of the actual credit card number as at **22**, **24** and is relatively unconcerned if the transaction code is published or otherwise disseminated to unauthorized entities. In a preferred embodiment wherein a merchant identifier is pre-coded in association with the transaction code, the pre-coding of the transaction code will prohibit an unauthorized use due at least in part to the fact that the merchant is specifically identified and any attempt to use the transaction code other than by the identified merchant will be prohibited. In addition, the merchant is prevented from "overcharging" or "extending" the purchase by fixing the dollar amount to satisfy the specific cost or limit

of the purchase as well as a specific time limit or time parameters in which the authorization for payment is valid. Such information, as set forth above, is communicated by the requested and subsequently designated payment category as set forth above. Restricted communication between the merchant and the custodial authorizing entity as at **26** is permitted exclusively for purposes of verification of the transaction code in a manner, which may utilize, at least to some extent, conventional facilities for the verification of a credit card number by most merchants or like commercial establishments. As a result, the merchant also has a desired verification as to the validity of a transaction and can effectively make arrangements to be paid by the credit card company.

If for some reason the transaction code is refused verification, the customer may be informed directly by the merchant as at **28** and or the transaction may be terminated as at **30**. Assuming verification of the transaction code by the custodial authorizing entity, the merchant proceeds to consummate the purchase and send the order, as at **32**, in the case of a remote commercial transaction.

FIGS. **3** and **4** are representative of the versatility of the system and method of the present invention wherein the customer **54** may receive the aforementioned promotional information from the merchant **56** by any appropriate means such as television solicitation as at **58**, phone solicitation as at **60** and/or personal solicitation as at **62**. Once the customer receives the promotional information, which may include the viewing of the product itself, or in advance if a general estimate as to the ultimate cost of an anticipate purchase(s) can be made prior to viewing promotional information, the customer contacts the custodial authorizing entity **64** by any appropriate electronic or conventional facilities such as direct phone to phone contact as at **66** and **66'** or direct computer contact as at **42'**, **45'**. Once the customer's authorization is confirmed, details of the anticipated transaction are established so as to determine a payment category, and the a transaction code is issued to the customer. The customer, either directly or through a representative, can then utilize the transaction code to consummate a transaction within the defined parameters of the payment category. Moreover, the merchant **56**, through a conventional, yet restricted communication with the custodial authorizing entity **64** by any of a plurality of conventional or electronic methods using computer to computer linking as at **44'**, **45'** or by telephone transmission as at **56'**, **66'**, can obtain a verification and subsequent payment utilizing the transaction code only.

As emphasized above, an important feature of the present invention is the ability of the customer to request a desired or a required payment category and the ability of the custodial authorizing entity **64** and/or a processing computer **45** of the custodial authorizing entity to issue a transaction code in accordance with the payment category. The payment categories, may be collectively defined as a variety of different types of transactions. Such transactions may include a single transaction for a specific amount of a purchase to be consummated. Alternatively, the payment category may include a single transaction defined by a single purchase having a maximum limit amount, wherein the specific or precise cost of the purchase has not been determined for a variety of reasons, and as such, the customer desires to set a maximum amount for which the single transaction may be made. Accordingly, with such a payment category, the exact amount may not be known in advance, but the customer is assured of not paying over the specifically designated maximum limit. In addition, the transactions are preferably, but not necessarily, authorized to be conducted only over a fixed life period of time, such as within twenty four hours, thereby ensuring that an outstanding transaction code does not remain valid if not used as generally intended. This limited time period can, of course be varied or omitted depending upon the wishes of the customer and/or the policies of the custodial authorizing entity. Also, these or any other payment category transactions may include a specific merchant identification to further restrict use of the transaction code.

The payment category may also include a multi-transaction authorization wherein more than one purchase may be made from one or a plurality of different merchants, each of which may or may not be identified by the customer and pre-coded in association with the transaction code, and wherein a total cost of the plurality of purchases may not exceed a maximum limit amount. This transaction can also be limited to having to take place within a predetermined, designated fixed life span, such as but not limited to twenty four hours. Accordingly, in some instances wherein a customer, or an agent of the customer, such as a child, guardian, or care giver, must make a number of transactions or purchases which are authorized by the customer, the customer may designate a maximum amount which can be spent utilizing a particular transaction code within a predetermined period of time, and/or can designate that only one merchant, whether designated or not, can use the transaction code.

As yet another alternative, the payment category may include a repeating transaction for a specific amount to be paid in each of a fixed number of intervals. For example, the customer may which to join a gym or receive services or products over a fixed number of payment intervals, such as every thirty days. Accordingly, the merchant will be authorized to charge the credit card account designated by the corresponding transaction code a fixed monthly payment. Similarly, a repeating transaction for a stated minimum interval such as every thirty days may be authorized for a specific amount for an unspecified number of intervals wherein the merchant will be authorized to continuously obtain payment on a "monthly" basis until the customer decides to cancel such authorization. Also, a more open ended transaction wherein charges may be performed until cancelled and with or without other limiting criteria may also be provided.

Since many modifications, variations and changes in detail can be made to the described preferred embodiment of the invention, it is intended that all matters in the foregoing description and shown in the accompanying drawings be interpreted as illustrative and not in a limiting sense. Thus, the scope of the invention should be determined by the appended claims and their legal equivalents.

Now that the invention has been described,

What is claimed is:

1. A method of performing secure credit card purchases, said method comprising the steps of:

a) contacting a custodial authorizing entity having custodial responsibility of account parameters of customer's credit card account;

b) supplying the custodial authorizing entity with at least account identification data;

c) defining a plurality of payment categories, at least one of said payment categories including at least two of said purchase authorization for a repeating transaction at a fixed amount payable at each of a fixed number of time intervals;

d) designating at least one of said payment categories:

e) generating a transaction code reflecting at least said designated payment category and a purchase authorization within said designated payment category;

f) communicating the transaction code to a merchant to consummate a purchase within defined purchase parameters;

g) verifying that said defined purchase parameters are within said designated payment category; and

h) obtaining said purchase authorization so as to confirm that said defined purchase parameters are within said designated payment category and complete the purchase.

2. A method as recited in claim **1** further comprising the step of obtaining said purchase authorization from the custodial authorizing entity.

3. A method as recited in claim **1** further comprising a step of communicating promotional information of offered subject matter to the customer by the merchant, pre-determining the purchase parameters of the purchase, and corresponding said designated payment category to said purchase parameters.

4. A method as recited in claim **1** further comprising the merchant communicating the transaction code to the custodial authorizing entity for verification.

5. A method as recited in claim **1** further comprising the custodial authorizing entity generating a transaction code which reflects at least said designated one of a plurality of said payment categories.

6. A method as recited in claim **5** further comprising defining said plurality of payment categories to include amount parameters for a cost of purchase.

7. A method as recited in claim **5** further comprising defining said plurality of payment categories to include time parameters during which the purchase can be completed.

8. A method as recited in claim **5** further comprising defining the plurality of payment categories to include authorization for a single transaction at a fixed amount for purchase within a predetermined period of time.

9. A method as recited in claim **5** further comprising defining the plurality of payment categories to include authorization for a single transaction at a maximum amount for purchase within a predetermined period of time.

10. A method as recited in claim **5** further comprising defining the plurality of payment categories to include at least two of the purchase authorizations for multiple transactions at a maximum total amount for items purchased within a predetermined time period.

11. A method as recited in claim **5** further comprising defining the plurality of payment categories to include authorization for a repeating transaction at a fixed amount payable at each of an unspecified number of time intervals.

12. A method as recited in claim **5** further comprising defining the plurality of payment categories to include:

a) authorization for a single transaction at a fixed amount for a purchase within a predetermined period of time,

b) authorization for a single transaction at a maximum amount for a purchase within a predetermined period of time,

c) authorization for multiple transactions at a maximum total amount for purchases within a predetermined time period,

d) authorization for a repeating transaction at a fixed amount for purchases payable at each of a fixed number of time intervals, and

e) authorization for a repeating transaction at a fixed amounts for purchases payable at each of an unspecified number of time intervals.

13. A method as recited in claim **5** further comprising defining the plurality of categories to include:

a) authorization for a single transaction at a fixed amount for a purchase,

b) authorization for a single transaction at a maximum amount for a purchase,

c) authorization for multiple transactions at a maximum total amount for purchases,

d) authorization for a repeating transaction at a fixed amount for purchases payable at each of a fixed number of time intervals, and

e) authorization for a repeating transaction at a fixed amounts for purchases payable at each of an unspecified number of time intervals.

14. A method as recited in claim **1** further comprising generating a transaction code which further reflects an identification of the merchant.

15. A method as recited in claim **1** further comprising the step of defining the plurality of categories to include a limited time interval during which said purchase authorization is valid.

16. A method of performing secure credit card purchases, said method comprising the steps of:

a) contacting a custodial authorizing entity having custodial responsibility of account parameters of a customer's credit card account;

b) supplying the custodial authorizing entity with at least account identification data;

c) defining a plurality of payment categories, said payment categories including at least (i) authorization for a single transaction at a fixed amount for a purchase; (i) authorization for a single transaction at a maximum amount for a purchase; and iii) authorization for multiple transactions at a maximum total amount for purchases;

d) designating at least one of said payment categories:

e) generating a transaction code reflecting at least said designated payment category and a purchase authorization within said designated payment category;

f) communicating the transaction code to a merchant to consummate a purchase within defined purchase parameters;

g) verifying that said defined purchase parameters are within said designated payment category; and

h) obtaining said purchase authorization so as to confirm that said defined purchase parameters are within said designated payment category and complete the purchase.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,324,526 B1 Page 1 of 1
DATED : November 27, 2001
INVENTOR(S) : John D'Agostino

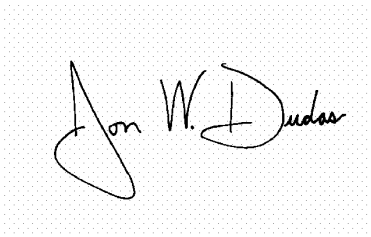
It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 8,
Lines 63 and 64, delete "at least two of said purchase authorization" and insert therefor -- at least two purchase authorization --.

Column 10,
Line 40, delete "i" (second occurrence) and insert therefor -- ii --.

Signed and Sealed this

Fourteenth Day of December, 2004



JON W. DUDAS
Director of the United States Patent and Trademark Office

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

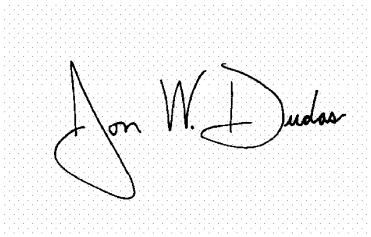
PATENT NO. : 6,324,526 B1
DATED : November 27, 2001
INVENTOR(S) : John D'Agostino

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 8,
Line 65, delete "authorization" and insert therefor -- authorizations --.

Signed and Sealed this

Fifth Day of April, 2005



JON W. DUDAS
Director of the United States Patent and Trademark Office

US006324526C1

(12) **EX PARTE REEXAMINATION CERTIFICATE** (6949th)

United States Patent
D'Agostino

(10) **Number: US 6,324,526 C1**
(45) **Certificate Issued: Jul. 21, 2009**

(54) **SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES**

(76) Inventor: **John D'Agostino**, 5120 NE. 27th Ter., Lighthouse Point, FL (US) 33064

Reexamination Request:
No. 90/007,481, Mar. 28, 2005

Reexamination Certificate for:
Patent No.: **6,324,526**
Issued: **Nov. 27, 2001**
Appl. No.: **09/231,745**
Filed: **Jan. 15, 1999**

Certificate of Correction issued Dec. 14, 2004.

Certificate of Correction issued Apr. 5, 2005.

(51) **Int. Cl.**
G06Q 20/00 (2006.01)

(52) **U.S. Cl.** **705/44**; 235/375
(58) **Field of Classification Search** 705/44
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2,167,543	A		7/1939	Bugenhagen
3,938,091	A		2/1976	Atalla et al.
4,423,316	A		12/1983	Sano et al.
4,707,592	A		11/1987	Ware
4,720,860	A		1/1988	Weiss
4,725,719	A		2/1988	Oncken et al.
4,747,050	A		5/1988	Brachtl et al.
4,797,920	A		1/1989	Stein
4,893,330	A		1/1990	Franco
5,097,505	A		3/1992	Weiss
5,130,519	A		7/1992	Bush et al.
5,163,097	A		11/1992	Pegg
5,193,114	A		3/1993	Moseley
5,196,840	A		3/1993	Leith et al.
5,202,826	A		4/1993	McCarthy
5,237,500	A	*	8/1993	Perg et al. 705/35
5,239,583	A		8/1993	Parrillo
5,287,268	A		2/1994	McCarthy
5,317,636	A		5/1994	Vizcaino
5,323,338	A		6/1994	Hawthorne
5,326,960	A		7/1994	Tannenbaum

(Continued)

FOREIGN PATENT DOCUMENTS

EP 0 081 921 A1 6/1983

(Continued)

OTHER PUBLICATIONS

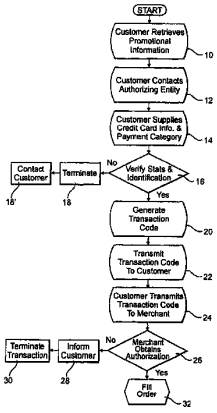
Eran Gabber and Abraham Silberschatz, A Minimal Distributed Protocol for Electronic Commerce, www.usenix.org/publications (Article), Oakland, USA, Nov. 18–21, 1996.

(Continued)

Primary Examiner—Jimmy G. Foster

(57) **ABSTRACT**

A method and system of performing secure credit card purchases in the context of a remote commercial transaction, such as over the telephone, wherein only the customer, once generally deciding upon a product or service to be purchased, communicates with a custodial authorizing entity, such as a credit card company or issuing bank wherein such entity has previous knowledge of the credit card number as well as custodial control of other account parameters such as interest rate, payment history, available credit limit etc. The customer supplies the custodial authorizing entity with the account identification data such as the credit card number and a requested one of a possible plurality of predetermined payment categories which define the dollar amount for the purchase and specific, predetermined time parameters within which authorization by the custodial authorizing entity will remain in effect. The custodial authorizing entity then generates a transaction code which is communicated exclusively to the customer wherein the customer in turn communicates only the transaction code to the merchant instead of a credit card number. The transaction code is indicative of merchant identification, credit card account identification and a designated one of the plurality of predetermined payment categories.



U.S. PATENT DOCUMENTS

5,363,449	A		11/1994	Bestock
5,428,684	A		6/1995	Akiyama et al.
5,466,919	A		11/1995	Hovakimian
5,478,994	A		12/1995	Rahman et al.
5,485,510	A		1/1996	Colbert
5,500,513	A		3/1996	Langhans et al.
5,504,808	A		4/1996	Hamrick, Jr.
5,555,497	A		9/1996	Helbling
5,577,109	A		11/1996	Stimson et al.
5,583,918	A		12/1996	Nakagawa
5,606,614	A		2/1997	Brady et al.
5,621,201	A		4/1997	Langhans et al.
5,627,355	A		5/1997	Rahman et al.
5,671,279	A		9/1997	Elgamal
5,694,471	A		12/1997	Chen et al.
5,696,908	A		12/1997	Muehlberger et al.
5,721,768	A		2/1998	Stimson et al.
5,724,424	A		3/1998	Gifford
5,748,908	A		5/1998	Yu
5,757,917	A		5/1998	Rose et al.
5,768,381	A		6/1998	Hawthorne
5,777,305	A		7/1998	Smith et al.
5,777,306	A		7/1998	Masuda
5,825,881	A		10/1998	Colvin, Sr.
5,826,241	A		10/1998	Stein et al.
5,826,243	A		10/1998	Musmanno et al.
5,832,087	A		11/1998	Hawthorne
5,845,281	A		12/1998	Benson et al.
5,864,830	A		1/1999	Armetta et al.
5,868,236	A		2/1999	Rademacher
5,883,810	A		3/1999	Franklin et al.
5,890,137	A		3/1999	Koreeda
5,893,907	A		4/1999	Ukuda
5,903,878	A		5/1999	Talati et al.
5,911,136	A	*	6/1999	Atkins ..... 705/36 R
5,914,472	A		6/1999	Foladare et al.
5,953,710	A		9/1999	Fleming
5,956,699	A		9/1999	Wong et al.
5,984,180	A		11/1999	Albrecht
5,991,749	A		11/1999	Morrill, Jr.
5,991,750	A		11/1999	Watson
6,000,832	A		12/1999	Franklin et al.
6,014,650	A		1/2000	Zampese
6,029,150	A		2/2000	Kravitz
6,029,890	A		2/2000	Austin
6,144,948	A		11/2000	Walker et al.
6,163,771	A		12/2000	Walker et al.
6,188,761	B1		2/2001	Dickerman et al.
6,226,624	B1		5/2001	Watson et al.
6,240,397	B1		5/2001	Sachs
6,267,292	B1		7/2001	Walker et al.
6,298,335	B1		10/2001	Bernstein
6,324,526	B1		11/2001	D'Agostino
6,341,724	B2		1/2002	Campisano
6,343,279	B1		1/2002	Bissonette et al.
6,375,084	B1		4/2002	Stanford et al.
6,422,462	B1		7/2002	Cohen
6,456,984	B1		9/2002	Demoff et al.
6,598,031	B1		7/2003	Ice
6,636,833	B1		10/2003	Flitcroft et al.
2001/0011249	A1		8/2001	Yanagihara et al.
2002/0120587	A1		8/2002	D'Agostino
2003/0018567	A1		1/2003	Flitcroft et al.
2003/0028481	A1		2/2003	Flitcroft et al.
2003/0097331	A1		5/2003	Cohen
2003/0216997	A1		11/2003	Cohen

FOREIGN PATENT DOCUMENTS

EP	0 590 861 A2	4/1994
EP	0 590 861 A3	4/1994
EP	0 590 961 A2	4/1994
FR	2 661 996 A1	11/1991
GB	2 145 265 A	3/1985
GB	2 252 270 A	8/1992
GB	2 327 831 A	2/1999
GB	2 361 790 A	10/2001
WO	WO 91/12693	5/1992
WO	WO 93/14476	7/1993
WO	WO 95/07512	3/1995
WO	WO 96/08756	3/1996
WO	WO 96/42150	12/1996
WO	WO 97/15893	5/1997
WO	WO 97/19549	5/1997
WO	WO 98/26376	6/1998
WO	WO 99/49424	9/1999
WO	WO 00/42486	7/2000

OTHER PUBLICATIONS

CITI.COM, Total Fraud Protection . . . Solutions for your safety and peace of mind, (printout) CBSD002144–CBSD002153.

Owen Thomas, Money Changers, www.ecompany.com, (Article), Oct. 2000.

Netchex—a short brief, www.tml.hut.fi/Stu/dies/Tik–110.50/1997/Ecomerce/netchex–5.html, (Article), Nov. 5, 2002.

GE Capital Financial Inc., GE Pre–Authorization System, (GE's website printout).

Virtual Credit Card (VCC), www.geocities.com/Eureka/Park/5014/vcc.htm, (printout). Jun. 28, 1999.

Smart Cards, disc.cba.uh.edu, (printout), Nov. 1, 2001.

Vincent Moscaritolo & Robert Hettinga, Digital Commerce for the Rest of Us Apple in a Geodesic Economy, www.shipwright.com/rants/rant_15.html, (article), Sep. 4, 1996.

Black Ives & Michael Earl, Mondex International Reengineering Money, London Business School Article, isds.bus.isu.edu/cases/mondex.html, Nov. 1, 2001.

Smart Card New Ltd's Information Gateway, www.smartcard.co.uk/articles/electronicmoney.html, Nov. 1, 2001.

Putting Risk in Perspective, (Article) Internet Outlook (Jul. 20, 1997), vol. 1 No. 3, www.webreference.com, Nov. 1, 2001.

Keith Lamond,Credit Card Transactions Real World and Online. www.virtualschools.edu/mon/ElectronicProperty/klamond/credit_card.htm, Sep. 11, 2001.

Steven P. Ketchpel & Andreas Paepcke, Shopping Models: A Flexible Architecture for Information Commerce, dbpubs.stanford.edu:8090, Oct. 1, 2002, (Stanford, USA).

* cited by examiner

EX PARTE REEXAMINATION CERTIFICATE ISSUED UNDER 35 U.S.C. 307

THE PATENT IS HEREBY AMENDED AS INDICATED BELOW.

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

Claims **1**–**16** are cancelled.

* * * * *

US007840486B2

(12) **United States Patent**
D'Agostino

(10) **Patent No.: US 7,840,486 B2**
(45) **Date of Patent: Nov. 23, 2010**

(54) **SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES**

(76) Inventor: **John D'Agostino**, 6237 Weymouth Dr., Sarasota, FL (US) 34238

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **11/252,009**

(22) Filed: **Oct. 17, 2005**

(65) **Prior Publication Data**

US 2006/0031161 A1 Feb. 9, 2006

Related U.S. Application Data

(63) Continuation of application No. 10/037,007, filed on Nov. 9, 2001, now abandoned, which is a continuation-in-part of application No. 09/231,745, filed on Jan. 15, 1999, now Pat. No. 6,324,526.

(51) **Int. Cl.**
G06Q 40/00 (2006.01)

(52) **U.S. Cl.** **705/44**; 705/41

(58) **Field of Classification Search** 705/39, 705/40, 44
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,938,091 A 2/1976 Atalla et al.
4,423,316 A 12/1983 Sano et al.
(Continued)

FOREIGN PATENT DOCUMENTS

CA 2167543 7/1997
(Continued)

OTHER PUBLICATIONS

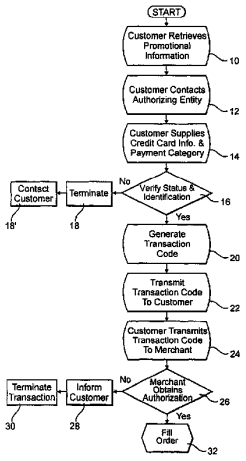
Lee et al.: Evoluntionary business models for e-cash with smart cards, Korea Advanced Institute of Science and Technology, Korea, http://koasas.kaist.ac.kr/bitstream/10203/4774/1/2000-092.pdf , pp. 352-358.*
(Continued)

Primary Examiner—Hani Kazimi
Assistant Examiner—Bijendra K Shrestha
(74) *Attorney, Agent, or Firm*—Maxey Law Offices, PLLC; Stephen Lewellyn

(57) **ABSTRACT**

A method and system of performing secure credit card purchases in the context of a remote commercial transaction, such as over the telephone, wherein only the customer, once generally deciding upon a product or service to be purchased, communicates with a custodial authorizing entity, such as a credit card company or issuing bank wherein such entity has previous knowledge of the credit card number as well as custodial control of other account parameters such as interest rate, payment history, available credit limit etc. The customer supplies the custodial authorizing entity with the account identification data such as the credit card number and a requested one of a possible plurality of predetermined payment categories which define the dollar amount for the purchase and specific, predetermined time parameters within which authorization by the custodial authorizing entity will remain in effect. The custodial authorizing entity then generates a transaction code which is communicated exclusively to the customer wherein the customer in turn communicates only the transaction code to the merchant instead of a credit card number. The transaction code is indicative of merchant identification, credit card account identification and a designated one of the plurality of predetermined payment categories.

30 Claims, 2 Drawing Sheets



U.S. PATENT DOCUMENTS

4,707,592	A		11/1987	Ware
4,720,860	A		1/1988	Weiss
4,725,719	A		2/1988	Oncken et al.
4,747,050	A		5/1988	Brachtl et al.
4,797,920	A		1/1989	Stein
4,893,330	A	*	1/1990	Franco 379/91.02
5,097,505	A		3/1992	Weiss
5,130,519	A		7/1992	Bush et al.
5,163,097	A		11/1992	Pegg
5,193,114	A		3/1993	Moseley
5,196,840	A		3/1993	Leith et al.
5,202,826	A		4/1993	McCarthy
5,239,583	A		8/1993	Parrillo
5,287,268	A		2/1994	McCarthy
5,317,636	A		5/1994	Vizcaino
5,323,338	A		6/1994	Hawthorne
5,326,960	A		7/1994	Tannenbaum
5,350,906	A		9/1994	Brody et al.
5,363,449	A		11/1994	Bestock
5,428,684	A		6/1995	Akiyama et al.
5,466,919	A		11/1995	Hovakimian
5,478,994	A		12/1995	Rahman et al.
5,485,510	A		1/1996	Colbert
5,500,513	A	*	3/1996	Langhans et al. 235/380
5,504,808	A		4/1996	Hamrick, Jr.
5,555,497	A		9/1996	Helbling
5,577,109	A		11/1996	Stimson et al.
5,583,918	A		12/1996	Nakagawa
5,606,614	A		2/1997	Brady et al.
5,621,201	A		4/1997	Langhans et al.
5,627,355	A		5/1997	Rahman et al.
5,671,279	A		9/1997	Elgamal
5,677,955	A		10/1997	Doggett et al.
5,694,471	A		12/1997	Chen et al.
5,696,908	A		12/1997	Muehlberger et al.
5,715,314	A		2/1998	Payne et al.
5,721,768	A		2/1998	Stimson et al.
5,724,424	A		3/1998	Gifford
5,727,163	A		3/1998	Bezos
5,729,594	A		3/1998	Klingman
5,748,908	A		5/1998	Yu
5,757,917	A		5/1998	Rose et al.
5,768,381	A		6/1998	Hawthorne
5,777,305	A		7/1998	Smith et al.
5,777,306	A		7/1998	Masuda
5,794,221	A		8/1998	Egendorf
5,815,657	A		9/1998	Williams et al.
5,822,737	A		10/1998	Ogram
5,825,881	A		10/1998	Colvin, Sr.
5,826,241	A		10/1998	Stein et al.
5,826,243	A		10/1998	Musmanno et al.
5,832,087	A		11/1998	Hawthorne
5,845,281	A	*	12/1998	Benson et al. 1/1
5,864,830	A		1/1999	Armetta et al.
5,868,236	A		2/1999	Rademacher
5,883,810	A		3/1999	Franklin et al.
5,890,137	A		3/1999	Koreeda
5,893,907	A		4/1999	Ukuda
5,903,878	A		5/1999	Talati et al.
5,914,472	A	*	6/1999	Foladare et al. 235/380
5,953,710	A	*	9/1999	Fleming 705/38
5,956,699	A		9/1999	Wong et al.
5,984,180	A		11/1999	Albrecht
5,991,749	A	*	11/1999	Morrill, Jr. 705/44
5,991,750	A	*	11/1999	Watson 705/44
6,000,832	A	*	12/1999	Franklin et al. 700/232
6,014,650	A	*	1/2000	Zampese 705/44
6,029,150	A	*	2/2000	Kravitz 705/39
6,029,890	A		2/2000	Austin
6,144,948	A		11/2000	Walker et al.
6,163,771	A	*	12/2000	Walker et al. 705/18
6,188,761	B1		2/2001	Dickerman et al.
6,226,624	B1	*	5/2001	Watson et al. 705/44
6,240,397	B1		5/2001	Sachs
6,267,292	B1		7/2001	Walker et al.
6,298,335	B1		10/2001	Bernstein
6,324,526	B1		11/2001	D'Agostino
6,339,766	B1		1/2002	Gephart
6,341,724	B2		1/2002	Campisano
6,343,279	B1		1/2002	Bissonette et al.
6,375,084	B1		4/2002	Stanford et al.
6,422,462	B1		7/2002	Cohen
6,456,984	B1	*	9/2002	Demoff et al. 705/40
6,598,031	B1		7/2003	Ice
6,636,833	B1		10/2003	Flitcroft et al.
2001/0011249	A1	*	8/2001	Yanagihara et al. 705/41
2002/0120587	A1		8/2002	D'Agostino
2002/0152158	A1	*	10/2002	Paleiov et al. 705/39
2003/0018567	A1		1/2003	Flitcroft et al.
2003/0028481	A1		2/2003	Flitcroft et al.
2003/0097331	A1		5/2003	Cohen
2003/0216997	A1		11/2003	Cohen

FOREIGN PATENT DOCUMENTS

EP	0 081 921	A1	6/1983
EP	0 590 861	A2	4/1994
EP	0 590 861	A3	4/1994
EP	0 590 961	A2	4/1994
FR	2 661 996	A1	11/1991
GB	2 145 265	A	3/1985
GB	2 252 270	A	8/1992
GB	2 327 831	A	2/1999
GB	2 361 790	A	10/2001
WO	WO 91/12693		5/1992
WO	WO 93/14476		7/1993
WO	WO 95/07512		3/1995
WO	WO 96/08756		3/1996
WO	WO 96/42150		12/1996
WO	WO 97/15893		5/1997
WO	WO 97/19549		5/1997
WO	WO 98/26376		6/1998
WO	WO 99/49424		9/1999
WO	WO 00/42486		7/2000

OTHER PUBLICATIONS

Jones, R.: Prepaid cards, an emerging internet payment mechanism, the Nuvantage Group, Jun. 2001, pp. 1-9.*

Eran Gabber and Abraham Silberschatz, A Minimal Distributed Protocol for Electronic Commerce, www.usenix.org/publications (Article), Oakland, USA, Nov. 18-21, 1996.

Citi.com, Total Fraud Protection . . . Solutions for your safety and peace of mind, (printout) CBSD002144-CBSD002153.

Owen Thomas, Money Changers, www.ecompany.com, (Article), Oct. 2000.

Netchex—a short brief, www.tml.hut.fi/StudiesiTik-110.50/1997/Ecomerce/netchex-5.html, (Article), Nov. 5, 2002.

GE Capital Financial Inc., GE Pre-Authorization System, (GE's website printout).

Matt Barthel, Diebold Plans Major Push in Market for Debit-Card Point of Sale Terminals, Sep. 28, 1993, American Banker, pp. 1-2.

Bob Woods, New Dell E-Commerce Guarantee Called "Weak", Aug. 13, 1998, Newbytes News pp. 1-2.

Anne Finnigan, The Safe Way to Shop Online, Good Housekeeping, Sep. 1998, pp. 1-2.

Paul Demery, Attaching the Smart Card Fortress, Credit Card Management, Sep. 1998, pp. 1-4.

Larry Chase, Taking Transactions Online, Target Marketting, Oct. 1998, 1-4.

Virtual Credit Card (VCC), www.geocites.com/Eureka/Park/5014/vcc.htm, (printout). Jun. 28, 1999.

Smart Cards, disc.cba.uh.edu, (printout), Nov. 1, 2001.

Vincent Moscaritolo & Robert Hettinga, Digital Commerce for the Rest of Us Apple in a Geodesic Economy, www.shipwright.com/rants/rant_15.html, (article), Sep. 4, 1996.

Black Ives & Michael Earl, Mondex International Reengineering Money, London Business School Article, isds.bus.Isu.edu/cases/mondex.html, Nov. 1, 2001.

Smart Card New Ltd's Information Gateway, www.smartcard.co.uk/articles/electronicmoney.html, Nov. 1, 2001.

Putting Risk in Perspective, (Article) Internet Outlook (Jul. 20, 1997), vol. 1 No. 3, www.webreference.com, Nov. 1, 2001.

Keith Lamond,Credit Card Transactions Real World and Online. www.virtualschools.edu/mon/ElectronicProperty/klamond/credit_card.htm, Sep. 11, 2001.

Steven P. Ketchpel & Andreas Paepcke, Shopping Models: A Flexible Architecture for Information Commerce, dbpubs.stanford.edu:8090, Oct. 1, 2002, (Stanford, USA).

Re-examination of U.S. Patent No. 6,324,526 granted to John D'Agostino, assigned U.S. Appl. No. 90/007,481, filed Mar. 28, 2005.

* cited by examiner

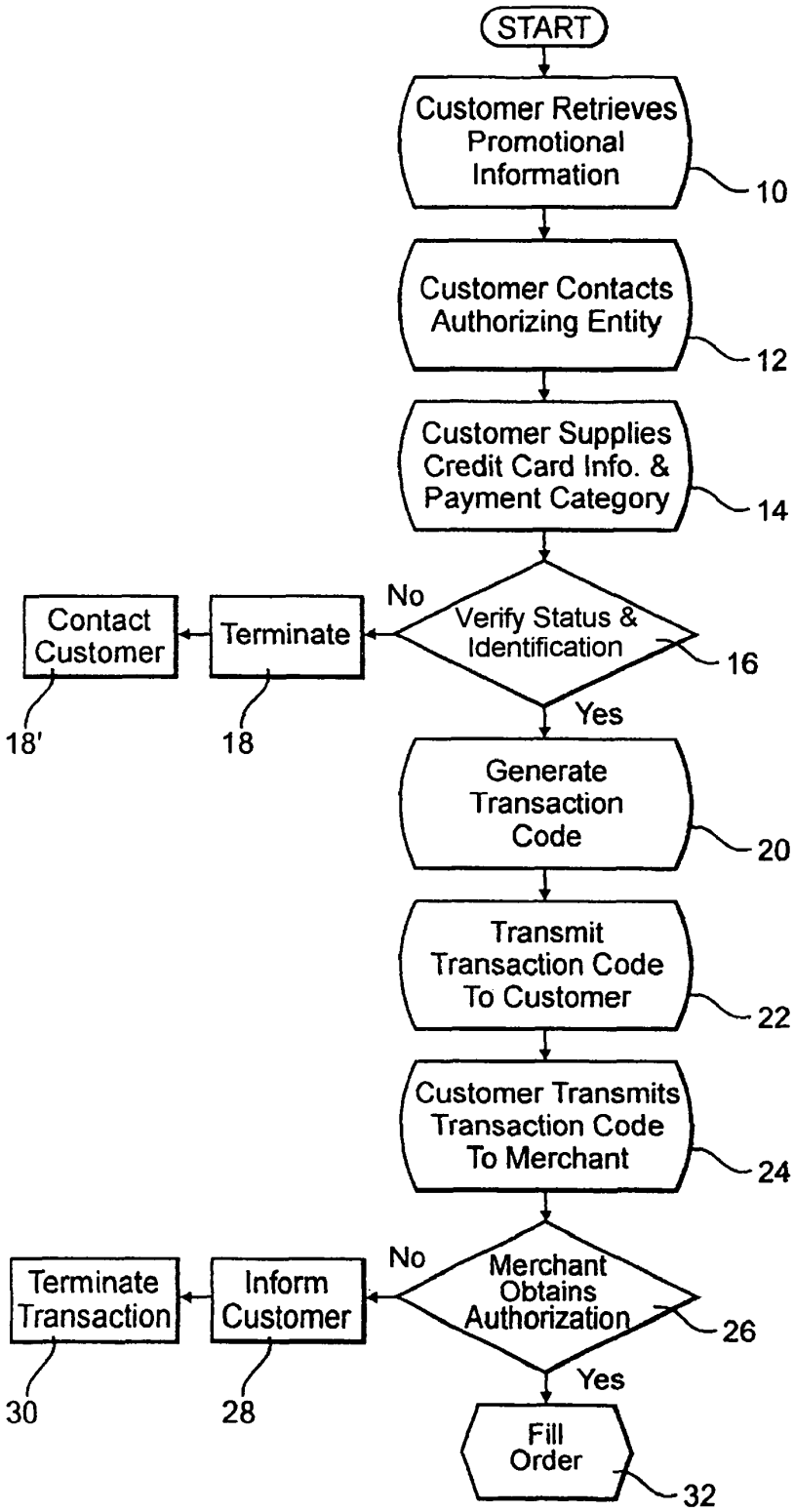

START
Customer Retrieves Promotional Information
10
Customer Contacts Authorizing Entity
12
Customer Supplies Credit Card Info. & Payment Category
14
Verify Status & Identification
16
No
Terminate
18
Contact Customer
18'
Yes
Generate Transaction Code
20
Transmit Transaction Code To Customer
22
Customer Transmits Transaction Code To Merchant
24
Merchant Obtains Authorization
26
No
Inform Customer
28
Terminate Transaction
30
Yes
Fill Order
32

FIG. 1

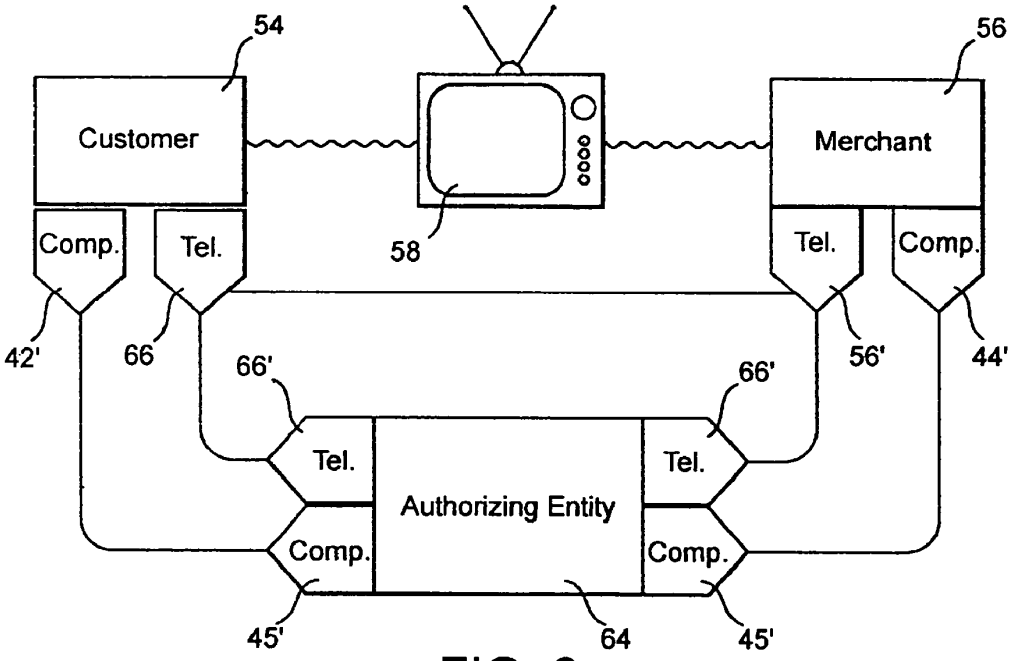

54
56
Customer
Merchant
58
Comp.
Tel.
Tel.
Comp.
42'
66
66'
66'
56'
44'
Tel.
Tel.
Authorizing Entity
Comp.
Comp.
45'
64
45'

FIG. 2

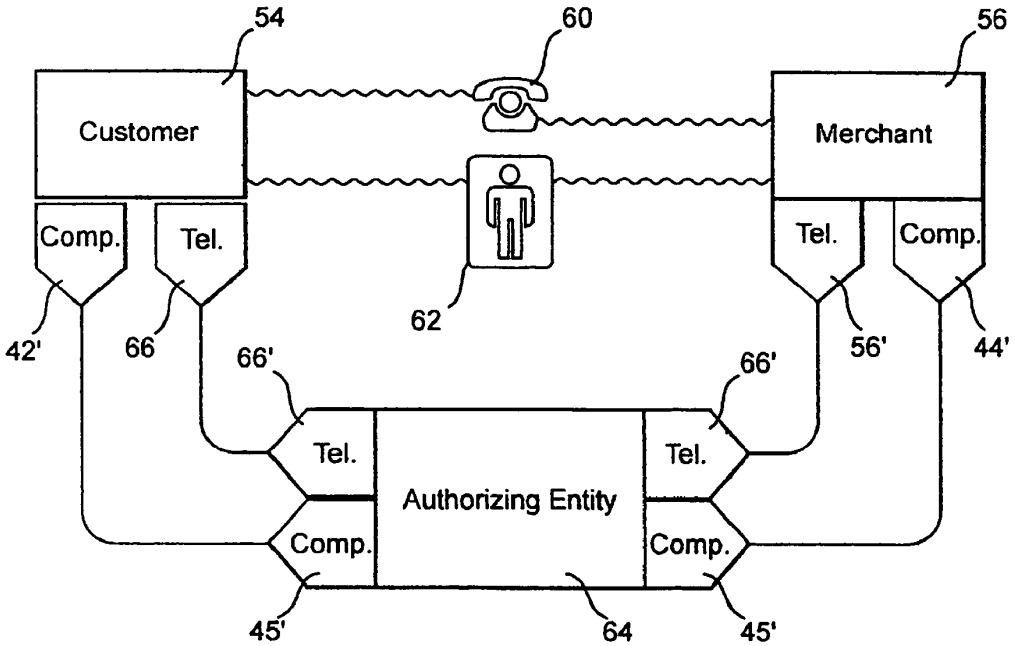

54
60
56
Customer
Merchant
Comp.
Tel.
Tel.
Comp.
62
42'
66
66'
66'
56'
44'
Tel.
Tel.
Authorizing Entity
Comp.
Comp.
45'
64
45'

FIG. 3

SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES

The present application is a Continuation of U.S. patent application Ser. No. 10/037,007, filed Nov. 4, 2001 now abandoned, which is a continuation-in-part of U.S. patent application Ser. No. 09/231,745, filed on Jan. 15, 1999, now U.S. Pat. No. 6,324,526, issued on Nov. 27, 2001.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to a system and method of performing secure credit card purchases in connection with remote commercial transactions, wherein a credit card holder does not have to reveal their credit card number to a merchant or a mechanism controlled by the merchant in order to accomplish a purchase, and wherein the merchant is still assured of the necessary credit verifications and approvals prior to authorizing and/or completing a credit card transaction, thereby increasing overall security by minimizing any access to credit card numbers without having to substantially modify or deviate from existing, accepted credit card transaction practices.

2. Description of the Related Art

The utilization of credit and debit cards to conduct transactions is ever increasing. This is especially the case with remote or "mail-order" transactions wherein merchants desire to be assured of a payment prior to shipping a product. For example, recent years have seen a substantial increase in the popularity of televised shopping networks to further supplement the popularity of catalogue type sales. Moreover, the increasing use and popularity of distributed computer networks such as the internet has also contributed to the dramatic increase in the number of remote commercial transactions conducted every day.

One primary reason associated with the rapid growth of remote commercial transactions is the ability of a merchant to reach an almost limitless number of potential customers at a substantially insignificant cost and with little or no operating overhead since an actual store is not required. Additionally, such sales techniques permit customers to view the products and services in a greatly expanded marketplace, representing a great number of vendors, without extensive travel and without foregoing the privacy and convenience of their home or other predetermined computer site in some cases. Simply put, a telephone or like communication avenue is all that is needed to place the consumer in contact with the merchant and complete the transaction.

The vast increase in popularity of remote commercial transactions conducted over the telephone or internet is further facilitated by the relatively simple protocols and procedures necessary to conduct such transactions. In particular, in order to complete a valid transaction, a merchant need not physically see the customer or the credit card, but must merely accept and enter a customer's credit card account number and an expiration date thereof to obtain authorization. This same convenience, however, is the primary disadvantage and/or problem associated with conducting commerce in the manners set forth above. Specifically, there is a great reluctance on the part of the customer to transmit the credit card account information, including the credit card number, because of the proliferation of fraud, and a well recognized lack of security directed to the protection of such account information. Indeed, it has been established that security and privacy concerns are realistic due to the fact that credit card account data is easily readable or interceptable by unauthorized parties, and can be readily used for all types of remote

transactions with minimal risk of being physically caught. In fact, unscrupulous individuals have many ways of gaining access to a consumer's legitimate remote transactions and thereby obtaining the credit card information. This information can be obtained from old credit card receipts or even from the unauthorized notation and use of the information by merchants or their employees after a legitimate transaction is made. Naturally, the latter is the most difficult to prevent utilizing known methods and systems unless a consumer is willing to completely forego the use of a credit card for purchases.

In the case of computerized remote transactions, as messages, including account data or other confidential information, move across the internet, they can easily pass through numerous computers, any one of which can be utilized to copy such confidential information or data, thereby leading to a further risk of potential fraud when conducting such transactions. Presently, some companies currently seek to address such security and privacy concerns by the employment of encryption programs and techniques. To this end there is an extensive facility associated with both public and private encryption schemes being deployed in order to guard the private or secured information being transmitted across the internet or like world wide networks. Unfortunately, however, even with such encryption techniques, the account information must usually still ultimately be transmitted to a third party who did not previously have access to that information previously. Even some more sophisticated systems which seek to interpose a separate computer or encryption entity between the consumer and the merchant so as to obtain authorization and forward it to the merchant, that information must still be made available to and/or transmitted to that third party, thereby leaving open an avenue for fraud or theft. Further, such encryption techniques, even if minimally effective for computerized remote transactions, are not truly useable for other conventional types of remote transactions, or even normal in person transactions.

Based on the above, there is an obvious need in the field of art associated with remote commercial transactions for a system and method of performing secure credit card purchases of goods and services which truly reduces the risk of potential fraud and theft by eliminating outside access to a consumer's private credit card information without requiring complex encryption equipment or significantly altering the ease and convenience of current transaction techniques. Further, such a system and method should also be effective for use in conventional, "in person" transactions as well, thereby providing an added measure of security and minimizing the hazards associated with the passing on of account information by unscrupulous merchants. Also, such a system should provide limits to potential loss or liability in a manner which does not impede the transaction.

SUMMARY OF THE INVENTION

The present invention is directed towards a system and method of performing secure credit card purchases, wherein payment for goods or services purchased is efficiently accomplished while eliminating the necessity of disclosure or dissemination of a consumers specific credit card number or other account data which the customer or other individual may wish to maintain in confidence. The system and method of the present invention incorporates the advantage of consummating the purchase by the customer through the selection of any one of a plurality of predetermined payment categories. Collectively, the payment categories represent a

variety of methods for accomplishing payment for a fixed transaction, a multiple transaction and/or a repeating transaction.

One embodiment of the system and method of the present invention comprises a customer receiving information, including specific data necessary for the purchase of any given product or service. This promotional information generated by the merchant can be received by any of a plurality of conventional means including advertisements, catalogues, computer network connections, direct person to person customer and merchant contact, telephone solicitation, mail orders, etc. Once the customer has identified the product or services which he/she wishes to purchase, the customer contacts and supplies a custodial authorizing entity with the requisite information concerning both the identification of a specific credit card or debit card account and a requested payment category. Additionally, security against unauthorized use of confidential account data may also preferably include information relating to the merchant's identification and/or location.

The custodial authorizing entity is preferably defined as the entity which has or has been assigned the custodial responsibility for the financial account data of a customer's credit card account, including a previous knowledge of the credit card number and other information such as credit limits, payment history, available credit amounts and other information which will determine the status of a given credit card account in terms of authorizing a requested payment for a current purchase.

As part of the security system for accomplishing a commercial transaction utilizing credit card or debit card payment, the custodial authorizing entity includes sufficient facilities, preferably including a processing computer or like applicable hardware for the generation of an exclusive transaction code. The transaction code is to be used in substitution for the credit card number and when utilized as authorized, will issue the merchant a credit approval, and will accomplish payment for the goods or services desired in the normal fashion normally associated with a credit or debit card transaction, without the publication or dissemination of an identifying credit card number for a specific customer's account to any entity that is not already aware of that information.

Further, a feature of the transaction code is its ability to indicate any one of preferably a plurality of predetermined payment categories which may be either requested by the customer or automatically chosen by the custodial authorizing entity based on the type of account or the type of purchase or other commercial transaction involved. Each of the payment categories are reflective of a different type of payment desired or required to consummate the intended purchase. More specifically, the plurality of payment categories may include a single transaction involving a specific dollar amount for a purchase within a specific time period, such as twenty four hours, during which authorization of the purchase remains valid. Alternately, a single transaction may be involved wherein a maximum limit or a dollar amount is determined above which the purchase will become invalidated and further wherein a fixed period of time is preferably established for maintaining authorization of such purchase. Other alternatives would involve one or more of the categories coded to define multiple transactions involving a maximum dollar amount for purchases, as well as a fixed period of time for authorization of such purchases, and/or a repeating transaction wherein payments may be automatically accessed by a merchant over a predetermined or unspecified time interval (such as every thirty days) for a specific dollar amount or a maximum dollar amount limit. Also, limits solely as to a specific merchant or a given time period can be effectively established for which the transaction code is valid.

A further feature of the present invention to be described in greater detail hereinafter, is the requirement that the transaction code, once received by the customer is transmitted to the merchant by the customer or a person specifically authorized by the customer. Only minimal contact by the merchant and the custodial authorizing entity is provided for purposes of the merchant verifying the validity of the transaction code utilizing a conventional process electronically or otherwise similar to the verification of a credit card number normally offered to a merchant for the purchase of goods or services. There is, therefore, no disclosure, publication or other dissemination of the specific credit card number of a given customer account beyond those entities who already know the information, and the transaction code is transmitted exclusively to the customer by the custodial authorizing entity who has the ability to better identify whether the customer is properly authorized to use the account. Moreover, the transaction code, once given out by the customer, only has a limited usefulness, thereby limiting the risk of misuse and minimizing the potential losses to be experienced by the credit card company and/or the account holder.

Accordingly, it is an object of the present invention to provide a system and attendant method for performing remote commercial transactions utilizing credit cards, which maximizes the security of the transaction and limits the potential liability to be experienced from a fraudulent transaction.

Yet another object of the present invention is to provide a secure system and method for establishing credit card purchases which eliminate the disclosure or dissemination of the actual credit card number to anyone other than a custodial authorizing entity which normally has custodial responsibilities for account information including the previously established credit card number.

It is another object of the present invention to provide a system and method of establishing secure credit card purchases through the generation of a transaction code which renders it extremely difficult or impossible to access or infiltrate a customer's credit card account by unauthorized means.

It is yet another object of the present invention to provide a secure method of completing a remote commercial transaction which eliminates the need to convey actual account information to a merchant, but which allows the merchant to conduct a normal verification of information needed to consummate a given purchase.

It is also an object of the present invention to provide a system and attendant method of accomplishing secure credit card purchases which eliminate the need to disclose or disseminate a given credit card number while providing the customer with the versatility of choosing any one of a plurality of predetermined payment categories.

It is yet another feature of the present invention to provide a system and method of accomplishing secure credit card payments having the versatility of allowing the customer to select any one of a plurality of payment categories which are indicative of a variance in the amount of a purchase as well as the time in which authorization for such payment is valid.

These and other objects, features and advantages of the present invention will become more clear when the drawings as well as the detailed description are taken into consideration.

BRIEF DESCRIPTION OF THE DRAWINGS

For a fuller understanding of the nature of the present invention, reference should be had to the following detailed description taken in connection with the accompanying drawings in which:

FIG. **1** is a schematic representation of a flow chart showing various steps involved in the performance of the system and method of the present invention for the secure credit card purchasing;

FIG. **2** is a schematic representation similar to that of FIG. **1** wherein customer to merchant contact is accomplished by conventional facilities such as television; and

FIG. **3** is a schematic representation similar that of FIG. **2** wherein customer to merchant contact is established either by phone or in person.

Like reference numerals refer to like parts throughout the several views of the drawings.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

As shown in the accompanying Figures, the present invention is directed towards a system and method for accomplishing secure credit card purchases. Moreover, these purchases can be "in person", but preferably include remote commercial transactions such as mail order, purchases over the internet, television solicitations, telephone solicitations, etc. Security is established by virtue of the elimination of the need to disclose an active credit card number and expiration date to the merchant or any other party other than the original credit card company, issuing bank or like financial institution which already has custodial responsibilities for the financial or account data associated with a given customer's credit card account.

More specifically and with reference to FIG. **1** the system as well as an attendant method is preferably instigated by the customer viewing a product, identifying a desired amount for a transaction and/or receiving promotional information as at **10**, either in person or by any of the electronic or more conventional techniques which will be described in greater detail with reference to FIGS. **2** through **3**. Once the customer reviews the product or promotional information and has sufficient information, such as including price, product or service identification, payment requirement, etc., regarding the remote commercial transaction to be conducted, the customer contacts, either by computer, telephone or in person, a custodial authorizing entity as at **12**. The custodial authorizing entity may herein be defined as comprising that entity or institution which has or has been designated by the entity which has custodial responsibility for the financial data and security of a given credit card account of a customer. As set forth above such custodial authorizing entity can be represented by the credit card company issuing a credit card to a given customer or alternately can be represented by a bank or other financial institution serving to sponsor a credit card or debit card to the extent of processing the debits and credit associated therewith. The authorizing entity's custodial responsibilities of course includes the previous knowledge and/or storage of the credit card number serving to identify a specific customer's credit card account. Once contacted, the customer then supplies appropriate identification data to inform the custodial authorizing entity of a specific customer's credit card account as at **14**. In addition, the customer will supply the custodial authorizing entity with additional required information needed to consummate the purchase as well as ensure the security of the account in order to prevent its unauthorized use. Such additional information may preferably include the identification of the merchant or merchants involved, when such information is deemed necessary, and a requested one of a plurality of predetermined payment categories to facilitate consummation of the purchase of the products or services desired. Such predetermined plurality of payment categories will be discussed in greater detail hereinafter.

Once the appropriate information has been received from the customer as indicated at **16**, the custodial authorizing entity verifies the credit card status and account identification of the customer to determine the viability of the account in terms of dollar amount limits, payment history, available credit balance, etc. If the accessed credit card account is not in good standing, the custodial authorizing entity will permanently or temporarily terminate the transaction as at **18** and/or communicate to the customer directly as at **18'** by any applicable means for purposes of informing the customer of the unacceptable status of the accessed credit card account. If the credit card account is in good standing, based at least in part on the requested payment category, (amount of payment), the custodial authorizing entity generates a transaction code as at **20**. The transaction code is used in substitution for the specific credit card number which would normally identify a customer's credit card account and would allow access thereto by any entity having possession of the credit card number whether or not such possession was authorized or unauthorized. More specifically, the transaction code is pre-coded to be indicative of a specific credit card account, preferably a merchant or merchants identification and a designated payment category, selected from the plurality of predetermined payment categories as set forth above. Once generated, the transaction code is communicated exclusively to the authorized and verified customer by the custodial authorizing entity as at **22**, wherein the system and method of the present invention preferably restricts communication between the custodial authorizing entity and the merchant except to conduct a normal verification as will be explained.

The verified customer thereafter and preferably within a time limit to be determined by the customer and pre-coded in association with the transaction code, will directly or through an authorized representative communicate the transaction code to the merchant as at **24**. The system and method of the preferred embodiment of the present invention contemplates that only the verified customer will transmit the generated transaction code to the merchant in the case of a remote commercial transaction, thereby limiting knowledge of the transaction code to those parties having a need to know. Of course, however, as the transaction code will generally have a limited value as defied by the verified customer when obtained, the verified customer may designate an agent or other entity to act as the customer on his/her behalf, with the amount of potential liability to be experienced by such a transaction to be limited to the amount defined by the verified customer when obtaining the transaction code.

At this point the purchase is consummated at least from the customer standpoint in that the customer has previously established the acceptable status of the account. Therefore the customer feels free to disclose the transaction code to the merchant or merchants instead of the actual credit card number as at **22**, **24** and is relatively unconcerned if the transaction code is published or otherwise disseminated to unauthorized entities. In a preferred embodiment wherein a merchant identifier is pre-coded in association with the transaction code, the pre-coding of the transaction code will prohibit an unauthorized use due at least in part to the fact that the merchant is specifically identified and any attempt to use the transaction

code other than by the identified merchant will be prohibited. In addition, the merchant is prevented from "overcharging" or "extending" the purchase by fixing the dollar amount to satisfy the specific cost or limit of the purchase as well as a specific time limit or time parameters in which the authorization for payment is valid. Such information, as set forth above, is communicated by the requested and subsequently designated payment category as set forth above. Restricted communication between the merchant and the custodial authorizing entity as at **26** is permitted exclusively for purposes of verification of the transaction code in a manner, which may utilize, at least to some extent, conventional facilities for the verification of a credit card number by most merchants or like commercial establishments. As a result, the merchant also has a desired verification as to the validity of a transaction and can effectively make arrangements to be paid by the credit card company.

If for some reason the transaction code is refused verification, the customer may be informed directly by the merchant as at **28** and or the transaction may be terminated as at **30**. Assuming verification of the transaction code by the custodial authorizing entity, the merchant proceeds to consummate the purchase and send the order, as at **32**, in the case of a remote commercial transaction.

FIGS. **3** and **4** are representative of the versatility of the system and method of the present invention wherein the customer **54** may receive the aforementioned promotional information from the merchant **56** by any appropriate means such as television solicitation as at **58**, phone solicitation as at **60** and/or personal solicitation as at **62**. Once the customer receives the promotional information, which may include the viewing of the product itself, or in advance if a general estimate as to the ultimate cost of an anticipated purchase(s) can be made prior to viewing promotional information, the customer contacts the custodial authorizing entity **64** by any appropriate electronic or conventional facilities such as direct phone to phone contact as at **66** and **66'** or direct computer contact as at **42'**, **45'**. Once the customer's authorization is confirmed, details of the anticipated transaction are established so as to determine a payment category, and a transaction code is issued to the customer. The customer, either directly or through a representative, can then utilize the transaction code to consummate a transaction within the defined parameters of the payment category. Moreover, the merchant **56**, through a conventional, yet restricted communication with the custodial authorizing entity **64** by any of a plurality of conventional or electronic methods using computer to computer linking as at **44'**, **45'** or by telephone transmission as at **56'**, **66'**, can obtain a verification and subsequent payment utilizing the transaction code only.

As emphasized above, an important feature of the present invention is the ability of the customer to request a desired or a required payment category and the ability of the custodial authorizing entity **64** and/or a processing computer **45** of the custodial authorizing entity to issue a transaction code in accordance with the payment category. The payment categories, may be collectively defined as a variety of different types of transactions. Such transactions may include a single transaction for a specific amount of a purchase to be consummated. Alternatively, the payment category may include a single transaction defined by a single purchase having a maximum limit amount, wherein the specific or precise cost of the purchase has not been determined for a variety of reasons, and as such, the customer desires to set a maximum amount for which the single transaction may be made. Accordingly, with such a payment category, the exact amount may not be known in advance, but the customer is assured of not paying over the specifically designated maximum limit. In addition, the transactions are preferably, but not necessarily, authorized to be conducted only over a fixed life period of time, such as within twenty four hours, thereby ensuring that an outstanding transaction code does not remain valid if not used as generally intended. This limited time period can, of course be varied or omitted depending upon the wishes of the customer and/or the policies of the custodial authorizing entity. Also, these or any other payment category transactions may include a specific merchant identification to further restrict use of the transaction code.

The payment category may also include a multi-transaction authorization wherein more than one purchase may be made from one or a plurality of different merchants, each of which may or may not be identified by the customer and pre-coded in association with the transaction code, and wherein a total cost of the plurality of purchases may not exceed a maximum limit amount. This transaction can also be limited to having to take place within a predetermined, designated fixed life span, such as but not limited to twenty four hours. Accordingly, in some instances wherein a customer, or an agent of the customer, such as a child, guardian, or care giver, must make a number of transactions or purchases which are authorized by the customer, the customer may designate a maximum amount which can be spent utilizing a particular transaction code within a predetermined period of time, and/or can designate that only one merchant, whether designated or not, can use the transaction code.

As yet another alternative, the payment category may include a repeating transaction for a specific amount to be paid in each of a fixed number of intervals. For example, the customer may which to join a gym or receive services or products over a fixed number of payment intervals, such as every thirty days. Accordingly, the merchant will be authorized to charge the credit card account designated by the corresponding transaction code a fixed monthly payment. Similarly, a repeating transaction for a stated minimum interval such as every thirty days may be authorized for a specific amount for an unspecified number of intervals wherein the merchant will be authorized to continuously obtain payment on a "monthly" basis until the customer decides to cancel such authorization.

Since many modifications, variations and changes in detail can be made to the described preferred embodiment of the invention, it is intended that all matters in the foregoing description and shown in the accompanying drawings be interpreted as illustrative and not in a limiting sense. Thus, the scope of the invention should be determined by the appended claims and their legal equivalents.

Now that the invention has been described,

What is claimed is:

1. A method of performing secure credit card purchases, said method comprising:

a) contacting a custodial authorizing entity having custodial responsibility of account parameters of a customer's account that is used to make credit card purchases;

b) supplying said custodial authorizing entity with at least account identification data of said customer's account;

c) defining a payment category including at least limiting purchases to a single merchant for at least one transaction, said single merchant limitation being included in said payment category prior to any particular merchant being identified as said single merchant;

d) designating said payment category thereby designating at least that a transaction code generated in accordance with said payment category can be used by only one merchant;

e) generating a transaction code by a processing computer of said custodial authorizing entity, said transaction code reflecting at least the limits of said designated payment category to make a purchase within said designated payment category;

f) communicating said transaction code to a merchant to consummate a purchase with defined purchase parameters;

g) verifying that said defined purchase parameters are within said designated payment category; and

h) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said designated payment category and to authorize payment required to complete the purchase.

2. The method of claim **1** further comprising the step of designating said single merchant subsequent to generating said transaction code.

3. The method of claim **1** wherein said step of communicating the transaction code to said merchant to consummate said purchase within defined purchase parameters further comprises designation of said single merchant.

4. The method of claim **1** wherein said step of generating said transaction code further comprises said customer obtaining said transaction code.

5. The method of claim **1** further comprising obtaining said authorization for said purchase from the custodial authorizing entity.

6. The method of claim **1** further comprising a step of communicating promotional information of offered subject matter to the customer by the merchant, pre-determining the purchase parameters of the purchase, and corresponding said designated payment category to said purchase parameters.

7. The method of claim **1** further comprising the merchant communicating the transaction code to the custodial authorizing entity for verification.

8. The method of claim **1** further comprising generating a transaction code which reflects at least one of a plurality of said payment categories.

9. The method of claim **8** further comprising defining at least one of said plurality of payment categories to include amount parameters for a cost of one or more purchases.

10. The method of claim **8** further comprising defining at least one of said plurality of payment categories to include time parameters during which the purchase can be completed.

11. The method of claim **8** further comprising defining at least one of said plurality of payment categories to include using said transaction code for a single transaction at a fixed amount for purchase within a predetermined period of time.

12. The method of claim **8** further comprising defining at least one of said plurality of payment categories to include using said transaction code for a single transaction at a maximum amount for purchase within a predetermined period of time.

13. The method of claim **12** further comprising defining at least one of said plurality of payment categories to include limiting purchases to said single transaction at said maximum amount for purchase within said predetermined period of time.

14. The method of claim **8** further comprising defining at least one of said plurality of payment categories to include using said transaction code for at least two purchases at a maximum total amount for items purchased within a predetermined time period.

15. The method of claim **14** further comprising defining at least one of said plurality of payment categories to include limiting purchases to said at least two purchases at said maximum total amount for items purchased within said predetermined time period.

16. The method of claim **8** further comprising defining at least one of said plurality of payment categories to include using said transaction code for at least two purchases for a repeating transaction at a fixed amount payable at each of a fixed number of time intervals.

17. The method of claim **16** further comprising defining at least one of said plurality of payment categories to include limiting purchases to said repeating transaction at said fixed amount payable at each of said fixed number of time intervals.

18. The method of claim **8** further comprising defining at least one of said plurality of payment categories to include using said transaction code for a repeating transaction at a fixed amount payable at each of an unspecified number of time intervals.

19. The method of claim **18** further comprising defining at least one of said plurality of payment categories to include limiting purchases to said repeating transaction at said fixed amount payable at each of said unspecified number of time intervals.

20. The method of claim **8** wherein said plurality of payment categories further include at least one of the group consisting of:

a) using said transaction code for a single transaction at a fixed amount for a purchase within a predetermined period of time,

b) using said transaction code for a single transaction at a maximum amount for a purchase within a predetermined period of time,

c) using said transaction code for multiple transactions at a maximum total amount for purchases within a predetermined time period,

d) using said transaction code for a repeating transaction at a fixed amount for purchases payable at each of a fixed number of time intervals, and

e) using said transaction code for a repeating transaction at a fixed amount for purchases payable at each of an unspecified number of time intervals.

21. The method of claim **8** wherein said plurality of payment categories further include at least one of the group consisting of:

a) using said transaction code for a single transaction at a fixed amount for a purchase,

b) using said transaction code for a single transaction at a maximum amount for a purchase,

c) using said transaction code for multiple transactions at a maximum total amount for purchases,

d) using said transaction code for a repeating transaction at a fixed amount for purchases payable at each of a fixed number of time intervals, and

e) using said transaction code for a repeating transaction at a fixed amount for purchases payable at each of an unspecified number of time intervals.

22. The method of claim **1** further comprising generating said transaction code to further reflect an identification of said single merchant.

23. The method of claim **22** further comprising defining said payment category to include limiting purchases to a limited time interval during which said purchase is permitted.

24. A method of performing secure credit card purchases, said method comprising:

a) identifying a pre-established account that is used to make credit card purchases;

b) designating at least one of a plurality of pre-defined payment categories which limit a nature of a subsequent

purchases, at least one of said payment categories including limiting purchases to a single merchant, said single merchant limitation being included in said payment category prior to any particular merchant being identified as said single merchant;

c) generating a transaction code by a processing computer of a custodial authorizing entity of said pre-established account, said transaction code associated with at least said pre-established account and the limits of said selected payment category, and different from said pre-established account;

d) communicating said transaction code to a merchant to consummate a purchase within defined purchase parameters;

e) verifying that said defined purchase parameters correspond to said designated payment category; and

f) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said designated payment category and to authorize payment required to complete the purchase; and

g) associating the purchase with said pre-established account.

25. A method of performing secure credit card purchases, said method comprising:

a) identifying a pre-established account that is used to make credit card purchases;

b) selecting a predetermined payment category which limits a nature, of a series of subsequent purchases to a single merchant, said single merchant limitation being included in said payment category prior to any particular merchant being identified as said single merchant;

c) generating a transaction code by a processing computer of a custodial authorizing entity of said pre-established account, said transaction code associated with at least said pre-established account and the limits of said selected payment category and different from said pre-established account;

d) communicating said transaction code to a merchant to consummate a purchase within defined purchase parameters;

e) verifying that said defined purchase parameters correspond to said selected payment category;

f) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said selected payment category and to authorize payment required to complete the purchase; and

g) associating the purchase with said pre-established account.

26. The method of claim **25** wherein said step of selecting said payment category which limits said nature of said series of subsequent purchases to said single merchant further comprises limiting said nature of said series of subsequent purchases to a fixed amount for each of said subsequent purchases.

27. The method of claim **25** wherein said step of selecting said payment category which limits said nature of said series of subsequent purchases to said single merchant further comprises limiting said nature of said series of subsequent purchases to a maximum total amount for said subsequent purchases.

28. The method of claim **25** wherein said step of verifying that said defined purchase parameters correspond to said selected payment category further identifies said merchant as said single merchant.

29. A method of performing secure credit card purchases, said method comprising the steps of:

a) identifying a pre-established account that is used to make credit card purchases;

b) selecting a pre-determined payment category which limits a nature of a subsequent purchase to a single merchant, said single merchant limitation being included in said payment category prior to any particular merchant being identified as said single merchant;

c) generating a transaction code by a processing computer of a custodial authorizing entity of said pre-established account, said transaction code associated with at least said pre-established account and the limits of said selected payment category, and different from said pre-established account;

d) designating a merchant as said single merchant;

e) communicating said transaction code to said merchant to consummate a purchase within defined purchase parameters;

f) verifying that said defined purchase parameters correspond to said selected payment category;

g) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said selected payment category and to authorize payment required to complete the purchase; and

h) associating the purchase with said pre-established account.

30. The method of claim **29** wherein said step of verifying that said defined purchase parameters correspond to said selected payment category further identifies said merchant as said single merchant.

* * * * *

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES
First Named Inventor/Applicant Name:	John D'Agostino
Filer:	Charles F. Wieland III/Christine Becker
Attorney Docket Number:	0076412-000029

Filed as Large Entity

ex parte reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Request for ex parte reexamination	1812	1	2520	2520
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**2520**

Electronic Acknowledgement Receipt	
EFS ID:	13726600
Application Number:	90012517
International Application Number:	
Confirmation Number:	5785
Title of Invention:	SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES
First Named Inventor/Applicant Name:	John D'Agostino
Customer Number:	21839
Filer:	Charles F. Wieland III/Christine Becker
Filer Authorized By:	Charles F. Wieland III
Attorney Docket Number:	0076412-000029
Receipt Date:	12-SEP-2012
Filing Date:	
Time Stamp:	17:11:43
Application Type:	Reexam (Third Party)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$2520
RAM confirmation Number	4904
Deposit Account	024800
Authorized User	WIELAND,CHARLES F.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees) Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees) Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	**Document Description**	**File Name**	**File Size(Bytes)/ Message Digest**	**Multi Part /.zip**	**Pages (if appl.)**
1	Transmittal Letter	ExParteReexamTransmittalsb0057.pdf	421779 4ab34a156a7ebb6077b2bc61641056523e98c944	no	3
Warnings:					
Information:					
2		029_RequestforExParteReexam.pdf	3943026 c462d532ba31df3206f6fb560891c09a48256741	yes	112
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Receipt of Original Ex Parte Reexam Request		1	83	
	Reexam Certificate of Service		84	84	
	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party		85	98	
	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party		99	112	
Warnings:					
Information:					
3	Copy of patent for which reexamination is requested	DAGOSTINO_USP_8036988.pdf	2099926 c3d670d3b14bdaf02665cd3fa4b7047325f84eb9	no	12
Warnings:					
Information:					
4	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	COHEN_USP_6422462.pdf	1893285 f0cbb3f0813d286122183800d5586d0293d31619	no	10
Warnings:					
Information:					
5	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	FRANKLIN_USP_5883810.pdf	2339686 58cc4ab582780537beee50dbc3b21720f2926b4d	no	15
Warnings:					
Information:					

6	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	JOAO_USP_5903830.pdf	7036603 188367c31f3385804eadea1b5a7719e45188341f	no	38
Warnings:					
Information:					
7	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	YANAGIHARA_USPubl_20010012 49.pdf	1818311 b1f4c3e322e677c4e8a117e103e8492d10a7f7f1	no	13
Warnings:					
Information:					
8	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	MUSMANNO_USP_5826243.pdf	1208925 78667be0b2bbcac1e68884f8b8d4a18ed618d034	no	9
Warnings:					
Information:					
9	Reexam - Info Disclosure Statement Filed by 3rd Party	029_1st_IDS.pdf	58257 5a25796bfec83528ac125fb51afa385e07fd3c67	no	2
Warnings:					
Information:					
10	Information Disclosure Statement (IDS) Form (SB08)	029_1st_PTO1449.pdf	67114 41eb1e794c689f7a6a2e16426294e2796d6b27df	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
11	Other Reference-Patent or Application Document	DAGOSTINO_USP6324526.pdf	1916795 201a9386b46955cb36bf45caca36a41657afebc6	no	13
Warnings:					
Information:					
12	Other Reference-Patent or Application Document	DAGOSTINO_USP7840486.pdf	1896884 73b7416a6337c0f5116f663b2ba93f5b86bb6da8	no	11
Warnings:					
Information:					
13	Fee Worksheet (SB06)	fee-info.pdf	30358 6803d681923d4c908e6460446e64311385b2f5ee	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	24730949	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/57 (02-09)
Approved for use through 02/28/2013. OMB 0651-0064
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

(Also referred to as FORM PTO-1465)

REQUEST FOR *EX PARTE* REEXAMINATION TRANSMITTAL FORM

Address to:
Mail Stop *Ex Parte* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attorney Docket No.: 0076412-000029

Date: September 12, 2012

1. ☒ This is a request for *ex parte* reexamination pursuant to 37 CFR 1.510 of patent number 8,036,988 issued October 11, 2011. The request is made by:
   ☐ patent owner. ☒ third party requester.

2. ☒ The name and address of the person requesting reexamination is:
   Charles F. Wieland III, Esq.
   Buchanan Ingersoll & Rooney PC
   1737 King Street, Suite 500, Alexandria, VA 22314

3. ☐ a. A check in the amount of $_____ is enclosed to cover the reexamination fee, 37 CFR 1.20(c)(1);
   ☒ b. The Director is hereby authorized to charge the fee as set forth in 37 CFR 1.20(c)(1) to Deposit Account No. 02-4800 ; **or**
   ☒ c. Payment by credit card. Form PTO-2038 is attached.

4. ☒ Any refund should be made by ☐ check or ☒ credit to Deposit Account No. 02-4800 37 CFR 1.26(c). If payment is made by credit card, refund must be to credit card account.

5. ☒ A copy of the patent to be reexamined having a double column format on one side of a separate paper is enclosed. 37 CFR 1.510(b)(4)

6. ☐ CD-ROM or CD-R in duplicate, Computer Program (Appendix) or large table
   ☐ Landscape Table on CD

7. ☐ Nucleotide and/or Amino Acid Sequence Submission
   If applicable, items a. – c. are required.
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM (2 copies) or CD-R (2 copies); **or**
      ii. ☐ paper
   c. ☐ Statements verifying identity of above copies

8. ☐ A copy of any disclaimer, certificate of correction or reexamination certificate issued in the patent is included.

9. ☒ Reexamination of claim(s) 1-38 (all issued claims) is requested.

10. ☒ A copy of every patent or printed publication relied upon is submitted herewith including a listing thereof on Form PTO/SB/08, PTO-1449, or equivalent.

11. ☐ An English language translation of all necessary and pertinent non-English language patents and/or printed publications is included.

12. ☒ The attached detailed request includes at least the following items:

a. A statement identifying each substantial new question of patentability based on prior patents and printed publications. 37 CFR 1.510(b)(1)
b. An identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited art to every claim for which reexamination is requested. 37 CFR 1.510(b)(2).

13. ☐ A proposed amendment is included (only where the patent owner is the requester). 37 CFR 1.510(e)

14. ☒ a. It is certified that a copy of this request (if filed by other than the patent owner) has been served in its entirety on the patent owner as provided in 37 CFR 1.33(c).
The name and address of the party served and the date of service are:

Maxey Law Offices, PLLC, Attention: Stephen Lewellyn, Esq.

15500 Roosevelt Boulevard, Suite 305

Clearwater, Florida 33760

Date of Service: Via Courier on September 12, 2012; **or**

☐ b. A duplicate copy is enclosed because service on patent owner was not possible. An explanation of the efforts made to serve patent owner **is attached**. See MPEP 2220.

15. Correspondence Address: Direct all communications about the reexamination to:

☒ The address associated with Customer Number: 21839

OR

☐ Firm or Individual Name

Address
Charles F. Wieland III, Esq.
Buchanan Ingersoll & Rooney PC, 1737 King Street, Suite 500

City Alexandria	State VA	Zip 22314
Country USA		
Telephone 703-836-6620	Email charles.wieland@bipc.com	

16. ☐ The patent is currently the subject of the following concurrent proceeding(s):

☐ a. Copending reissue Application No. _____
☐ b. Copending reexamination Control No. _____
☐ c. Copending Interference No. _____
☐ d. Copending litigation styled:

_____

_____

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

/Charles F. Wieland III/ — Authorized Signature
September 12, 2012 — Date
Charles F. Wieland III — Typed/Printed Name
33,096 — Registration No.
☐ For Patent Owner Requester
☒ For Third Party Requester

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Reexamination of John D'AGOSTINO Patent No.: 8,036,988 Issued: October 11, 2011 For: SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES	**MAIL STOP *EX PARTE* REEXAM** Group Art Unit: Unassigned Examiner: Unassigned Confirmation No.: Unassigned

REQUEST FOR *EX PARTE* REEXAMINATION

ATTN: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The undersigned ("Requester") requests *ex parte* reexamination of claims 1 through 38 of U.S. Patent No. 8,036,988 for "System and Method for Performing Secure Credit Card Transactions" to John D'Agostino ("D'Agostino") issued on October 11, 2011, filed on October 12, 2010 (the "'988 Patent"), in view of the substantial new questions of patentability raised by the prior art submitted with this request. The submitted prior art renders those claims anticipated under 35 U.S.C. § 102(b) and obvious under 35 U.S.C. § 103(a), thus warranting reexamination of those claims.

In support of its request, Requester provides the following:

- Copies of the prior art references that raise "substantial new questions of patentability" with respect to claims 1 through 38 of the '988 Patent (35 U.S.C. § 303);

- A statement pointing out each substantial new question of patentability for each of claims 1 through 38 of the '988 patent for which reexamination is requested (37 C.F.R. § 1.510(b)(1));
- A detailed explanation of the pertinence and manner of applying the cited prior art references to each of claims 1 through 38 of the '988 Patent (37 C.F.R. § 1.510(b)(2));
- A copy of the entire '988 Patent, including the front face, drawings, and specification/claims (37 C.F.R. § 1.510(b)(3) and (b)(4)); and
- Fees for requesting reexamination (37 C.F.R. § 1.20(c)(1)).

TABLE OF CONTENTS

Listing of Attachments

Attachment A – Claim Chart of D'Agostino's claims and written description verses Cohen

Attachment B – Claim Chart of D'Agostino's claims and written description verses Franklin, Joao, Yanagihara and Musmanno

Listing of Exhibits

Exhibit 1 Cohen, U.S. Patent No. 6,422,462

Exhibit 2 Franklin et al., U.S. Patent No. 5,883,810

Exhibit 3 Joao et al., U.S. Patent No. 5,903,830

Exhibit 4 Yanagihara et al., U.S. Patent Application 2001/0011249

Exhibit 5 Musmanno et al., U.S. Patent No. 5,826,243

I. STATEMENT UNDER 37 C.F.R. § 1.510(B)(1) POINTING OUT SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

A. The Disclosure of the '988 Patent

The business method claims of the '988 Patent issued after one non-final rejection and subsequent amendment, without comment regarding Reexamination Control No. 90/007,481 in which all related claims of parent U.S. Patent No. 6,324,526 were held unpatentable, and without comment regarding other prior examinations.

The '988 Patent was issued following remarks by Mr. D'Agostino in the Response to Non-Final Office Action, filed on March 18, 2011, that the claimed methods "[do] not identify a merchant prior to the generation of the transaction code" (p. 13).[1] However, as Mr. D'Agostino was aware from the prosecution of the reexamination of his earlier patent, this teaching is squarely found in the prior art, as explained in detail below.

Further, the Examiner stated as a reason for allowance "With regard to claim 1, the prior art of records, alone or combined, does neither anticipate nor render obvious, inter alia, as a whole, the uniquely patentable feature of '*defining at least one payment category to include at least limiting a number of transactions to one or more merchants, said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants*' in a method of performing secure credit card purchase." (Emphasis in original.)

[1] Support for this argument and the claim language was not provided by the written description, and if support exists at all, it would have to be only marginally supported by the multi-transaction maximum limit amount feature found at col. 8, ll. 18-34 of the '988 Patent. In recognition that requesting reexamination for issues arising under 35 U.S.C. § 112 is not proper (see, 37 C.F.R. § 1.552(a)), the subject claims are given the broadest reasonable interpretation and in accordance with the patent holder's asserted interpretation in Mr. D'Agostino's letters in which he asserts his patents.

As explained below, the highlighted language does not present a meaningful limitation in the claims when parsed, and to the degree it can be interpreted to be limiting, is found in the art asserted herein.

In light of this prosecution history, a substantial new question of patentability would be apparent in light of prior art that discloses, teaches or suggest features such as "identifying a merchant prior to the generation of a transaction code." This teaching is also evident from the art cited herein, as explained below.

The prosecution included rejections over a different Franklin patent (U.S. Patent No. 6,000,832) than applied herein, in view of Yanagihara. The Franklin patents not have the same disclosure and the '832 Franklin is not relied upon herein.

The '988 Patent discloses a business method wherein a custodial authorizing entity receives account information from an account holder, identifying an account that is used to make credit card purchases. The custodial authorizing entity receives a request from the account holder for a transaction code, which can be used to make a purchase within a payment category that limits transactions to a single merchant, the single merchant being included in the payment category prior to any particular merchant being identified as the single merchant. The custodial authorizing entity generates the transaction code utilizing a processing computer, the transaction code being associated with the account and reflecting at least the limits of the payment category. The custodial authorizing entity then communicates the transaction code to the account holder, and afterward will receive a request to authorize payment for a purchase using the transaction code. The custodial authorizing entity authorizes payment for the purchase if the purchase is within the payment category.

B. Overview and Scope of Independent Claims 1, 17, 18, 21, and 22 of the '988 Patent

i. Claim Scope

(a) "Comprising"

The term "comprising" opens the methods recited in each of the claims 1 through 38 to additional manipulative steps. *Exergen Corporation v. Wal-Mart Stores, Inc.*, 575 F.3d 1312, 1319 (Fed. Cir. 2009); *CIAS, Inc. v. Alliance Gaming Corp.*, 504 F.3d 1356, 1360 (Fed. Cir. 2007); *Invitrogen Corp. v. Biocrest Mfg., L.P.*, 327 F.3d 1364, 1368 (Fed. Cir. 2003).

(b) The Claim Recitation "limiting a number of transactions to one or more merchants, said one or more merchants limitation being including in said payment category prior to any particular merchant being identified as one of said one or more merchants" is not limiting

Each of independent claims 1, 17, 19, and 22 recite "limiting a number of transactions to one or more merchants." The use of "one or more" means that the number of merchants can be a single merchant having a number of transactions or any number of merchants, which encompasses the total universe of possibilities. As a result, the transactions are "limited" to any possible number of merchants, which is not a limitation at all. Thus, the recited claim recitation becomes non-limiting. It seems apparent from the Examiner's remarks that rely on this recitation that he did not understand this phraseology (Non-Final Office Action, p.5).

In addition, independent claims 1, 17, 19, and 22 further recite defining or selecting a payment category including "limiting a number of transactions to one or more merchants, said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more

merchants." Because the "said one or more merchants limitation" is not a limitation at all, this leads to an ambiguity in the recitation of including the limitation in said payment category "prior to any particular merchant being identified as one of said one or more merchants." Giving the claim its broadest reasonable interpretation, this recitation becomes simply defining or selecting any payment category before a customer selects a merchant, which seems to encompass the universe of practical possibilities, because the only remaining possibility is to "define" a payment category after selecting a merchant, but before designating the category - which is backwards, at best. It is with this interpretation that Requester understands claims 1, 17, 19, and 22 as discussed herein.

If the Office holds that the "prior to any particular merchant being identified as one of said one or more merchants" was in fact limiting, then the aforementioned claims could be interpreted as reciting defining or selecting any form of payment category prior to identifying any particular merchant. For the convenience of the Office, Requester will also provide arguments for anticipation or obviousness for this alternative interpretation of independent claims 1, 17, 19, and 22.

(c) Indefiniteness

It is recognized that indefiniteness under the second paragraph of 35 U.S.C. § 112 is not a basis for rejection during reexamination. See 37 C.F.R. § 1.552(a). However, under the present circumstances, a considering of indefiniteness issues is appropriate because the manifest indefiniteness of the claims impacts the scope of the claims and, hence, also impacts the obviousness issue.

(i) "Purchase Parameters"

Each of the independent claims of 1, 17, and 19 recite "communicating said transaction code to a merchant to consummate a purchase with defined purchase parameters; verifying that said defined purchase parameters are within said designated payment category; and providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said designated payment category." However, the '988 Patent does not provide any definition for "purchase parameters", and in fact, does not contain a single instance of the term in the entire specification outside of the claims newly presented in the continuation application that resulted in the '988 Patent. As a result, Requester is not provided with any context for which to define "purchase parameters," which is used in three separate manipulative steps in the methods of claims 1, 17 and 19.

Accordingly, Requester presents a "best guess" interpretation of this ambiguous and undefined term and for sake of argument construes "purchase parameters" to include transaction details for the purchase, such as payment card number, payment card expiration date, cardholder name for the payment card, transaction amount, etc. Requester respectfully submits that the interpretation of the recitation "purchase parameters" including transaction details as discussed herein is not inconsistent with the written description or the language of the claims of the '988 Patent, though support for the claim recitation is not particularly clear either.

(ii) The Claim Limitation "verifying that said defined purchase parameters are within said designated payment category"

Independent claims 1, 17, and 19 recite "verifying that said defined purchase parameters are within said designated payment category." The specification for the '988 Patent fails to disclose what the recited "verifying" step entails. The specification provides that:

> Restricted communication between the merchant and the custodial authorizing entity as at 26 is permitted exclusively for purposes of verification of the transaction code in a manner, which may utilize, at least to some extent, conventional facilities for the verification of a credit card number by most merchants or like commercial establishments. As a result, the merchant also has a desired verification as to the validity of a transaction and can effectively make arrangements to be paid by the credit card company.

Col. 7, ll. 13-22. The '988 Patent mentions verification of transaction codes and of a transaction generally, but does not disclose verifying that purchase parameters are within said designated payment category.

"Payment categories" appear to be defined as a variety of different types of transactions (col. 7, ll. 61-63). As an example, a payment category may include a single transaction for a specific purchase amount. Assuming purchase parameters to include transaction details for a transaction, as stated above, for sake of argument and to comply with the requirements of a reexamination request, Requester construes "verifying that said defined purchase parameters are within said designated payment category" to include verifying that the transaction details for a transaction are in compliance with (e.g., match with) the corresponding transaction details of the designated payment category. For example, if a payment category includes a single transaction for a specific purchase amount, such as $50, then the "verifying"

manipulative step will include verifying that the transaction details of the transaction include a purchase amount of $50. Requester respectfully submits that the interpretation of this recitation as discussed herein is not inconsistent with the written description or the language of the claims of the '988 Patent, though support for the claim recitation is not particularly clear either.

ii. Claim 1

Claim 1 recites a method for performing secure credit card purchases, comprising the steps of: contacting a custodial authorizing entity, supplying the custodial authorizing entity with account identification data of a customer's account, defining at least one payment category, designating the payment category, generating a transaction code reflecting the limits of the payment category, communicating the transaction code to a merchant to consummate a purchase, verifying that the purchase is within the designated payment category, and providing authorization for the purchase to confirm that the purchase is within the designated payment category and to authorize payment required to complete the purchase.

iii. Claim 17

Claim 17, which also recites a method of performing secure credit card purchases, is nearly the same as claim 1, except it is written in the point-of-view of a payment card processor. To this end, claim 17, when differing from claim 1, recites identifying a pre-established account that is used to make credit card purchases, selecting a payment category that limits the nature of a series of subsequent purchases, and associating a verified and authorized purchase with the pre-established account.

iv. Claim 19

Claim 19, which recites a method of performing secure credit card purchases, is identical to claim 17, except that the predetermined payment category is limited to only a single subsequent purchase, and it also includes a step of designating a merchant.

v. Claim 21

Claim 21, which recites a method for implementing a system for performing secure credit card purchases, is similar to claim 19 in that it is primarily from the point-of-view of a payment card processor and is directed to making a purchase within a payment category, but further comprises receiving a request to authorize payment in the transaction and authorizing the payment, in addition to limiting the payment category to a single merchant.

vi. Claim 22

Claim 22, which also recites a method for implementing a system for performing secure credit card purchases, is identical to claim 21, except that it recites a payment category that limits transactions to "one or more merchants" rather than a single merchant.

C. Overview of the Cited Art and Grounds for Reexamination

The references asserted herein were cited in a massive Information Disclosure Statement (IDS) during the prosecution of the '988 Patent. The IDS cited 162 U.S. patents and US published applications, 26 non-U.S. patent publications, and 20 non-patent literature publications, along with citation to Reexamination Control No. 90/007,481 that resulted in cancellation of all of the claims of Mr. D'Agostino's first

patent (U.S. 6,324,526) directed to the same basic claimed system. The IDS was filed March 21, 2011, the day a non-final rejection issued and shortly before a Notice of Allowance issued on April 29, 2011. Mr. D'Agostino did not explain the relevance of any of the documents cited therein, point to any as particularly relevant, did not identify those previously relied upon, nor did he point out that the claims of the '526 patent were cancelled in light of prior art during reexamination over, among other patents, the Cohen patent relied upon herein. It should be also noted that obviousness-type double patenting rejections issued in the '988 patent prosecution on March 21, 2011, and Mr. D'Agostino filed a Terminal Disclaimer over his first patent, all the claims of which had been cancelled as unpatentable during the Reexamination over the prior art applied herein.

It would seem apparent to question the patentability of one claim set (e.g., a claim set in the '988 Patent) after it has been held to be obvious over another claim set (e.g., in the '526 patent) that has been held to be unpatenable.

Under the Patent and Trademark Office Authorization Act of 2002 ("the 2002 Act"), a substantial new question of patentability can be raised by patents and printed publications "previously cited by or to the Office or considered by the Office" ("old art"). As stated in MPEP 2216, "[t]he revision permits raising a substantial new question of patentability based solely on old art, but only if the old art is 'presented/viewed in a new light, or in a different way, as compared with its use in the earlier concluded examination(s), in view of a material new argument or interpretation presented in the request.'" It is evident that the ex parte examiner was not sufficiently informed and did not appreciate the significance of this prior art. In essence the prior art relied upon

herein is presented in a new or effectively first light given that it was based in a massive IDS that the ex parte examiner manifestly did not fully appreciate.

i. U.S. Patent No. 6,422,462 to Cohen ("Cohen")(Exhibit 1)

Cohen, issued on July 23, 2002, is prior art to the '988 Patent[2] before the earliest claimed filing date of the '988 Patent, in that it has an effective filing date of March 30, 1998 via U.S. Provisional Application Serial Number 60/079,884. In Reexamination Control No. 90/007,481, the Board of Patent Appeals and Interferences expressly rejected Mr. D'Agostino's contentions that Cohen was not entitled to the provisional filing date in finding it was prior art. Decision of January 30, 2009. In fact, Mr. D'Agostino did not contest sufficiency of the disclosure, but rather only alleged technical errors in the claiming of priority.

The disclosure of Cohen relates to improved credit cards and methods for credit card transactions, specifically for customized use credit cards and more secure transmission of credit card information (col. 1, ll. 48-62).

Cohen discloses an account holder contacting their credit card company, verifying their identity, and then being provided with a disposable or customized number to be used for a single or limited range of transactions (col. 3, ll. 41-48). The account holder can indicate in advance what the single or customized use of the number is to be used for (col. 3, ll. 49-52).

[2] The '988 Patent claims priority back to Application Serial Number 09/231,745 filed on January 15, 1999, but the next link in the priority chain of the '988 Patent (Application No. 10/037,007 filed Nov. 9, 2001) acknowledged CIP status and, as pointed out above, various claim terms do not have clear support, meaning that the effective filing date could October 12, 2010, depending on how one interprets the claims. This analysis has not been done as being unnecessary given the effective prior art date of Cohen under §102(e).

Once the account holder has received the number, they can communicate the number to a merchant like it was a regular credit card number, which the merchant can authorize with the credit card company (col. 5, ll. 35-39). The credit card company can authorize the use of the customized number, or deny it if it is used for anything other than the single or customized use indicated by the account holder. For example, if the number is only to be used for airline reservations, and other use is attempted, the transaction will be declined (col. 7, ln. 66-col. 8, ln. 5).

Examples of the customized uses for which a disposable or customized number can be indicated may include a time limit (col. 6, ln. 7), a specified sequence (col. 4, ln. 13), specific merchant or industry (col. 8, ll. 2-14), specific individuals or groups of individuals (col. 8, ll. 15-16), a specific merchant or merchants (col. 8, ll. 33-34), purchase amount (col. 8, ln. 44), geographic area (col. 8, ll. 58-59), security level (col. 10, ln. 5), etc. These various customized uses can also be used in combination, such as a customized number to be used on specific dates, for specific amounts, etc. (col. 10, ll. 24-35).

The Board of Patent Appeal and Interferences, in Reexamination Control No. 90/007,481, stated the following findings of fact.

FINDINGS OF FACT

The record supports the following findings of fact (FF) by a preponderance of the evidence.

1. Cohen was filed on March 30, 1999 and claims the benefit under § 119(e) of Provisional Application No. 60/079,884 filed March 30, 1998.

2. The '526 patent issued on November 27, 2001 to the Appellant from patent application No. 09/231,745 filed January 15, 1999.

3. The Appellant does not challenge Cohen's claim to priority based on whether the granted patent is sufficiently supported by the provisional application.

4. Cohen describes a method of performing secure credit card purchases to reduce fraud in credit card transactions (col. 1, l. 60-col. 2, l. 8; col. 2, ll. 32-35) by issuing a credit card with a credit card number that is customized by the user so as to limit, or restrict, its use (col. 2, ll. 56-59; Fig. 1). The method includes contacting a credit card company (i.e., custodial authorizing entity) that has custodial responsibility of account parameters of a customer's credit card account by calling the credit card company or via the Internet (col. 3, ll. 42-48; col. 12, ll. 34-60), and supplying the custodial authorizing entity with account identification data which may include the credit card number and verification data (col. 3, ll. 42-48; col. 12, ll. 36-45).

5. Cohen also describes a plurality of payment categories that includes (i) authorization for a single transaction at a fixed amount for a purchase (col. 5, ll. 17-25), (ii) authorization for a single transaction at a maximum amount for a purchase (col. 5, ll. 5-16; col. 8, ll. 37-39), and iii) authorization for multiple transactions at a maximum total amount for purchases (col. 8, ll. 41-49).

6. Cohen teaches designation of a payment category via customization of the particular credit card for limited use (col. 2, ll. 56-59), for example, by using a form which is "filled out by the cardholder (or by the authorized person on the card or an authorized card user) to set the desired customization parameters" (col. 12, ll. 51-57).

7. Cohen further describes generating a credit card with a credit card number (i.e., transaction code) that is restricted in use so as to reflect the designated payment category and a purchase authorization within the designated payment category (col. 2, ll. 35-39; col. 3, ll. 4-40).

8. In Cohen, the credit card number is communicated to a merchant to consummate a purchase within the defined purchase parameters upon verifying that the defined purchase parameters are within the designated payment category (col. 5, ll. 35-49). The purchase is completed upon obtaining the purchase authorization which confirms that the defined purchase parameters are within the designated payment category (col. 5, ll. 44-49; Fig. 1).

9. Cohen further describes that the credit cart could be customized "for use in a particular store itself or a particular chain of stores (such as a particular restaurant, or a particular chain of restaurants)" (col. 8, ll. 32-35 and 40- 47).

10. Cohen does not describe a category having at least two purchase authorizations for a repeating transaction at a fixed amount which are payable at a fixed number of time intervals.

11. Musmanno describes a system for controlling a master account and nested sub-accounts where the sub-accounts separate out specific re-occurring expenses, such as car payments and mortgage payments (col. 2, ll. 40-47; col. 3, ll. 5-18; col. 5, ll. 26-59; Fig. 3, numerals 370, 380 and 390).

These findings were not contested in the Patent Office, nor the related litigation, D'Agostino v. Citibank, N.A., No. 8:04-cv-1506-T-23 MSS (M.D. Fla.), which was dismissed in light of the cancellation of all the '526 claims.

ii. U.S. Patent No. 5,883,810 to Franklin et al. (Franklin) (Exhibit 2)

Franklin, was filed on September 24, 1997 and is prior art to the '988 Patent under 35 U.S.C. §102(e). It was filed more than a year before the earliest possible effective filing date of the '988 Patent. See, footnote 2. The disclosure of Franklin relates to systems and methods for facilitating commerce using credit cards, debit cards, and other types of payment cards using an electronically recognizable card that has a private, permanent account number by issuing temporary transaction numbers on a transactional basis without exposure of the permanent account number (Franklin, col. 1, ll. 6-16).

In Franklin, an issuing institution (i.e., the '988 Patent's "custodial authorizing entity") receives a request from a customer for a transaction number. The issuing institution generates a temporary transaction number for a single transaction, and associate it with the customer's account. The issuing institution provides the transaction number to the customer, who can then provide it to the merchant as the payment card number for a transaction (col. 2, ll. 5-11).

Franklin's temporary transaction number is treated the same as any regular credit card number. The merchant handles the transaction number in a similar fashion, including seeking authorization from the issuing institution (col. 2, ll. 23-27). Franklin's temporary transaction number can also be linked to extra transaction information to further increase the security. For example, the transaction number might be tied to a

specific purchase amount, to a particular merchant ID, or be given an expiration term such that the number becomes invalid after the term expires (col. 2, ll. 48-55).

The issuing institution in Franklin receives an authorization request from the merchant using the merchant's existing computer system (col. 10, ll. 39-41). The issuing institution will examine the transaction number to determine whether it is a valid number (col. 10, ll. 61-63). If transaction details are included in the authorization request, and if there are records on the transaction number used in the request, the issuing institution may examine extra transaction information, such as the purchase amount or merchant ID disclosed above, to double check the accuracy of the request and ensure that the transaction in the authorization request complies with the requirements of the generated transaction code (col. 11, ll. 11-21).

iii. U.S. Patent No. 5,903,830 to Joao et al. (Joao) (Exhibit 3)

Joao was filed on June 12, 1997, before the earliest possible effective filing date of the '988 Patent, and is prior art to the '988 Patent under 35 U.S.C. §102(e). See, footnote 2.

The disclosure of Joao relates to financial transaction authorization, notification, and/or security apparatus and method for use in providing authorization, notification, and/or security in conjunction with credit card use (col. 1, ll. 8-16).

Joao discloses a transaction security apparatus including a receiver for receiving a limitation and restriction on account usage for a payment card account. Limitations or restrictions that may be placed on an account, which may be pre-selected by the cardholder, may include limits or restrictions on the types of transactions authorized, the merchants which may be authorized to accept the card, limits on the purchase amount

for transactions, the geographical area or location where the card may be used, authorized times for card usage (e.g., specific days, dates, times, etc.), or a combination thereof (col. 16, ll. 13-34).

In Joao, an authorization request for a transaction is processed. The transaction is processed such that if a restriction or limitation that has been placed on the account has been violated, then the transaction is not approved and/or not authorized (col. 17, ln. 66 to col. 18, ln. 6). The security apparatus of Joao maintains a count of the number of unauthorized transactions, and, once the number of unauthorized transactions reaches a predetermined limit, the associated card may be de-activated in order to prevent fraud or misuse (col. 17, ll. 37-49).

iv. U.S. Patent Publication No. 2001/0011249 to Yanagihara et al. (Yanagihara)

Yanagihara was filed on May 5, 1998, before the earliest possible effective filing date of the '988 Patent, and is prior art to the '988 Patent under 35 U.S.C. §102(e). See, footnote 2.

The disclosure of Yanagihara relates to an electronic money card for dealing with money electronically (paragraph [0001]). The electronic money card on Yanagihara is capable of storing usable limits of electronic money and passwords on a per-user or per-usage basis (paragraph [0004]). The usable limit of electronic money indicates the maximum limit of electronic money that the user can withdraw, and an aggregate amount indicates the total sum of electronic money that has been read from the electronic money card. This allows for the electronic money card to be programmed by the cardholder in such a way as to protect the electronic money card from being used fraudulently (paragraph [0019]).

The cardholder in Yanagihara can set per-usage limits of transaction amounts based on passwords that may vary from usage limit to usage limit (paragraph [0028]). For example, a first password may allow a withdrawal or charge on the card for a first amount, whereas a second password may allow a withdrawal or charge on the card for a second amount (paragraphs [0026-0029]). Aggregate usage limits may also be used, where the first password may allow withdrawals or charges for the first amount multiple times, until the aggregate usage limit has been reached (paragraph [0029]). This may allow a plurality of people to share a single card in common, such as a family, where each is provided with their own password that represents usage limits unique to the individual person, which may include usage limits on the purchase type, such as for books, food, clothes, etc. (paragraph [0038]).

Yanagihara also discloses a transaction record for recording data on transactions that the electronic money card has been used for. Data that may be recorded in the transaction record may include a user ID, transaction date, transaction category, amount transacted, and usage category (paragraph [0020]). This may allow for additional usage limits to be placed on the electronic money card or on individual users, such as authorizing or limiting transactions to a specific date, time, category, merchant, etc. Combined with the above usage limits for individual users, a cardholder may provide the electronic money card number and a unique password for multiple merchants that the cardholder owes a monthly, recurring fee, which may include a limit on transaction amount and date. This would allow each merchant to withdraw or charge the monthly fee for the specific transaction amount once a month, and not allow the merchant to exceed these limits.

v. U.S. Patent No. 5,826,243 to Musmanno

Musmanno was filed on January 3, 1994, before the earliest possible effective filing date of the '988 Patent, and is prior art to the '988 Patent under 35 U.S.C. §102(e).

As found by the BPAI, "Musmanno describes a system for controlling a master account and vested sub-accounts separate out specific recurring expenses, such as car payments and mortgage payments (col. 2, ll. 40-47; col. 3, ll. 5-18; col. 5, ll. 26-59; Fig. 3 numerals 370,380 and 390)." Decision, p. 8. Further at p. 38, the BPAI found the following to be true of Musmanno:

> However, we agree with the Examiner's alternative basis for the obviousness rejection of independent claims 1 and 17 based on the contention that "it is notoriously well known that the prevalent scheme for making car or mortgage payments involves multiple equal payments at a number of time intervals" (Ans. 8). This contention is not in dispute (Ans. 24; Reply Br. 4). The Examiner articulates that it would have been obvious to one of ordinary skill in the art to provide such a payment category in the method described in Cohen because periodic payments in car and mortgage payments is "so prevalent and notorious in the art that one of ordinary skill in the art would have expected[,] and therefore[,] would have found obvious[,] making equal payments for these types of payments . . ." and "[t]he desirability for making equal payments would have been readily apparent from the increased convenience of predictability that equal payments provide" (Ans. 8 and 17).
>
> We agree. The Examiner's articulated reason is rational and sufficient to conclude that including a payment category for a repeating transaction in the method described in Cohen would have been obvious to one of ordinary skill in the art. *See KSR*, 127 S.Ct. at 1741. In our view, the inclusion of a payment category for a repeating transaction to the payment categories already provided in Cohen (FF 5) is merely a predictable variation that yields a predicable result. *Id.* at 1739-40.

vi. Grounds for Rejection

As set forth in detail *infra*, each of claims 1-38 of the '988 Patent are anticipated under 35 U.S.C. § 102(e) by Cohen. Further, claims 11 and 12 are obvious over Cohen in view of Musmanno.

Additionally, each of claims 1-8, 15, 19-24, 27, 29-32, 35, and 27-38 of the '988 Patent are anticipated under 35 U.S.C. § 102(b) by Franklin. Claims 16, 25, 28, 33, and 36 would have been obvious under 35 U.S.C. § 103(a) over Franklin. Claims 17 and 18 would have been obvious under 35 U.S.C. § 103(a) over Franklin in view of Joao. Claims 9-14, 26, and 34 would have been obvious under 35 U.S.C. § 103(a) over Franklin in view of Yanagihara.

D. Aspects of the Law Governing Reexamination

i. Claim Interpretation

In determining whether a "substantial new question of patentability" exists to make reexamination appropriate, "the PTO must apply the broadest, reasonable meaning to the claim language, taking into account any definitions presented in the specification." *In re Bass*, 314 F.3d 575, 577 (Fed. Cir. 2002) (citing *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984)); *accord In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1369 (Fed. Cir. 2004) ("PTO is obligated to give claims their broadest reasonable interpretation during examination.") Thus, in this Request, the identified claims are given their broadest reasonable interpretation consistent with the '988 Patent specification. *In re Suitco Surface, Inc.*, *supra*.

ii. Anticipation

An inventor is not entitled to a patent if "the invention was patented...in this or a foreign country...more than one year prior to the date of the application for patent in the United States" or if "the invention was described in - (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent[.]" 35 U.S.C. §§ 102(b),(e). "A claim is anticipated only if each and every element set forth in the claims is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631. The express, implicit, or inherent disclosures of a prior art reference may be relied upon in the rejection of claims under 35 U.S.C. § 102. "The inherent teaching of a prior art reference, a question of fact, arises both in the context of anticipation and obviousness." *In re Napier*, 55 F.3d 610, 613 (Fed. Cir. 1995).

iii. Obviousness

An inventor may not obtain a patent "if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." 35 U.S.C. § 103(a). The Supreme Court has held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR International Co. v. Teleflex, Inc. et al.*, 127 S.Ct. 1727, 1739 (2007). The Court noted that "[w]hen work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different

one. In a person of ordinary skill can implement a "predictable variation" of an existing system, then "§ 103 likely bars its patentability." *Id.* at 1740.

iv. Evidentiary Standards

A substantial new question of patentability may be found based on references that a reasonable examiner would consider, by a preponderance of the evidence, important in deciding whether the claims of the '988 Patent are patentable. See *Xerox Corp. v. 3Com Corp.*, 69 F.Supp.2d 404, 407 (W.D.N.Y. 1999) ("[I]n a reexamination proceeding before the PTO, there is no presumption of validity and there must only be a preponderance of the evidence to show unpatentability before the PTO may reject the patent claim(s)."); *Bruning v. Hirose*, 161 F.3d 681, 685 (Fed. Cir. 1998) (patents do not "retain the presumption of validity during reexamination proceedings"); see also *In re Etter*, 756 F.2d 852, 858 (Fed. Cir. 1985) (statutory presumption of patent validity does not apply in patent reexamination proceedings, such that the examiner need not satisfy the "clear and convincing evidence" burden to reject a claim).

Moreover, see MPEP § 2242 ("It is not necessary that a 'prima facie' case of unpatentability exist as to the claim in order for 'a substantial new question of patentability' to be present as to the claim....") (citing *In re Etter*, 756. F.2d 825, 857 n.5 (Fed. Cir. 1985)).

v. Originally Cited References Filed But Not Applied

Under 35 U.S.C. § 303(a), "[t]he existence of a substantial new question of patentability is not precluded by the fact that a patent or printed publication was previously cited by or to the Office or considered by the Office." It simply needs to be presented in a new light in a material new argument. MPEP 2216.

II. DETAILED EXPLANATION UNDER 37 C.F.R. § 1.510(B)(2) OF THE PERTINENCY AND MANNER OF APPLYING THE CITED PRIOR ART TO EVERY CLAIM FOR WHICH REEXAMINATION IS REQUESTED

A. Claims 1-38 are anticipated under 35 U.S.C. § 102(e) by Cohen

Set forth below is a detailed explanation of the anticipation of each of claims 1-38 of the '988 Patent under 35 U.S.C. § 102(e) by Cohen as shown in the claim chart of Attachment A. Independent claims 1, 17, 19, 21, and 22 are set forth in the form of an element-by-element claim analysis.

i. Claim 1

a) "A method of performing secure credit card purchases, said method comprising:"

The claimed business method is directed to "accomplishing secure credit card purchases" (col. 5, ll. 28-30).

Similarly, Cohen discloses that "[i]t is an object of the present invention to provide improved credit cards and methods for credit card transactions" and that "[i]t is a further object of the present invention to provide methods and apparatus for secure transmission of credit card information" (Cohen, col. 1, ll. 48-62). Accordingly, Cohen anticipates secure credit card purchases.

b) "contacting a custodial authorizing entity having custodial responsibility of account parameters of a customer's account that is used to make credit card purchases"

The custodial authorizing entity "may herein be defined as comprising that entity or institution which has been designated by the entity which has custodial responsibility for the financial data and security of a given credit card account of a customer. As set forth above, such custodial authorizing entity can be represented by the credit card company issuing a credit card to a given customer...." (col. 5, ll. 53-60).

This is the same as Cohen, which discloses "a user dial[ing] into her credit card company" (Cohen, col. 3, ll. 42-44). It is well known in the art that a credit card company has custodial responsibility of a customer's account used to make credit card purchases. Accordingly, a user dialing into her credit card company is anticipatory of contacting a custodial authorizing entity as claimed.

c) "supplying said custodial authorizing entity with at least account identification data of said customer's account"

The '988 Patent discloses that "the customer then supplies appropriate identification data to inform the custodial authorizing entity of a specific customer's credit card account" (col. 5, ln. 66 - col. 6, ln. 2).

Similarly, in Cohen, the user "provid[es] the ordinary credit card number and verification data" to her credit card company (Cohen, col. 3, ll. 42-45). This supplies the credit card company, the custodial authorizing entity, with account identification data of the customer's account. Accordingly, Cohen anticipates the supplying manipulative step of claim 1.

d) "defining at least one payment category to include at least limiting a number of transactions to one or more merchants"

As discussed previously, "limiting a number of transactions to one or more merchants" is, in effect, non-limiting due to its recitation of "one or more merchants." Taking the broadest reasonable interpretation, the recitation is simply directed towards the defining of at least one payment category. As also stated previously, a payment category is a type of transactions, with different payment categories being a variety of types of transactions (col. 7, ll. 61-63). The '988 Patent provides, as an example, that a

payment category may include a multi-transaction authorization where more than one purchase may be made from one or a plurality of different merchants (col. 8, ll. 18-20).

Cohen discloses that the card can "be customized for only particular uses or groups of uses," which would constitute payment categories as claimed by the '988 Patent (Cohen, col. 7, ll. 66-67). In addition, some of the uses that the card can be customized for include the card only being valid "for use for that particular type of charge (computer or hardware stores...[or] for use in a particular store itself or a particular chain of stores" (Cohen, col. 8, ll. 25-34). Therefore, the customized use can include limiting a number of transactions to one or more merchants.

e) "said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants"

As stated above, the "one or more merchants' limitation" is in effect a non-limitation. Therefore, this recitation, which includes the "one or more merchants limitation" in said payment category prior to identifying any particular merchant, also becomes a non-limitation. Accordingly, Cohen's disclosure of customized uses for a card anticipates defining a payment category as recited in claim 1 of the '988 Patent.

However, as also discussed previously, this recitation, when read with the "defining" manipulative step as a whole, might be viewed to be limiting such that a payment category must be defined prior to the identification of any particular merchant being included in said payment category. With respect to this interpretation, Cohen discloses that a card "could be issued to the user which is only valid for use for that particular *type* of charge" (Cohen, col. 8, ll. 25-28) (emphasis added). A customized use card with a customized use for only that particular type of charge would result in a card

with a merchant limitation (e.g., only those merchants of that type) prior to any particular merchant (e.g., a specific merchant of that type) being identified. Accordingly, Cohen anticipates this recitation of the '988 Patent.

f) "designating said payment category"

Cohen discloses that "...a user can indicate in advance of purchase...what the single use or the customized credit card number is to be used for" (Cohen, col. 3, ll. 49-52). This is in effect a designation of a customized use, which is anticipatory of designating a payment category as is recited in claim 1 of the '988 Patent.

g) "generating a transaction code by a processing computer of said custodial authorizing entity"

The '988 Patent defines the transaction code "to be used in substitution for the credit card number and when utilized as authorized, will issue the merchant a credit approval, and will accomplish payment for the goods or services desired in the normal fashion..." (col. 6, ll. 33-34).

Just like the transaction code, Cohen discloses "credit cards or credit card numbers are generated" by the credit card company (Cohen, col. 2, ll. 35-36). The disposable or customized credit card numbers can be indistinguishable from ordinary credit card numbers such that "both users and vendors are encouraged to use the credit card in the same manner as regular credit cards" (Cohen, col. 3, ll. 6-9).

h) "said transaction code reflecting at least the limits of said designated payment category to make a purchase within said designated payment category"

The customized or disposable credit card numbers of Cohen, like the transaction code of the '988 Patent, may have a "single or a limited range use," where the single or customized use corresponds to the single or customized use previously indicated

(Cohen, col. 3, ll. 47-48). Accordingly, the customized credit card number reflects the limits of the payment category, in that the card number can only be used for the designated customized use.

i) "communicating said transaction code to a merchant to consummate a purchase with defined purchase parameters"

The '988 Patent discloses that "the verified customer...will directly or through an authorized representative communicate the code to the merchant..." and that "...the merchant proceeds to consummate the purchase..." (col. 7, ll. 27-28). As stated above, the specification of the '988 Patent does not disclose the term "purchase parameters," and Requester construes the term to include traditional transaction details, such as merchant identification, purchase amount, purchase date and time, etc.

Cohen discloses that "...the user transmits his or her credit card information to the vendor. That vendor then verifies the transaction..." (Cohen, col. 5, ll. 36-37). It is well known in the art that the process of a vendor verifying a transaction includes requesting authorization for the transaction from the issuer of the credit card used in the transaction, and that authorization requests include transaction details (e.g., defined purchase parameters). Accordingly, transmission of the credit card information to the vendor for verification anticipates the communicating step as recited in claim 1 of the '988 Patent.

j) "verifying that said defined purchase parameters are within said designated payment category"

As discussed previously, Requester construes the "verifying" step to include verifying that the transaction details of the purchase are in compliance with (e.g., match with) transaction details of the designated payment category. To this end, the '988

Patent merely discloses communication between the custodial authorizing entity and the merchant for purposes of verification of the transaction code (col. 7, ll. 13-16).

Likewise, as stated above, Cohen discloses that the vendor "then verifies the transaction" such that the card "is only valid for use for that particular type of charge...such that if the [user] tries to use it for anything else...the charge will be declined" (Cohen, col. 8, ll. 25-32). This constitutes "verifying the defined purchase parameters being within the payment category," such that if the transaction details are not within the customized use associated with the card, the charge will be declined. Accordingly, Cohen anticipates the verifying step recited in claim 1.

k) "providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said designated payment category and to authorize payment required to complete the purchase"

Cohen discloses that, as part of the verification/authorization of the transaction "...the credit card company notes the identity of the vendor, authorizes the transaction (if the credit card number is valid and the purchaser has sufficient funds available), and forwards the authorization code to the vendor" (Cohen, col. 5, ll. 45-49). Accordingly, as stated above, the authorization of the transaction confirms that the purchase parameters are within the customized use, and the forward of the authorization code to the vendor authorizes the payment required to complete the transaction. Therefore, Cohen anticipates this recitation of claim 1.

Based upon the foregoing, it is apparent that Cohen discloses the method for performing secure credit card purchases as recited in claim 1 of the '988 patent, thereby anticipating the claimed business method within the meaning of 35 U.S.C. § 102(e).

ii. Claim 2

"The method of claim 1 further comprising the step of designating at least one of said one or more merchants subsequent to generating said transaction code"

The '988 Patent does not expressly state what "designating at least one of said one or more merchants *subsequent* to generating said transaction code" may include. The use of the word "designate" is not defined nor is any definition provided for by context of its use. Furthermore, relevant disclosure in the '988 Patent is unclear as to the possible meaning, as it discloses that "...the customer may designate...that only one merchant, whether designated or not, can use the transaction code" (col. 8, ll. 30-34). In addition to the obvious ambiguity in stating that the customer may designated that a merchant, designated or not, can use the transaction code, there is no indication of how a merchant is designated. Accordingly, based on the accompanying disclosure of the '988 Patent, Requester for purpose of this Request, *arguendo,* construes designating at least one of said one or more merchants to include communicating the transaction code to the one or more merchants, which thereby designates the merchant receiving the transaction code as one of the one or more merchants.

Likewise, Cohen discloses "...the user transmit[ting] his or her credit card information to the vendor," which would thereby designated the vendor as one of the one or more merchants subsequent to the generation of the credit card number. Col. 3, ll. 49-52..

iii. Claims 3 and 20

"wherein said step of communicating the transaction code to a merchant to consummate said purchase within defined purchase parameters further comprises designation of said merchant as one of said one or more merchants"

Claim 3 includes the above recitation and is dependent from claim 1. Claim 20 includes the same recitation, but is instead dependent from claim 19.

As stated above with respect to claim 2, the '988 Patent does not provide a definition as to what "designation of said merchant" may include. Accordingly, Requester construes for purpose of this request, *arguendo,* the step of communicating the transaction code to a merchant to include the designation of said merchant. As also stated previously with respect to claim 2, Cohen discloses generating a customized credit card number, which may then be submitted to the vendor (Cohen, col. 5, ll. 36-37).

iv. Claim 4

"wherein said step of generating said transaction code further comprises said customer obtaining said transaction code"

Cohen discloses "...a user...is provided with a disposable or customized number..." (Cohen, col. 3, ll. 43-45). The user being provided with the customized credit card number is the same as the customer obtaining the transaction code. Accordingly, Cohen anticipates claim 4 of the '988 Patent.

v. Claim 5

"generating a transaction code which reflects at least one of a plurality of said payment categories"

The '988 Patent discloses that the transaction code may be "pre-coded to be indicative of...a designated payment category, selected from the plurality of predetermined payment categories..." (col. 6, ll. 33-36).

Cohen discloses that the disposable or customized card number "can also be customized for only particular uses or groups of uses" (Cohen, col. 7, ll. 66-67).

Accordingly, the customized number would reflect at least one of a group of customized uses.

vi. Claim 6

"defining at least one payment category to include amount parameters for a cost of one or more purchases"

Cohen discloses that "[a] customized credit card could be issues to the user which is only valid...to the credit limit decided by the issuer or [user]..." (Cohen, col. 8, ll. 25-30). The provided credit limit signifies amount parameters for a cost that may be included as at least one of the customized uses that may be designated.

vii. Claim 7

"defining at least one payment category to include time parameters during which the purchase can be completed"

The '988 patent discloses "time parameters during which the purchase can be completed" to be "more specifically...a specific time period, such as twenty four hours, during which authorization of the purchase remains valid" (col. 3, ll. 56-60).

Cohen discloses that "...each of the disposable credit cards can be given an expiration date...[t]hus, if the credit card is not used within the time limit, it expires" (Cohen, col. 6, ll. 4-7). Accordingly, Cohen discloses time parameters during which the purchase can be completed.

viii. Claim 8

"defining at least one payment category to include limiting said transaction code to a single transaction for a purchase within a predetermined period of time"

Similar to claim 7, above, claim 8 recites a purchase within a predetermined period of time, but additionally limits the transaction code to a single transaction.

Likewise, Cohen discloses that a card may "be valid for a specific predetermined amount of time" (Cohen, col., 7, ll. 61-62). In addition, Cohen also discloses that the card may be used for a single transaction, stating that "[w]ith respect to the disposable card, the user is instructed that, after use of the number once, the number may not be used again" (Cohen, col. 3, ll. 60-62). Accordingly, Cohen's disposable card valid for a specific predetermined period of time anticipates claim 8 of the '988 Patent.

ix. Claim 9

"defining at least one payment category to include limiting purchases to a single transaction at a maximum amount for purchase within a predetermined period of time"

As discussed above, Cohen discloses that a disposable card number could be used for a single transaction, which may also only be valid up to a specific credit limit. Additionally, as also discussed above, Cohen discloses that the card may also only be valid for a specific predetermined amount of time. Furthermore, Cohen directly discloses this specific recitation, stating that "[t]he card could be valid only for purchase on that particular day, to a certain designated purchase limit, and even, if desired only in a certain store..." (Cohen, col. 8, ll. 43-45).

x. Claim 10

"defining at least one payment category to include limiting purchases to at least one payment category to at least two purchases at a maximum total amount for items purchased within a predetermined period of time"

Claim 10 includes the same recitation of claim 9, but is directed towards "at least two purchases" at a maximum total amount, rather than the "single transaction" recited in claim 9.

As discussed previously, Cohen discloses throughout that a disposable card number may be used for a single use, while a customized card number may be used for customized use, which can include multiple transactions of multiple types, or from "groups of stores or types of stores, or types of purchases or items" (Cohen, col. 8, ll. 43-47). Accordingly, Cohen anticipates the recitation of claim 10 of the '988 Patent.

xi. Claims 11 and 12

"defining at least one payment category to include using said transaction code for at least two purchases for a repeating transaction at a fixed amount payable at each of a fixed number of time intervals"

As discussed previously, Cohen discloses defining a payment category (e.g., customized uses) to include using the credit card number for at least two purchases with a designated purchase limit (e.g., fixed amount payable). In addition to this, Cohen also discloses that "the card can have a user customized range of dates or series of dates" (Cohen, col. 7, ll. 44-46). The customized range or series of dates could be used to effect a repeating transaction, by the customized series of dates being a repeatable series. Likewise, a limit placed on the series could result in a fixed number of time intervals. Accordingly, Cohen anticipates the recitations of claim 11 of the '988 Patent.

Claim 12 is dependent from claim 11, and recites a payment category limiting purchases to the repeating transaction recited in claim 11. Accordingly, for the same reasons as discussed with respect to claim 11, claim 12 is anticipated by Cohen.

xii. Claim 13

"defining at least one payment category to include using said transaction code for a repeating transaction at a fixed amount payable to each of an unspecified number of time intervals"

Claim 13 includes a recitation identical to that of claim 12, except that the number of time intervals recited in claim 13 is unspecified.

As discussed above, Cohen discloses that "the card can have a user customized range of dates or series of dates" for fixed amounts. (Cohen, col. 7, ll. 44-46). When the series of dates is customized to have no end but rather be a series of repeating dates (e.g., every Wednesday, the first of every month, etc.) as is disclosed in Cohen, then the credit card number would be used for a repeating transaction at an unspecified number of time intervals. Accordingly, Cohen anticipates claim 13 of the '988 Patent.

xiii. Claims 14, 26, and 34

"defining at least one payment category to include limiting a repeating transaction to a maximum dollar amount"

Claims 14, 26, and 34 each include the above recitation and are dependent from claims 1, 21, and 22, respectively.

As discussed previously with respect to claims 11-13, Cohen discloses a repeating transaction as well as a designated purchase limit. In addition, Cohen discloses that "combinations of dates of transactions, types of transactions, amounts for individual and/or total transactions, etc. on a single card, or on multiple cards, can be set as well" (Cohen, col. 10, ll. 31-35). Accordingly, Cohen discloses the combination of groups of uses, which includes limiting a repeating transaction to a maximum dollar amount.

xiv. Claims 15, 27, and 35

"defining at least one payment category to include limiting purchases to a limited time interval during which a purchase is permitted"

Claims 15, 27, and 35 each include the above recitation, and are dependent from claims 1, 21, and 22, respectively.

As discussed above with respect to claim 7, Cohen discloses that "...each of the disposable credit cards can be given an expiration date...[t]hus, if the credit card is not used within the time limit, it expires" (Cohen, col. 6, ll. 4-7). And specifically, Cohen also discloses that the card "...could also be valid for a specific predetermined amount of time" (Cohen, col. 7, ll. 61-62). Accordingly, Cohen anticipates the claimed limited time interval during which a purchase is permitted.

xv. Claims 16, 28, and 36

"communicating said transaction code to the customer at the location of the merchant for use in person"

Claims 16, 28, and 36 each include the above recitation and are dependent from claims 1, 21, and 22, respectively.

Like the '988 Patent, Cohen discloses that the disposable or customized credit card number are ideally suited for Internet or other network-based financial transactions, but may also be used in person. Along these lines, Cohen discloses that there may be a physical manifestation of the card, that may be provided to the vendor such that "[t]he vendor could read the number of the disposable or customized card, could scan the number with a bar code scanner, could read a magnetic strip on the disposable card, or so forth" (Cohen, col. 4, ll. 31-35). Accordingly, Cohen discloses that the transaction

code may be communicated to the customer at the location of the merchant for use in person.

xvi. Claims 17 and 19

a) "A method of performing secure credit card purchases, said method comprising the steps of:"

As pointed out above with respect to claim 1, Cohen discloses that "[i]t is an object of the present invention to provide improved credit cards and methods for credit card transactions" and that "[i]t is a further object of the present invention to provide methods and apparatus for secure transmission of credit card information" (Cohen, col. 1, ll. 48-62). Accordingly, Cohen anticipates secure credit card purchases.

b) "identifying a pre-established account that is used to make credit card purchases"

Cohen discloses that the user "provid[es] the ordinary credit card number and verification data" to her credit card company (Cohen, col. 3, ll. 42-45). It is well known in the art that providing the ordinary credit card number and verification data to a credit card company is for the purpose of identifying a pre-established account used to make purchase with provided same credit card.

c) "selecting a pre-determined payment category which limits its a nature, of a series of subsequent purchases to one or more merchants"

As discussed previously, limiting the nature of a subsequent purchase to one or more merchants is, in effect, non-limiting due to its recitation of "one or more merchants." Taking the broadest reasonable interpretation, the recitation is simply directed towards the defining of at least one payment category.

As stated with respect to claim 1, Cohen discloses that the card can "be customized for only particular uses or groups of uses," which would constitute payment categories as claimed by the '988 Patent (Cohen, col. 7, ll. 66-67). In addition, some of the uses that the card can be customized for include the card only being valid "for use for that particular type of charge (computer or hardware stores...[or] for use in a particular store itself or a particular chain of stores" (Cohen, col. 8, ll. 25-34). Therefore, the customized use can include limiting a number of transactions to one or more merchants. As also discussed previously, Cohen also discloses that the customized uses may include limited use for both a series of subsequent purchase or a single subsequent purchase.

d) "said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants"

As discussed with respect to claim 1, this recitation is a non-limitation. If this recitation is held as following a different interpretation than Requester submits as being the broadest reasonable interpretation, then Cohen discloses that a card "could be issued to the user which is only valid for use for that particular *type* of charge" (Cohen, col. 8, ll. 25-28) (emphasis added). A customized use card with a customized use for only that particular type of charge would result in a card with a merchant limitation (e.g., only those merchants of that type) prior to any particular merchant (e.g., a specific merchant of that type) being identified. Accordingly, Cohen anticipates this recitation of the '988 Patent.

e) "generating a transaction code by a processing computer of a custodial authorizing entity of said pre-established account"

As discussed with respect to claim 1, Cohen discloses "credit cards or credit card numbers are generated" by the credit card company (Cohen, col. 2, ll. 35-36). The disposable or customized credit card numbers can be indistinguishable from ordinary credit card numbers such that "both users and vendors are encouraged to use the credit card in the same manner as regular credit cards" (Cohen, col. 3, ll. 6-9).

f) "said transaction code associated with at least said pre-established account and the limits of said selected payment category"

The '988 Patent states that "the transaction code is pre-coded to be indicative of a specific credit card account...and a designated payment category" (col. 6, ll. 33-35).

Similarly, The customized or disposable credit card numbers of Cohen, like the transaction code of the '988 Patent, may have a "single or a limited range use," where the single or customized use corresponds to the single or customized use previously indicated (Cohen, col. 3, ll. 47-48). In addition, Cohen also discloses that "...the credit card can be marked, if desired, to show both that it has been processed to charge money to the person's account...," which illustrates the association of the customized credit card with the specific credit card account (Cohen, col. 4, ll. 36-38).

g) "different from said pre-established account"

The '988 Patent discloses that "[t]he transaction code is used in substitution for the specific credit card number which would normally identify a customer's credit card account..." and thus be different from the pre-established account (col. 6, ll. 28-30).

Along these same lines, Cohen discloses that "[n]o vendor would ever...receive or have access to the user's permanent credit card number. Rather, the vendor would

receive a disposable credit card number from the user's supply" (Cohen, col. 4, ll. 26-31). Accordingly, Cohen discloses that the disposable or customized credit card number is different from the account number of the user's pre-established account.

h) "communicating said transaction code to said merchant consummate a purchase within defined purchase parameters"

As discussed with respect to the identical recitation in claim 1, although the '988 Patent specification does not use the term "purchase parameters," Cohen discloses that "...the user transmits his or her credit card information to the vendor. That vendor then verifies the transaction..." (Cohen, col. 5, ll. 36-37). It is well known in the art that the process of a vendor verifying a transaction includes requesting authorization for the transaction from the issuer of the credit card used in the transaction, and that authorization requests include transaction details (e.g., defined purchase parameters).

i) "verifying that said defined purchase parameters correspond to said selected payment category"

As discussed previously with respect to claim 1's identical recitation, Cohen discloses that the vendor "then verifies the transaction" such that the card "is only valid for use for that particular type of charge...such that if the [user] tries to use it for anything else...the charge will be declined" (Cohen, col. 8, ll. 25-32). This constitutes "verifying the defined purchase parameters being within the payment category," such that if the transaction details are not within the customized use associated with the card, the charge will be declined.

j) "providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said selected payment category and to authorize payment required to complete the purchase"

As discussed with respect to this recitation included in claim 1, Cohen discloses that, as part of the verification/authorization of the transaction "...the credit card company notes the identity of the vendor, authorizes the transaction (if the credit card number is valid and the purchaser has sufficient funds available), and forwards the authorization code to the vendor" (Cohen, col. 5, ll. 45-49). Accordingly, as stated above, the authorization of the transaction confirms that the purchase parameters are within the customized use, and the forward of the authorization code to the vendor authorizes the payment required to complete the transaction. Therefore, Cohen anticipates this recitation of claim 17.

k) "associating the purchase with said pre-established account"

The '988 Patent does not expressly disclose that the purchase is associated with the pre-established account. However, the '988 Patent does disclose that "the transaction code is pre-coded to be indicative of a specific credit card account," which, if the transaction code is used in the purchase, would enable the purchase to be associated with the specific credit card account (col. 6, ll. 33-34).

Likewise, Cohen discloses, as discussed above, that "...the credit card can be marked, if desired, to show both that it has been processed to charge money to the person's account..." (Cohen, col. 4, ll. 36-38). By showing that the transaction has been processed, and that money has been charged to the person's account, the transaction is therefore associated with the charge on the person's account and is therefore

associated with the pre-established account. Accordingly, Cohen anticipates this recitation.

Claim 19 is almost identical to claim 17, except for two recitations. First, in claim 19, the "selecting a predetermined payment category" step recites a single subsequent purchase instead of the series of subsequent purchases recited in claim 17. As discussed above, Cohen discloses disposable card numbers for a single transaction. Second, claim 19 also includes the recitation "designating a merchant as one of said one or more merchants." As discussed previously with respect to claims 2, 3, and 20, Cohen discloses that a merchant may be designated by the customer "transmit[ting] his or her credit card information to the vendor," which anticipates this recitation (Cohen, col. 5, ll. 36-37).

Based upon the foregoing, it is apparent that Cohen discloses the method for performing secure credit card purchases as recited in claims 17 and 19 of the '988 Patent, thereby anticipating the claimed business methods within the meaning of 35 U.S.C. § 102(e).

xvii. Claim 18

"said step of verifying that said defined purchase parameters correspond to said selected payment category further identifies said merchant as one of said one or more merchants"

Cohen discloses that "[u]pon use of the card, the information regarding the transaction is transmitted to the credit card company, as is known in the art" (Cohen, col. 13, ln. 66 - col. 14, ln. 1). It is well known in the art that merchant identification is included in the transaction details transmitted to the credit card company. Accordingly, during the verification of the transaction details, the merchant is identified as one of the

one or more merchants based on the included merchant identification. Accordingly, Cohen anticipates claim 18 of the '988 Patent.

xviii. Claims 21 and 22

The recitations of claim 22 are identical to the recitations of claim 21, except that where claim 21 recites "a single merchant," claim 22 recites "one or more merchants." However, as noted above, the "one or more merchants" limitation as recited in claim 22, is, in effect, a non-limiter, and thus claim 22 is directed to the same method of claim 21, but without the limitation of "a single merchant" in accordance with the broadest reasonable interpretation.

a) "A method for implementing a system for performing secure credit card purchases, the method comprising:"

As pointed out above with respect to claims 1 and 17, Cohen discloses that "[i]t is an object of the present invention to provide improved credit cards and methods for credit card transactions" and that "[i]t is a further object of the present invention to provide methods and apparatus for secure transmission of credit card information" (Cohen, col. 1, ll. 48-62). Accordingly, Cohen anticipates secure credit card purchases.

b) "receiving account information from an account holder identifying an account that is used to make credit card purchases"

As stated previously, Cohen discloses that the user "provid[es] the ordinary credit card number and verification data" to her credit card company (Cohen, col. 3, ll. 42-45). This constitutes account information that is received from the user (the account holder). It is well known in the art that providing the ordinary credit card number and verification data to a credit card company is for the purpose of identifying a pre-established account

used to make purchase with provided same credit card. Accordingly, Cohen anticipates this recitation.

c) "receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant"

As stated above, this recitation as included in claim 22, is directed to limiting transactions to "one or more merchants" rather than the "a single merchant" recited in claim 21.

Cohen discloses that "[a] user dials into her credit card company before making a transaction, and...is provided with a disposable or customized number" where the user "...can indicate in advance of purchase...what the single use or the customized credit card number is to be used for" (Cohen, col. 3, ll. 49-52). As discussed above, the single or customized use may include types of charges, a particular merchant, multiple merchants, etc. Accordingly, Cohen discloses a request from an account holder for a customized credit card number to make a purchase that limits transactions to either a single merchant or one or more merchants as the case may be.

d) "said single merchant limitation being included in said payment category prior to any particular merchant being identified as said single merchant"

As stated above, claim 22 includes this recitation, but directed toward the limitation being included prior to any particular "one or more merchant" being identified. As discussed with respect to claims 1 and 17, this recitation is non-limiting and thus, under the broadest reasonable interpretation, the transaction code would be for making a purchase within a designated payment category, without regard to merchant limitations. Under an alternative interpretation, as also discussed previously, the

transaction code would be within a designated payment category prior to the designation of any merchant.

As to the recitation as it appears in claim 21, the '988 Patent specification does not include any language directed towards "limit[ing] a transaction to a single merchant...prior to any particular merchant being identified as said single merchant" to provide for context and understanding of the recitation. Requester for sake of this Request, *arguendo* construes the recitation to include requiring that a transaction code only being used at one merchant as opposed to multiple merchants, and that the limitation is imposed prior to any particular merchant being identified as the one merchant.

Cohen discloses that a card "could be issued to the user which is only valid for use for that particular *type* of charge" (Cohen, col. 8, ll. 25-28) (emphasis added). A customized use card with a customized use for only that particular type of charge would result in a card with a merchant limitation (e.g., only those merchants of that type) prior to any particular merchant (e.g., a specific merchant of that type) being identified. Accordingly, Cohen anticipates this recitation of claims 21 and 22.

e) "generating a transaction code utilizing a processing computer of a custodial authorizing entity, said transaction code associated with said account"

As discussed with respect to claims 1 and 17, Cohen discloses "credit cards or credit card numbers are generated" by the credit card company (Cohen, col. 2, ll. 35-36). The disposable or customized credit card numbers can be indistinguishable from ordinary credit card numbers such that "both users and vendors are encouraged to use the credit card in the same manner as regular credit cards" (Cohen, col. 3, ll. 6-9). In

addition, as discussed previously regarding claim 17, Cohen also discloses that "...the credit card can be marked, if desired, to show both that it has been processed to charge money to the person's account...," which illustrates the association of the customized credit card with the specific credit card account (Cohen, col. 4, ll. 36-38).

f) "reflecting at least the limits of said payment category, to make a purchase within said payment category"

As discussed above, the customized or disposable credit card numbers of Cohen, like the transaction code of the '988 Patent, may have a "single or a limited range use," where the single or customized use corresponds to the single or customized use previously indicated (Cohen, col. 3, ll. 47-48). Accordingly, this means that the customized card number reflects at least the limits of the customized use for making a purchase within the customized use.

g) "communicating said transaction code to said account holder"

Cohen discloses that, upon dialing in to the credit card company, the account holder "...is provided with a disposable or customized number..." (Cohen, col. 3, ll. 43-45). Accordingly, this anticipates communicating the disposable or customized number to the account holder.

h) "receiving a request to authorize payment for a purchase using said transaction code"

Although the '988 Patent does not disclose the receipt of an authorization request for authorizing payment for a purchase using said transaction code, it does disclose communication between the merchant and the custodial authorizing entity for obtaining verification and subsequent payment using the transaction code (col. 7, ll. 49-55). Based on the foregoing, Requester construes this recitation to include receiving an

authorization request for a transaction, such as between the merchant and the custodial authorizing entity, as is consistent with the specification of the '988 Patent.

Although the '988 Patent does not explicitly disclose this recitation, Cohen provide explicit disclosure of "receiving the request for verification" from the vendor using the customized credit card (Cohen, col. 5, ll. 35-49). This request for verification, as is well known in the art, is the same as the request to authorize payment. Accordingly, Cohen anticipates this recitation.

i) "authorizing payment for said purchase if said purchase is within said payment category"

As discussed previously with respect to the "verifying" step of claims 1 and 17, Cohen discloses that, as part of the verification/authorization of the transaction "...the credit card company notes the identity of the vendor, authorizes the transaction (if the credit card number is valid and the purchaser has sufficient funds available), and forwards the authorization code to the vendor" (Cohen, col. 5, ll. 45-49). Accordingly, as stated above, the authorization of the transaction confirms that the purchase parameters are within the customized use, and the forward of the authorization code to the vendor authorizes the payment required to complete the transaction.

xix. Claims 23 and 31

"wherein the step of receiving account information from the account holder identifying an account that is used to make credit card purchases further comprises receiving information identifying a credit card account"

Claims 23 and 31 each contain this recitation, and are directed to claims 21 and 22, respectively.

As stated above with respect to claims 21 and 22, Cohen discloses the user dialing into her credit card company and providing "the ordinary credit card number and verification data" that constitutes information identifying a credit card account (Cohen, col. 3, ll. 42-45). Accordingly, Cohen anticipates this recitation.

xx. Claims 24 and 32

> **"wherein the step of generating a transaction code utilizing a processing computer of a custodial authorizing entity further comprises generating a transaction code which reflects at least one of a plurality of predetermined payment categories"**

Claims 24 and 32 each contain this recitation, and are directed to claims 21 and 22, respectively.

Like discussed above, Cohen discloses generating a disposable or customized credit card number that "can also be customized only for particular uses or groups of uses" (Cohen, col. 7, ll. 66-67). As the card number is customized for at least one of the plurality of uses, it therefore reflects at least one of the plurality of predetermined payment categories.

xxi. Claims 25 and 33

> **"wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant further comprises receiving a request from said account holder for a transaction code to make a purchase within a payment category that is automatically chosen by a custodial authorizing entity"**

Claims 25 and 33 each include the above recitation and are dependent from claims 21 and 22, respectively.

As discussed previously, Cohen discloses receiving a request for a disposable or customized credit card number from a user to make a purchase within a payment

category. It is inherent that, based on the user "indicat[ing] in advance of purchase...what the single use or the customized credit card number is to be used for" the credit card company would automatically chose the corresponding payment category. Because the payment categories, and authorization of cards as being within those payment categories, are managed by the credit card company, it is well known in the art that the credit card company would automatically choose the corresponding payment category (e.g., based on the information indicated by the user).

xxii. Claims 29 and 37

"wherein said step of receiving a request to authorize payment for a purchase using said transaction code further identifies said single merchant"

Claims 29 and 37 each contain this recitation, and are directed to claims 21 and 22, respectively.

As stated above with respect to the "receiving a request" step of claims 21, and 22, Cohen discloses that "[u]pon use of the card, the information regarding the transaction is transmitted to the credit card company, as is known in the art" where it is known in the art that transaction details included as part of the authorization request include merchant identification that identifies a merchant (Cohen, col. 13, ln. 66 - col. 14, ln. 1). In further support, Cohen also discloses that, as part of the authorization process, "...the credit card company notes the identity of the vendor..." and thus identifies the merchant (Cohen, col. 5, ll. 45-49).

xxiii. Claims 30 and 38

"wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant further comprises receiving a request from said

account holder for a transaction code to make a purchase within a predetermined payment category that is further limited in accordance with transaction details provided by said account holder"

Claims 30 and 38 each contain this recitation, and are directed to claims 21 and 22, respectively.

The '988 Patent specification does not disclose that transaction details are to be provided by the account holder, but are rather established by the custodial authorizing entity (see col. 7, ll. 43-45). Regardless of the ambiguity of the disclosure of the '988 Patent, Cohen discloses that as part of the request for a customized number "...a user can indicate in advance of purchase...what the single use or the customized credit card number is to be used for" (Cohen, col. 3, ll. 49-52). The customized number can be further limited as the "user could even identify the general or specific type and amount of transaction in advance," which constitutes transaction details provided by the user (Cohen, col. 5, ll. 23-25).

Conclusion

Based on the foregoing, Cohen discloses the methods for performing and for implementing a system for performing secure credit card purchases as claimed in the '988 Patent, and anticipates the subject matter claimed in each of claims 1-38 of the '988 Patent under 35 U.S.C. § 102(e).

B. Claims 11 and 12 are obvious over Cohen in view of Musmanno

It is noted that in Reexamination Control No. 90/007,481, the BPAI stated that "Cohen does not describe a category having at least two purchase authorizations for a

repeating transaction at a fixed amount which are payable at a fixed number of time intervals." Decision at p. 7.

It seems that BPAI did not envision the interpretation of Cohen as offered in the preceding section A (xi). However, it did find this feature in Musmanno, per the quoted text above. Hence, the BPAI has already found this feature does not lend patentable subject matter in the context of Mr. D'Agostino's disclosed system and nothing in the slightly different permutation of features of the '988 Patent would not lead to an unobvious or unexpected result. Rather, it is using a known feature or element for its known purpose to yield a predictable result and is therefore an unpatentable obvious variation. KSR Int'l Co. v. Teleflex, Inc., 550 U.S. 398 (2007).

C. Claims 1-8, 15, 19-24, 27, 29-32, 35, and 37-38 are anticipated under 35 U.S.C. § 102(b) by Franklin.

Set forth below is a detailed explanation of the anticipation of each of claims 1-8, 15, 19-24, 27, 29-32, 35, and 37-38 of the '988 Patent under 35 U.S.C. § 102(e) by Franklin.

Independent claims 1, 21, and 22 are set forth in the form of an element-by-element claim analysis.

i. Claim 1

a) "A method of performing secure credit card purchases, said method comprising:"

The claimed method is directed to "accomplishing secure credit card purchases" (col. 5, ll. 28-30). As previously discussed, however, in the context of the claimed invention, the preamble "purchases" amounts to a mere recitation of intended use, and

not a limitation on the claimed method which, under the broadest reasonable interpretation, may include wire transfers, cash advances, balance transfers, etc. in addition to traditional payment card purchases.

Franklin discloses "systems and methods for conducting online transactions using an *electronically realizable card* that has a private, permanent account number" (Franklin, col. 1, ll. 10-16). An issuing institution generates a temporary transaction number, associated with the permanent account number, for use in a single transaction. "To the merchant, the transaction number is treated the same as any regular credit card number" (Franklin, col. 2, ll. 23-25). The temporary transaction number disclosed in Franklin accomplishes secure credit card purchases.

b) "contacting a custodial authorizing entity having custodial responsibility of account parameters of a customer's account that is used to make credit card purchases"

The custodial authorizing entity "may herein be defined as comprising that entity or institution which has been designated by the entity which has custodial responsibility for the financial data and security of a given credit card account of a customer." As set forth above, such custodial authorizing entity can be represented by the credit card company issuing a credit card to a given customer...." (col. 5, ll. 53-60).

Franklin discloses "send[ing] a request to the issuing institution" (Franklin, col. 2, ll. 13-14). The issuing institution may be an institution that issues a commerce card to a customer. The issued card may be assigned a permanent customer account number, which is maintained on behalf of the customer by the issuing institution (Franklin, col. 2, ll. 5-6). Accordingly, Franklin's sending a request to the issuing institution anticipates the contact a custodial authorizing entity recited in claim 1 of the '988 Patent.

c) "supplying said custodial authorizing entity with at least account identification data of said customer's account"

The '988 Patent discloses that "the customer then supplies appropriate identification data to inform the custodial authorizing entity of a specific customer's credit card account" (col. 5, ln. 66 - col. 6, ln. 2). "Appropriate identification data may preferably include the identification of the merchant or merchants involved...." (col. 6, ll. 6-8).

Franklin discloses that, as part of a customer's request for a temporary transaction number, "[t]he customer is prompted by the dialog box to input a password for identification purposes. This password might be the private key...or it may be a separate name or number created by the customer" (Franklin, col. 8, ll. 45-49). The issuing institution then "immediately verifies the identity and authenticity of the customer" (Franklin, col. 8, ll. 57-59).

d) "defining at least one payment category to include at least limiting a number of transactions to one or more merchants"

As discussed previously, "limiting a number of transactions to one or more merchants" is, in effect, non-limiting due to its recitation of "one or more merchants." Taking the broadest reasonable interpretation, the recitation is simply directed towards the defining of at least one payment category. As also stated previously, a payment category is a type of transactions, with different payment categories being a variety of types of transactions (col. 7, ll. 61-63). The '988 Patent provides, as an example, that a payment category may include a single transaction for a specific purchase amount.

Franklin discloses the temporary transaction number capable of being "linked to extra transaction information to ensure that the number is used only for one specific

transaction" (Franklin, col. 2, ll. 48-50). The extra transaction information may include, for instance, a "specific purchase amount," a merchant ID, or a short expiration term on the transaction number (Franklin, col. 2, ll. 50-55). Accordingly, the extra transaction information of Franklin, which may specify a type of transaction (e.g., based on a specific purchase amount), anticipates the payment category of the '988 Patent.

e) "said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants"

As stated above, the "one or more merchants limitation" is in effect a non-limitation. Therefore, this recitation, which includes the "one or more merchants limitation" in said payment category prior to identifying any particular merchant, also becomes a non-limitation. Accordingly, Franklin's disclosure of extra transaction information that may include a merchant ID anticipates defining a payment category as recited in claim 1 of the '988 Patent.

However, as also discussed previously, this recitation, when read with the "defining" manipulative step as a whole, for sake of argument may be read to be limiting such that a payment category must be defined prior to the identification of any particular merchant being included in said payment category. With respect to this interpretation, Franklin discloses that "the transaction number *can* be linked to transaction information" and that "the issuing institution *might* tie the transaction number...to a particular merchant ID" (Franklin, col. 2, ll. 48-52). Therefore, in some embodiments, a payment category may be defined (e.g., for a specific purchase amount) without a particular merchant being identified. Accordingly, Franklin anticipates this recitation of claim 1 of the '988 Patent under either possible interpretation.

f) "designating said payment category"

Franklin discloses that "the issuing institution might tie the transaction number to" extra transaction information (Franklin, col. 2, ll. 50-52). Extra transaction information, as stated above, anticipates the recited payment category. Accordingly, the disclosure of tying the transaction number to extra transaction information anticipates designating a payment category. In addition, Franklin further discloses that in some instances, rather than the issuing institution, the customer may "enter information pertaining to the purchase" which may be used for the issuing bank to then "tie the transaction number to the specific transaction data" (Franklin, col. 10, ll. 1-5). Accordingly, Franklin discloses that a payment category may be designated by either the issuing institution, or alternatively, by the customer.

g) "generating a transaction code by a processing computer of said custodial authorizing entity"

The '988 Patent defines the transaction code as being "pre-coded to be indicative of a specific credit card account" and "to be used in substitution for the credit card number and when utilized as authorized, will issue the merchant a credit approval, and will accomplish payment for the goods or services desired in the normal fashion..." (col. 3, ll. 40-45; col. 6, ll. 33-34).

Franklin discloses that "the issuing bank generates a random temporary transaction number..." (Franklin, col. 4, ll. 50-51). The random temporary transaction number is "associate[d] with the permanent account number" and "looks like a real card number...[t]o the merchant, the transaction number is treated the same as any regular credit card number" (Franklin, col. 2, ll. 15-24).

h) "said transaction code reflecting at least the limits of said designated payment category to make a purchase within said designated payment category"

As stated previously, Franklin discloses that "the transaction number can be linked to extra transaction information," which may include a specific purchase amount, particular merchant ID, or a short expiration term, which are some of the various types of payment categories (Franklin, col. 2, ll. 48-55). Accordingly, the transaction number reflects at least the limits of the designated payment category, as it is linked to the extra transaction information that comprises the payment category. Franklin further discloses that the extra transaction information, which is tied to the transaction number, will be examined "to double check the accuracy of the request," which will allow the transaction number to reflect the limits of the payment category to make a purchase that is within the payment category (Franklin, col. 11, ll. 17-21).

i) "communicating said transaction code to a merchant to consummate a purchase with defined purchase parameters"

The '988 Patent discloses that "the verified customer...will directly or through an authorized representative communicate the code to the merchant..." and that "...the merchant proceeds to consummate the purchase..." (col. 7, ll. 27-28). As stated above, the specification of the '988 Patent does not disclose the term "purchase parameters," and Requester construes the term to include traditional transaction details, such as merchant identification, purchase amount, purchase date and time, etc.

Franklin discloses that "[t]he customer...submits the number to the merchant" (Franklin, col. 2, ll. 17-18). "[T]he merchant computer 30 treats the transaction number of the online commerce card no differently than it treats a standard credit card number..." and "...submits a request for authorization over a payment network 36 to the

bank computing center 32" (Franklin, col. 10, ll. 43-50). The submitting of an authorization request of a standard credit card number is the consummation of a purchase, with defined purchase parameters (e.g., purchase amount) included in the authorization request.

j) "verifying that said defined purchase parameters are within said designated payment category"

As discussed previously, Requester construes the "verifying" step to include verifying that the transaction details of the purchase are in compliance with (e.g., match with) transaction details of the designated payment category. To this end, the '988 Patent discloses communication between the custodial authorizing entity and the merchant for purposes of verification of the transaction code (col. 7, ll. 13-16).

Franklin discloses that "[i]f a record is found, the account manager 60 examines any extra transaction information, such as purchase amount and merchant ID, which is typically included in the authorization request to double check the accuracy of the request" (Franklin, col. 11, ll. 17-21). Accordingly, the account manager verifies that the defined purchase parameters (which are typically included in the authorization request) are within the designated payment category "to double check the accuracy of the request."

k) "providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said designated payment category and to authorize payment required to complete the purchase"

Franklin discloses that "when the bank computer 32 receives the authorization request, it first examines the transaction number to determine whether it is a valid number" (Franklin, col. 10, ll. 61-63). As stated above, examining the transaction

number may include examining extra transaction information to confirm that the defined purchase parameters are within the designated payment category. Franklin further discloses that "[t]he bank computing center 32 then returns the authorization reply to the merchant computer 30" such that "the credit limit of the customer's account is drawn down in the amount of the authorization..." (Franklin, col. 11, ll. 38-45).

Based upon the foregoing, it is apparent that Franklin discloses the method for performing secure credit card purchases as recited in claim 1 of the '988 patent, thereby anticipating the claimed method within the meaning of 35 U.S.C. § 102(b).

ii. Claim 2

"designating at least one of said one or more merchants subsequent to generating said transaction code"

The '988 Patent does not expressly disclose what "designating at least one of said one or more merchants *subsequent* to generating said transaction code" may include. The use of the word "designate" is not defined nor is any definition provided for by context of its use. Furthermore, relevant disclosure in the '988 Patent is unclear as to the possible meaning, as it discloses that "...the customer may designate...that only one merchant, whether designated or not, can use the transaction code" (col. 8, ll. 30-34). In addition to the obvious ambiguity in stating that the customer may designated that a merchant, designated or not, can use the transaction code, there is no indication of how a merchant is designated. Accordingly, based on the accompanying disclosure of the '988 Patent, Requester for sake of the Request, *arguendo,* construes designating at least one of said one or more merchants to include communicating the transaction code to the one or more merchants, which thereby designates the merchant receiving the transaction code as one of the one or more merchants.

Franklin discloses generating a temporary transaction number, which may then be submitted to the merchant (Franklin, col. 2, ll. 15-18). As stated previously, the temporary transaction number in Franklin may be generated without being tied to a particular merchant ID (Franklin, col. 11, ll. 17-21). Accordingly, when the transaction number, which is not tied to a particular merchant, is submitted to a merchant, the merchant is designated with respect to the transaction number. Therefore, Franklin anticipates the recitation of claim 2.

iii. Claims 3 and 20

"wherein said step of communicating the transaction code to a merchant to consummate said purchase within defined purchase parameters further comprises designation of said merchant as one of said one or more merchants"

Claim 3 includes the above recitation and is dependent from claim 1. Claim 20 includes the same recitation, but is instead dependent from claim 19.

As stated above with respect to claim 2, the '988 Patent does not provide a definition as to what "designation of said merchant" may include. Accordingly, Requester construes the step of communicating the transaction code to a merchant to include the designation of said merchant. As also stated previously with respect to claim 2, Franklin discloses generating a temporary transaction number, which may then be submitted to the merchant (Franklin, col. 2, ll. 15-18).

iv. Claim 4

"wherein said step of generating said transaction code further comprises said customer obtaining said transaction code"

Franklin discloses that, after the issuing institution has generated the transaction number, "[t]he customer receives the transaction number..." (Franklin, col. 2, ll. 17-18).

In an additional embodiment, Franklin discloses that "the issuing bank computer 32 sends the transaction number to the customer computer 28..." (Franklin, col. 10, ll. 7-8). In both instances, the customer has obtained the transaction number following generation of said transaction number.

v. Claim 5

"generating a transaction code which reflects at least one of a plurality of said payment categories"

The '988 Patent discloses that the transaction code may be "pre-coded to be indicative of...a designated payment category, selected from the plurality of predetermined payment categories..." (col. 6, ll. 33-36).

Franklin discloses that "the transaction number can be linked to extra transaction information," which represents at least one payment category. Accordingly, by linking the transaction number to the extra transaction information, the issuing institution generates a transaction code that reflects at least one of a plurality of payment categories.

vi. Claim 6

"defining at least one payment category to include amount parameters for a cost of one or more purchases"

Franklin discloses that extra transaction information that may be linked to a transaction number may include "a specific purchase amount" (Franklin, col. 2, ll. 17-21). The "specific purchase amount" is an amount parameter for a cost of a purchase, which may be used to define at least one payment category. Accordingly, Franklin anticipates the recitation of claim 6.

vii. Claim 7

"defining at least one payment category to include time parameters during which the purchase can be completed"

The '988 patent discloses "time parameters during which the purchase can be completed" to be "more specifically...a specific time period, such as twenty four hours, during which authorization of the purchase remains valid" (col. 3, ll. 56-60).

Franklin discloses that the extra transaction information may include "a short expiration term on the transaction number, so that the number becomes invalid after the expiration term lapses" (Franklin, col. 2, ll. 52-55). As such, when the expiration term, the time parameter, has ended, the purchase cannot be completed.

viii. Claim 8

"defining at least one payment category to include limiting said transaction code to a single transaction for a purchase within a predetermined period of time"

Similar to claim 7, above, claim 8 recites a purchase within a predetermined period of time, but additionally limits the transaction code to a single transaction. Franklin discloses that "the transaction number can be linked to extra transaction information to ensure that the number is only used for one specific transaction" (Franklin, col. 2, ll. 48-50).

ix. Claims 15, 27, and 35

"defining at least one payment category to include limiting purchases to a limited time interval during which a purchase is permitted"

Claims 15, 27, and 35 each include the above recitation, and are dependent from claims 1, 21, and 22, respectively.

As discussed above with respect to claim 7, Franklin discloses that extra transaction information may include "a short expiration term on the transaction number, so that the number becomes invalid after the expiration term lapses" (Franklin, col. 2, ll. 52-55). Accordingly, purchases are limited to the limited time interval of the short expiration term.

x. Claim 19

a) "A method of performing secure credit card purchases, said method comprising the steps of:"

As pointed out above with respect to claim 1, Franklin discloses "systems and methods for conducting online transactions using an electronically realizable card that has a private, permanent account number" (Franklin, col. 1, ll. 10-16). An issuing institution generates a temporary transaction number, associated with the permanent account number, for use in a single transaction. "To the merchant, the transaction number is treated the same as any regular credit card number" (Franklin, col. 2, ll. 23-25). The temporary transaction number disclosed in Franklin accomplishes secure credit card purchases.

b) "identifying a pre-established account that is used to make credit card purchases"

Franklin discloses the issuing institution identifying the customer account for an account associated with an online commerce card. Specifically, "[t]he bank computer 32...immediately verifies the identity and authenticity of the customer..." and that "...the number from the credit card or debit card is the customer account number used to identify the data record for the online commerce card" (Franklin, col. 8, ll. 57-59; col. 7, ll. 43-45). Accordingly, the identification of the customer account number and data

record for the card anticipates the identification of a pre-established account used to make credit card purchases.

c) "selecting a pre-determined payment category which limits its nature of a subsequent purchase to one or more merchants"

As discussed previously, limiting the nature of a subsequent purchase to one or more merchants is, in effect, non-limiting due to its recitation of "one or more merchants." Taking the broadest reasonable interpretation, the recitation is simply directed towards the defining of at least one payment category.

As stated with respect to claim 1, Franklin discloses the temporary transaction number capable of being "linked to extra transaction information to ensure that the number is used only for one specific transaction," and thus limiting the nature of a subsequent purchase (Franklin, col. 2, ll. 48-50). The extra transaction information may include, for instance, a merchant ID, which will limit the subsequent purchase to one or more merchants (Franklin, col. 2, ll. 50-55).

d) "said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants"

As discussed with respect to claim 1, this recitation is a non-limitation. If this recitation is construed following a different interpretation than Requester submits as being the broadest reasonable interpretation, then Franklin discloses that "the transaction number *can* be linked to transaction information" and that "the issuing institution *might* tie the transaction number...to a particular merchant ID" (Franklin, col. 2, ll. 48-52). Therefore, in some embodiments, a payment category may be defined (e.g., for a specific purchase amount) without a particular merchant being identified.

Additionally, the tying of a transaction number to a particular merchant ID may not include identifying a particular merchant as one of said one or more merchants, as a particular merchant ID may correspond to a particular merchant industry, or a particular merchant type, while not identifying a specific merchant of the particular merchant industry or type.

e) "generating a transaction code by a processing computer of a custodial authorizing entity of said pre-established account"

As discussed with respect to claim 1, Franklin discloses that "the issuing bank generates a random temporary transaction number..." (Franklin, col. 4, ll. 50-51). The issuing bank anticipates the claimed custodial authorizing entity, as also discussed above.

f) "said transaction code associated with at least said pre-established account and the limits of said selected payment category"

The '988 Patent states that "the transaction code is pre-coded to be indicative of a specific credit card account...and a designated payment category" (col. 6, ll. 33-35).

Similarly, Franklin discloses that the temporary transaction number is generated "and associate[d] with the permanent account..." (Franklin, col. 2, ll. 15-17). Franklin also discloses that the transaction number "can be linked to extra transaction information," which associates the transaction number with the limits of the linked extra transaction information (e.g., purchase amount limits) (Franklin, col. 2, ll. 48-52).

g) "different from said pre-established account"

The '988 Patent discloses that "[t]he transaction code is used in substitution for the specific credit card number which would normally identify a customer's credit card account..." and thus be different from the pre-established account (col. 6, ll. 28-30).

Along these same lines, Franklin discloses that the issuing institution will identify the transaction number as being a transaction number "as opposed to a real customer account number" and that the transaction number is used "as a proxy for the customer account number" during transactions (Franklin, col. 2, ll. 18-20; col. 5, ll. 6-8). As such, Franklin discloses that the transaction number is different from the permanent customer account number.

h) "designating a merchant as one of said one or more merchants"

As discussed with respect to claims 2, 3, and 20, Franklin discloses that a merchant may be designated by the customer "submit[ting] that number to the merchant" (Franklin, col. 2, ll. 18-19) and disclosing that "the transaction number can be linked to transaction information" and that "the issuing institution might tie the transaction number. . . to a particular merchant ID (Franklin, col. 2, ll. 48-52).

i) "communicating said transaction code to said merchant consummate a purchase within defined purchase parameters"

As discussed with respect to the identical recitation in claim 1, although the '988 Patent specification does not use the term "purchase parameters," Franklin discloses that "[t]he merchant 30 receives the transaction number from the Internet and processes the transaction number using its existing computer system" (Franklin, col. 10, ll. 39-41). The submitting of an authorization request of a standard credit card number is the consummation of a purchase, with defined purchase parameters (e.g., purchase amount) included in the authorization request.

j) "verifying that said defined purchase parameters correspond to said selected payment category"

As discussed previously with respect to claim 1's identical recitation, Franklin discloses that "[i]f a record is found, the account manager 60 examines any extra transaction information, such as purchase amount and merchant ID, which is typically included in the authorization request to double check the accuracy of the request" (Franklin, col. 11, ll. 17-21). Accordingly, the account manager verifies that the defined purchase parameters (which are typically included in the authorization request) are within the designated payment category "to double check the accuracy of the request."

k) "providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said selected payment category and to authorize payment required to complete the purchase"

As discussed with respect to this recitation included in claim 1, Franklin discloses that "when the bank computer 32 receives the authorization request, it first examines the transaction number to determine whether it is a valid number" (Franklin, col. 10, ll. 61-63). In addition, examining the transaction number may include examining extra transaction information to confirm that the defined purchase parameters are within the designated payment category. Franklin further discloses that "[t]he bank computing center 32 then returns the authorization reply to the merchant computer 30" such that "the credit limit of the customer's account is drawn down in the amount of the authorization..." (Franklin, col. 11, ll. 38-45).

l) "associating the purchase with said pre-established account"

The '988 Patent does not expressly disclose that the purchase is associated with the pre-established account. However, the '988 Patent does disclose that "the transaction code is pre-coded to be indicative of a specific credit card account," which, if the transaction code is used in the purchase, would enable the purchase to be associated with the specific credit card account (col. 6, ll. 33-34).

Franklin discloses that, as part of the processing of the purchase, "[t]he issuing bank 26 then swaps the customer account number for the transaction number and processes the authorization request..." (Franklin, col. 5, ll. 10-12). Swapping out the transaction number with the customer account number for the authorization of the purchase ensures that the purchase is associated with the specific credit card account. There is further evidence of this association in Franklin, as "the credit limit of the customer's account is drawn down in the amount of the authorization...," which shows the association of the purchase and the customer's account (Franklin, col. 11, ll. 38-45).

Based upon the foregoing, it is apparent that Franklin discloses the method for performing secure credit card purchases as recited in claim 19 of the '988 patent, thereby anticipating the claimed method within the meaning of 35 U.S.C. § 102(b).

xi. Claims 21 and 22

The recitations of claim 22 are identical to the recitations of claim 21, except that where claim 21 recites "a single merchant," claim 22 recites "one or more merchants." However, as noted above, the "one or more merchants" limitation as recited in claim 22, is, in effect, a non-limiter, and thus claim 22 is directed to the same method of claim 21, but without the limitation of "a single merchant" in accordance with the broadest reasonable interpretation.

a) "A method for implementing a system for performing secure credit card purchases, the method comprising:"

As pointed out above with respect to claims 1 and 19, Franklin discloses "systems and methods for conducting online transactions using an electronically realizable card that has a private, permanent account number" (Franklin, col. 1, ll. 10-16). An issuing institution generates a temporary transaction number, associated with the permanent account number, for use in a single transaction. "To the merchant, the transaction number is treated the same as any regular credit card number" (Franklin, col. 2, ll. 23-25).

b) "receiving account information from an account holder identifying an account that is used to make credit card purchases"

Franklin discloses that "the customer is prompted to input a password for identification purposes. The password might be a private key or it may be a separate name or number created by the customer" (Franklin, col. 8, ll. 45-49). Following the providing of information from the customer, "[t]he bank computer...immediately verifies the identity and authenticity of the customer..." (Franklin, col. 8, ll. 57-59). Accordingly,

the issuing institution receives information from the account holder to identify an account.

As stated above with respect to claim 19, the verification of the identity of the customer includes identifying the customer account number, which is used to identify the account for the online commerce card, which is used to make credit card purchases (Franklin, col. 7, ll. 43-45).

c) "receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant"

As stated above, this recitation as included in claim 22, is directed to limiting transactions to "one or more merchants" rather than the "a single merchant" recited in claim 21.

In Franklin, the customer may "...send a request to the issuing institution to issue a transaction number..." (Franklin, col. 2, ll. 13-14). The transaction number, as stated above, can be linked to extra transaction information. In order to determine this information, as part of the request to issue a transaction number, the customer may "enter information pertaining to the purchase, like the purchase price, the model or item number, the merchant name, and the like" (Franklin, col. 10, ll. 1-3). Accordingly, this results in the transaction number being for a purchase within a specified payment category. If the customer supplies the merchant name, then the transactions would be limited to a single merchant. Alternatively, the extra transaction information might include the extra transaction information "to ensure that the number is only used for one specific transaction," which would limit the transaction number to a single merchant (Franklin, col. 2, ll. 48-50).

d) "said single merchant limitation being included in said payment category prior to any particular merchant being identified as said single merchant"

As stated above, claim 22 includes this recitation, but directed toward the limitation being included prior to any particular "one or more merchant" being identified. As discussed with respect to claims 1 and 19, this recitation is non-limiting and thus, under the broadest reasonable interpretation, the transaction code would be for making a purchase within a designated payment category, without regard to merchant limitations. Under an alternative interpretation, *arguendo,* as also discussed previously, the transaction code would be within a designated payment category prior to the designation of any merchant.

As to the recitation as it appears in claim 21, the '988 Patent specification does not include any language directed towards "limit[ing] a transaction to a single merchant...prior to any particular merchant being identified as said single merchant" to provide for context and understanding of the recitation. Requester construes the recitation to include requiring that a transaction code only being used at one merchant as opposed to multiple merchants, and that the limitation is imposed prior to any particular merchant being identified as the one merchant.

Franklin discloses that the transaction number might be tied to a particular merchant ID (Franklin, col. 2, ll. 51-52). In instances where the transaction number is not tied to a particular merchant ID, then the single merchant limitation, as discussed above, would be included prior to the identification of a particular merchant.

e) "generating a transaction code utilizing a processing computer of a custodial authorizing entity, said transaction code associated with said account"

As discussed with respect to claims 1 and 19, Franklin discloses that "the issuing bank generates a random temporary transaction number..." (Franklin, col. 4, ll. 50-51). The issuing bank anticipates the claimed custodial authorizing entity, as also discussed above. Franklin also discloses that the temporary transaction number is generated "and associate[d] with the permanent account..." (Franklin, col. 2, ll. 15-17).

f) "reflecting at least the limits of said payment category, to make a purchase within said payment category"

As discussed previously with respect to claim 19, Franklin discloses that the transaction number "can be linked to extra transaction information," which associates the transaction number with the limits of the linked extra transaction information (e.g., purchase amount limits), which would make the purchase using the transaction number within the payment category (Franklin, col. 2, ll. 48-52).

g) "communicating said transaction code to said account holder"

Franklin discloses that "the issuing bank 26 issues the transaction number to the customer..." (Franklin, col. 4, ll. 53-54). In one embodiment, the transaction number may be communicated to the customer (the account holder) when "...the issuing bank computer 32 sends the transaction number to the customer computer 28" (Franklin, col. 10, ll. 7-8).

h) "receiving a request to authorize payment for a purchase using said transaction code"

Although the '988 Patent does not disclose the receipt of an authorization request for authorizing payment for a purchase using said transaction code, it does disclose

communication between the merchant and the custodial authorizing entity for obtaining verification and subsequent payment using the transaction code (col. 7, ll. 49-55). Based on the foregoing, Requester construes this recitation to include receiving an authorization request for a transaction, such as between the merchant and the custodial authorizing entity, as is consistent with the specification of the '988 Patent.

Along these lines, Franklin discloses that "the bank computer 32 receives the authorization request" from the merchant, and that upon receiving the request, "it first examines the transaction number..." (Franklin, col. 10, ll. 61-62). Thus, the issuing institution receives a request to authorize payment for a purchase using the transaction number.

i) "authorizing payment for said purchase if said purchase is within said payment category"

As discussed previously with respect to the "verifying" step of claims 1 and 19, Franklin discloses that "the account manager 60 examines any extra information, such as purchase amount and merchant ID...to double check the accuracy of the request," which will identify if the purchase is within the payment category (Franklin, col. 11, ll. 17-21). If the authorization request is successful, payment is authorized in the form of drawing down the credit limit of the customer's account (Franklin, col. 11, ll. 41-45).

xii. Claims 23 and 31

"wherein the step of receiving account information from the account holder identifying an account that is used to make credit card purchases further comprises receiving information identifying a credit card account"

Claims 23 and 31 each contain this recitation, and are directed to claims 21 and 22, respectively.

As stated above with respect to claims 21 and 22, Franklin discloses that "[t]he bank computer...immediately verifies the identity and authenticity of the customer..." using the provided information, and that the identified customer is associated with a credit card account (Franklin, col. 8, ll. 57-59). Accordingly, the information received from the account holder identifying an account is information that can therefore identify a credit card account.

xiii. Claims 24 and 32

"wherein the step of generating a transaction code utilizing a processing computer of a custodial authorizing entity further comprises generating a transaction code which reflects at least one of a plurality of predetermined payment categories"

Claims 24 and 32 each contain this recitation, and are directed to claims 21 and 22, respectively.

Franklin discloses generating a temporary transaction number where "the transaction number can be linked to extra transaction information..." (Franklin, col. 2, ll. 48-52). The extra transaction information may include a specific purchase amount, a particular merchant ID, a short expiration time, etc., or combinations thereof, each of which represent a predetermined payment category. Accordingly, as the transaction number can be linked to the information, it may reflect at least one of the plurality of predetermined payment categories.

xiv. Claims 29 and 37

"wherein said step of receiving a request to authorize payment for a purchase using said transaction code further identifies said single merchant"

Claims 29 and 37 each contain this recitation, and are directed to claims 21 and 22, respectively.

As stated above with respect to the "receiving a request" step of claims 21, and 22, Franklin discloses that "the bank computer 32 receives the authorization request" from the merchant (Franklin, col. 10, ll. 61-62). Furthermore, Franklin discloses that merchant identification is among the information typically included in the authorization request (Franklin, col. 11, ll. 18-22). Accordingly, receipt of the authorization request identifies the single merchant.

xv. Claims 30 and 38

"wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant further comprises receiving a request from said account holder for a transaction code to make a purchase within a predetermined payment category that is further limited in accordance with transaction details provided by said account holder"

Claims 30 and 38 each contain this recitation, and are directed to claims 21 and 22, respectively.

Although the '988 Patent specification does not disclose that transaction details are to be provided by the account holder, but are rather established by the custodial authorizing entity (see col. 7, ll. 43-45), Franklin discloses that the issuing institution "may require the customer to enter information pertaining to the purchase, like the purchase price, the model or item number, the merchant name, and the like" (Franklin, col. 9, ln. 66 - col. 10, ln. 3). This information is linked to the generated transaction number, such that the transaction number may only be used for a transaction in accordance with the provided extra transaction information (Franklin, col. 9, ll. 63-66).

Conclusion

Based on the foregoing, Franklin discloses the methods for performing and for implementing a system for performing secure credit card purchases as claimed in the '988 Patent, and anticipates the subject matter claimed in each of claims 1-8, 15, 19-24, 27, 29-32, 35, and 37-38 of the '988 Patent under 35 U.S.C. § 102(b).

D. Claims 16, 25, 28, 33, and 36 would have been obvious under 35 U.S.C. § 103(a) over Franklin

Set forth below is a detailed explanation of the obviousness of each of claims 16, 25, 28, 33, and 36 under 35 U.S.C. § 103(a) over Franklin.

i. Claims 16, 28, and 36

"communicating said transaction code to the customer at the location of the merchant for use in person"

Claims 16, 28, and 36 each include the above recitation and are dependent from claims 1, 21, and 22, respectively.

Franklin discloses that "[t]he customer receives the transaction number and submits the number to the merchant..." (Franklin, col. 2, ll. 17-18). Although Franklin is directed towards the use of transaction numbers in online commerce and does not expressly disclose use of the transaction number in person, it would have been obvious to a person having ordinary skill in the art at the time of the invention of the '988 Patent to take the transaction number of Franklin, which looks like and is used as a real credit card number, to perform the communication of the transaction code to the customer at the location of the merchant for use in person.

ii. Claims 25 and 33

"wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant further comprises receiving a request from said account holder for a transaction code to make a purchase within a payment category that is automatically chosen by a custodial authorizing entity"

Claims 25 and 33 each include the above recitation and are dependent from claims 21 and 22, respectively.

As discussed previously, Franklin discloses that the customer may request a transaction code to make a purchase within a payment category, and may additionally "enter information pertaining to the purchase, like the purchase price the model or item number, the merchant name, and the like" (Franklin, col. 9, ll. 1-3). It would have been obvious for a person having ordinary skill in the art to take the system of Franklin, where the customer may submit extra transaction information along with a request for a transaction code, and have the issuing institution automatically chose a payment category (e.g., based on the submitted extra information). As payment categories are used in the authorization process, to ensure a transaction is within the payment category, it makes sense that the issuing institution would automatically chose the payment category based on provided information in the request, rather than the customer.

Based on the foregoing, it is apparent that claims 16, 25, 28, 33, and 36 would have been obvious under 35 U.S.C. § 103(a) over Franklin.

E. Claims 17 and 18 would have been obvious under 35 U.S.C. § 103(a) over Franklin in view of Joao

Set forth below is a detailed explanation of the obviousness of each of claims 17 and 18 under 35 U.S.C. § 103(a) over Franklin in view of Joao.

i. Claim 17

Claim 17 is identical to claim 19, discussed in detail above, except for the recitation of the "selecting a predetermined payment category" step. In claim 19, the step recited that the predetermined payment category limits the nature of a "subsequent purchase" to one or more merchants, whereas, in claim 17, the step recites that the predetermined payment category limits the nature "of a series of subsequent purchases" to one or more merchants.

As discussed above with respect to claim 19, Franklin discloses that the extra transaction information may limit the nature of a subsequent purchase, but is directly to a "single transaction" and not a "series of subsequent purchases." Joao discloses placing limitations and/or restrictions on the use of a card, which may include "the type of transactions which are allowed and/or authorized" or "the dollar amounts of transactions pertaining to each authorized vendor" (Joao, col. 16, ll. 18-30). Accordingly, Joao discloses a plurality of payment categories that may limit the nature of a *series* of subsequent purchases, as it is directed towards restrictions and/or limitations on multiple transactions.

It would have been obvious to a person having ordinary skill in the art at the time of the invention of the '988 Patent to take the method of Franklin, which selects a predetermined payment category limiting the nature of a single purchase, and modify it to be used for a series of subsequent purchases in light of Joao's teaching of limitations

on the nature of multiple transactions, and arrive at the invention as claimed in claim 17 of the '988 Patent.

ii. Claim 18

Franklin discloses that, as part of the authorization process of the purchase, the purchase including defined purchase parameters (e.g., transaction details), "the account manager 60 examines any extra transaction information, such as purchase amount and merchant ID...to double check the accuracy of the request" (Franklin, col. 11, ll. 17-21). Accordingly, verifying that the defined purchase parameters correspond to said payment category includes a merchant ID, which thereby identifies the merchant, as recited in claim 18.

Based on the foregoing, it is apparent that claims 17 and 18 would have been obvious under 35 U.S.C. § 103(a) over Franklin in view of Joao.

F. Claims 9-14, 26, and 34 would have been obvious under 35 U.S.C. § 103(a) over Franklin in view of Yanagihara

Set forth below is a detailed explanation of the obviousness of each of claims 17 and 18 under 35 U.S.C. § 103(a) over Franklin in view of Yanagihara.

i. Claim 9

"defining at least one payment category to include limiting purchases to a single transaction at a maximum amount for purchase within a predetermined period of time"

As discussed above, Franklin discloses that "the transaction number can be linked to extra transaction information to ensure the number is only used for one specific transaction" (Franklin, col. 2, ll. 48-50). Franklin also discloses that the extra transaction

information may include a specific purchase amount and within a predetermined period of time, but does not include a maximum amount for purchase.

Yanagihara discloses that a usable limit may be placed on the electronic money card, "the usable limit indicat[ing] the maximum limit of electronic money the user can withdraw" (Yanagihara, para. [0019]). It would have been obvious for a person having ordinary skill in the art at the time of the invention of the '988 Patent to take the extra transaction information of Franklin and include a maximum limit as taught by Yanagihara. In some instances a specific purchase amount may be difficult to ascertain prior to the transaction, such as the purchase of a service where a tip may be added to the price. Using the maximum limit of Yanagihara in addition to the predetermined period of time of Franklin would ensure that such transactions could still be processed, while still allowing for account security.

ii. Claim 10

"defining at least one payment category to include limiting purchases to at least one payment category to at least two purchases at a maximum total amount for items purchased within a predetermined period of time"

Claim 10 includes the same recitation of claim 9, but is directed towards "at least two purchases" at a maximum total amount, rather than the "single transaction" recited in claim 9.

As discussed above, Franklin is directed to a single transaction during a predetermined period of time, but not disclose limiting at least two purchases to a maximum total amount. As also discussed previously, Yanagihara discloses a usable limit for a maximum total amount for a transaction. In addition, Yanagihara also discloses an aggregate amount, which applies for multiple (e.g., at least two)

purchases, such that a purchase amount is not only "compared with the usable limit, but also the sum of the amount of money currently withdrawn and the aggregate amount of money so far paid" (Yanagihara, para. [0029]).

It would have been obvious at the time of the invention of the '988 Patent for a person having ordinary skill in the art to combine the teachings of Franklin and Yanagihara to define a payment category limiting at least two purchases to a maximum total amount within a predetermined period of time.

iii. Claims 11 and 12

"defining at least one payment category to include using said transaction code for at least two purchases for a repeating transaction at a fixed amount payable at each of a fixed number of time intervals"

As discussed above with respect to claim 1, Franklin teaches defining at least one payment category to include using a transaction code, but does not disclose using the transaction code for at least two purchases for a repeating transaction at a fixed amount payable at each of a fixed number of time intervals.

Yanagihara discloses that payment conditions may be placed on an electronic money card that may limit multiple transactions using the electronic money card (Yanagihara, para. [0019]). Yanagihara also discloses that for each transaction, transaction details (e.g., purchase parameters) may be captured and stored, including "a transaction date 224, a transaction category 225, an amount transacted 226, and a usage category 227. The transaction date 224 indicates the year, month and day in which the electronic money is read and written" (Yanagihara, para. [0020]).

Yanagihara is directed to an electronic money card that the cardholder may share with others, the card having limits and payment conditions such that the other

users must stay within the limits agreed upon (Yanagihara, para. [0003]). It would have been obvious for a person having ordinary skill in the art to use the usage limits and transaction record of Yanagihara to limit purchases for a repeating transaction at a fixed amount payable at each of a fixed number of time intervals. It would also have been obvious for a person having ordinary skill in the art to combine these teachings of Yanagihara regarding limits for users (e.g., merchants) withdrawing from an electronic money card, to the teachings of Franklin regarding limits for a transaction from a transaction number, and achieve the invention as claimed in claim 11 of the '988 Patent.

Claim 12 is dependent from claim 11, and recites a payment category limiting purchases to the repeating transaction recited in claim 11. Accordingly, for the same reasons as discussed with respect to claim 11, claim 12 would have been obvious to a person having ordinary skill in the art based on the teachings of Franklin and Yanagihara.

iv. Claim 13

"defining at least one payment category to include using said transaction code for a repeating transaction at a fixed amount payable to each of an unspecified number of time intervals"

Claim 13 includes a recitation identical to that of claim 12, except that the number of time intervals recited in claim 13 is unspecified.

As discussed above, it would have been obvious to a person having ordinary skill in the art to combine the teachings of Franklin and Yanagihara to achieve a method for performing secure credit card purchases including defining a payment category to include using a transaction code for a repeating transaction at a fixed amount payable for a fixed number of time intervals. Accordingly, it would also be obvious to a person

having ordinary skill in the art to modify the method to include defining the payment category to include using a transaction code for a repeating transaction for an unfixed number of time intervals. Yanagihara is directed towards allowing a cardholder to provide users with their electronic money card for withdrawals (e.g., charges) with various payment conditions. It would be obvious for a cardholder to provide a merchant with their card for charging a fixed amount payable at a time interval, such as for a monthly fee for a service (e.g., cable, television, landscaping, mortgage payments, etc.). In some instances, there may be a fixed number of time intervals, such as for a one year subscription to a service, while in many others, the number of intervals is unspecified, such as for a utility. Accordingly, it would be obvious for a person having ordinary skill in the art to combine the teachings of Franklin and Yanagihara to achieve the invention as recited in claim 13 of the '988 Patent.

v. Claims 14, 26, and 34

"defining at least one payment category to include limiting a repeating transaction to a maximum dollar amount"

Claims 14, 26, and 34 each include the above recitation and are dependent from claims 1, 21, and 22, respectively.

As discussed previously with respect to claims 11-13, Yanagihara discloses setting payment conditions including a maximum dollar amount and the storage of transaction details, including a "usage identification code" that "indicates what purpose a user uses the electronic money card 106 for" (Yanagihara, para. [0019-0020]). Accordingly, it would be obvious to a person having ordinary skill in the art to modify the teachings of Yanagihara to set payment conditions for a repeating transaction based on transaction details, such as the usage identification code, usage category, etc., such

that a merchant could be provided the electronic money card number for repeated withdrawals without exceeding a maximum usage limit per transaction or aggregate limit per all transactions.

Based on the foregoing, it is apparent that claims 9-14, 26, and 34 would have been obvious under 35 U.S.C. § 103(a) over Franklin in view of Yanagihara.

III. CONCLUSION

Based on the above-identified prior art and the arguments herein, the Office should declare that there are substantial new questions of patentability with respect to claims 1-38 of the '988 Patent, and that claims 1-38 should be rejected as anticipated under 35 U.S.C. § 102(e), or, alternatively, that claims 1-8, 15, 19-24, 27, 29-32, 35, and 37-38 should be rejected as anticipated under 35 U.S.C. § 102(b) and that claims 9-14, 16-18, 25-26, 28, 33-34, and 36 should be rejected as obvious under 35 U.S.C. § 103(a) for at least the reasons identified above.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: September 12, 2012 By: _____

Charles F. Wieland III
Registration No. 33,096

Customer No. 21839
703 836 6620

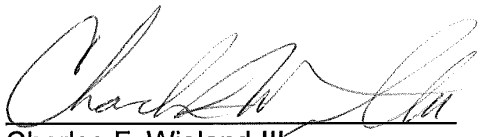
CERTIFICATE OF SERVICE

It is hereby certified by the undersigned that a true copy of the Request for *Ex Parte* Reexamination, and all attachments, filed on September 12, 2012 was mailed via courier to:

Stephen J. Lewellyn, Esq.
Maxey Law Offices, PLLC
15500 Roosevelt Boulevard, Suite 305
Clearwater, Florida 33760

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: September 12, 2012 By: 

Charles F. Wieland III
Registration No. 33096

Customer No. 21839
703 836 6620

Appendix A – '988 Patent Claims and Written Description versus Cohen

'988 Patent Claims	Closest Explanation in '988 Patent	Disclosure in Cohen (6,422,462)
1. A method of performing secure credit card purchases, said method comprising:	"...the present invention is directed towards a system and method for accomplishing secure credit card purchases" (col. 5, ll. 28-30).	"It is an object of the present invention to provide improved credit cards and methods for credit card transactions...[i]t is a further object of the present invention to provide methods and apparatus for secure transmission of credit card information" (Cohen, col. 1, ll. 48-62).
a) contacting a custodial authorizing entity having custodial responsibility of account parameters of a customer's account that is used to make credit card purchases;	"...the customer contacts, either by computer, telephone, or in person, a custodial authorizing entity as at 12. The custodial authorizing entity may herein be defined as comprising that entity or institution which has or has been designated by the entity which has custodial responsibility for the financial data and security of a given credit card account of a customer" (col. 5, ll. 51-57).	"...a user dials into her credit card company..." (Cohen, col. 3, ll. 42-44).
b) supplying said custodial authorizing entity with at least account identification data of said customer's account;	"Once contacted, the customer then supplies appropriate identification data to inform the custodial authorizing entity of a specific customer's credit card account as at 15" (col. 5, ln. 66 - col. 6, ln. 2).	"...a user dials into her credit card company...and after providing the ordinary credit card number and verification data..." (Cohen, col. 3, ll. 42-45).
c) defining at least one payment category to include at least limiting a number of transactions to one or more merchants,	[In light of this recitation, the claims are limited to the embodiment described at col. 8, ll. 18-34.] "The payment category may also include a multi-transaction authorization wherein more than one purchase may be made from one or a plurality of different merchants..." (col. 8, ll. 18-20).	"The card can also be customized for only particular uses or groups of uses" (Cohen, col. 7, ll. 66-67). "A customized credit card could be issued to the user which is only valid for use for that particular type of charge (computer hardware or software stores)...[or] for use in a particular store itself or a particular chain of stores" (Cohen, col. 8, ll. 25-34).
said one or more merchants limitation	"...each of which may or may not be	"A customized credit card could be issued

being included in said payment category prior to any particular merchant being identified as one of said one or more merchants;	identified by the customer and pre-coded in associated with the transaction code" (col. 8, ll. 19-22).	to the user which is only valid for use for that particular *type* of charge (computer hardware or software stores)..." (Cohen, col. 8, ll. 25-28) (emphasis added).
d) designating said payment category;	"Further, a feature of the transaction code is its ability to indicate any one of preferably a plurality of predetermined payment categories which may either be requested by the customer or automatically chosen by the custodial authorizing entity..." (col. 3, ll. 48-52).	"...a user can indicate in advance of purchase...what the single use or the customized credit card number is to be used for" (Cohen, col. 3, ll. 49-52).
e) generating a transaction code by a processing computer of said custodial authorizing entity,	"...the custodial authorizing entity generates a transaction code as at 20" (col. 6, ll. 26-28).	"A user dials into her credit card company before making a transaction, and...is provided with a disposable or customized number" (Cohen, col. 3, ll. 41-45). "These credit cards or credit card numbers are generated..." (Cohen, col. 2, ll. 35-36).
said transaction code reflecting at least the limits of said designated payment category to make a purchase within said designated payment category;	"...a merchant identifier is pre-coded in associate within the transaction code, the pre-coding of the transaction code will prohibit an unauthorized use due at least in part to the fact that the merchant is specifically identified and any attempt to use the transaction code other than by the identified merchant will be prohibited" (col. 7, ll. 1-6).	"A customized credit card could be issued to the user which is only valid for use for that particular type of charge" (Cohen, col. 8, ll. 25-27). "A customized credit card...is only valid for use for that particular type of charge...such that if the employee tries to use it for anything else...the charge will be declined" (Cohen, col. 8, ll. 25-32)
f) communicating said transaction code to a merchant to consummate a purchase with defined purchase parameters;	"The verified customer...will directly or through an authorized representative communicate the code to the merchant as at 24" (col. 6, ll. 44-48). "...the merchant proceeds to consummate the purchase..." (col. 7, ll. 27-28).	"...the user transmits his or her credit card information to the vendor. That vendor then verifies the transaction..." (Cohen, col. 5, ll. 36-37).
g) verifying that said defined purchase parameters are within said	Inferred, but not directly supported, by the specification. See, col. 7, ll. 13-16	"That vendor then verifies the transaction..." (Cohen, col. 5, ln. 37).

designated payment category; and	("Restricted communication between the merchant and the custodial authorizing entity as at 26 is permitted exclusively for purposes of verification of the transaction code...").	"A customized credit card...is only valid for use for that particular type of charge...such that if the employee tries to use it for anything else...the charge will be declined" (Cohen, col. 8, ll. 25-32)
h) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said designated payment category and to authorize payment required to complete the purchase.	No direct support found in specification. See, col. 7, ll. 18-22 ("As a result, the merchant also has a desired verification as to the validity of a transaction and can effectively make arrangements to be paid by the credit card company").	"...the credit card company notes the identity of the vendor, authorizes the transaction (if the credit card number is valid and the purchaser has sufficient funds available), and forwards the authorization code to the vendor" (Cohen, col. 5, ll. 45-49).
2. The method of claim 1 further comprising the step of designating at least one of said one or more merchants subsequent to generating said transaction code.	"...the customer may designate...that only one merchant, whether designated or not, can use the transaction code" (col. 8, ll. 30-34).	"...the user transmits his or her credit card information to the vendor" (Cohen, col. 5, ll. 36-37).
3. The method of claim 1 wherein said step of communicating the transaction code to a merchant to consummate said purchase within defined purchase parameters further comprises designation of said merchant as one of said one or more merchants.	"The verified customer...will directly or through an authorized representative communicate the code to the merchant as at 24" (col. 6, ll. 44-48). "...the merchant proceeds to consummate the purchase..." (col. 7, ll. 27-28).	"Upon use of the card, the information regarding the transaction is transmitted to the credit card company, as is known in the art" (Cohen, col. 13, ln. 66-col. 14, ln. 1) where merchant identification in transaction details is known in the art.
4. The method of claim 1 wherein said step of generating said transaction code further comprises said customer obtaining said transaction code.	"Once generated, the transaction code is communicated exclusively to the authorized and verified customer by the custodial authorizing entity as at 22" (col. 6, ll. 37-39).	"...a user...is provided with a disposable or customized number..." (Cohen, col. 3, ll. 43-45).
5. The method of claim 1 further comprising generating a transaction code which reflects at least one of a plurality of said payment categories.	"...the transaction code is pre-coded to be indicative of...a designated payment category, selected from the plurality of predetermined payment categories..." (col. 6, ll. 33-36).	"The card can also be customized for only particular uses or groups of uses" (Cohen, col. 7, ll. 66-67).
6. The method of claim 1 further comprising defining at least one payment category to include amount parameters for	"More specifically, the plurality of payment categories may include a single transaction involving a specific dollar	"A customized credit card could be issued to the user which is only valid...to the credit limit decided by the issuer or [user]..."

a cost of one or more purchases.	amount for a purchase..." (col. 3, ll. 56-58).	(Cohen, col. 8, ll. 25-30).
7. The method of claim 1 further comprising defining at least one payment category to include time parameters during which the purchase can be completed.	"More specifically, the plurality of payment categories may include...a specific time period, such as twenty four hours, during which authorization of the purchase remains valid." (col. 3, ll. 56-60).	"...each of the disposable credit cards can be given an expiration date...[t]hus, if the credit card is not used within the time limit, it expires" (Cohen, col. 6, ll. 4-7).
8. The method of claim 1 further comprising defining at least one payment category to include limiting said transaction code to a single transaction for a purchase within a predetermined period of time.	"More specifically, the plurality of payment categories may include a single transaction...for a purchase within a specific time period, such as twenty four hours, during which authorization of the purchase remains valid." (col. 3, ll. 56-60).	"With respect to the disposable card, the user is instructed that, after use of the number once, the number may not be used again" (Cohen, col. 3, ll. 60-62). "It could also be valid for a specific predetermined amount of time" (Cohen, col. 7, ll. 61-62).
9. The method of claim 1 further comprising defining at least one payment category to include limiting purchases to a single transaction at a maximum amount for purchase within a predetermined period of time.	"More specifically, the plurality of payment categories may include a single transaction involving a specific dollar amount for a purchase within a specific time period..." (col. 3, ll. 56-59).	"The card could be valid only for purchase on that particular day, to a certain designated purchase limit, and even, if desired only in a certain store" (Cohen, col. 8, ll. 43-45).
10. The method of claim 1 further comprising defining at least one payment category to include limiting purchases to at least one payment category to at least two purchases at a maximum total amount for items purchased within a predetermined period of time.	"Other alternatives would involve one or more of the categories coded to define multiple transactions involving a maximum dollar amount for purchases, as well as a fixed period of time for authorization of such purchases..." (col. 3, ln. 65 to col. 4, ln. 1).	"The card could be valid only for purchase on that particular day, to a certain designated purchase limit, and even, if desired only in...groups of stores or types of stores, or types of purchases or items" (Cohen, col. 8, ll. 43-47).
11. The method of claim 1 further comprising defining at least one payment category to include using said transaction code for at least two purchases for a repeating transaction at a fixed amount payable at each of a fixed number of time intervals.	"Other alternatives would involve one or more of the categories coded to define...a repeating transaction wherein payments may be automatically accessed by a merchant over a predetermined or unspecified time interval (such as every thirty days) for a specific dollar amount or a maximum dollar amount limit" (col. 3, ln. 65 to col. 4, ln. 5).	"Thus, in accordance with these embodiments, the card can have a user customized range of dates or series of dates" (Cohen, col. 7, ll. 44-46). "It could also be valid for a specific predetermined amount of time" (Cohen, col. 7, ll. 61-62). "The card could be valid only for purchase on that particular day, to a certain designated purchase limit..." (Cohen, col. 8, ll. 43-45).
12. The method of claim 11 further	"Other alternatives would involve one or	"A customized credit card...is only valid for

comprising defining at least one payment category to include limiting purchases to said repeating transaction at said fixed amount payable at each of said fixed number of time intervals.	more of the categories coded to define...a repeating transaction wherein payments may be automatically accessed by a merchant over a predetermined or unspecified time interval (such as every thirty days) for a specific dollar amount or a maximum dollar amount limit" (col. 3, ln. 65 to col. 4, ln. 5).	use for that particular type of charge...such that if the employee tries to use it for anything else...the charge will be declined" (Cohen, col. 8, ll. 25-32).
13. The method of claim 1 further comprising defining at least one payment category to include using said transaction code for a repeating transaction at a fixed amount payable to each of an unspecified number of time intervals.	"Similarly, a repeating transaction for a stated minimum interval, such as every thirty days may be authorized for a specific amount for an unspecified number of intervals..." (col. 8, ln. 43-45).	"Thus, in accordance with these embodiments, the card can have a user customized range of dates or series of dates" (Cohen, col. 7, ll. 44-46) where the series of dates need not have an end.
14. The method of claim 1 further comprising defining at least one payment category to include limiting a repeating transaction to a maximum dollar amount.	"Other alternatives would involve one or more of the categories coded to define...a repeating transaction ...for a specific dollar amount or a maximum dollar amount limit" (col. 3, ln. 65 to col. 4, ln. 5).	"Thus, in accordance with these embodiments, the card can have a user customized range of dates or series of dates" (Cohen, col. 7, ll. 44-46). "A customized credit card could be issued to the user which is only valid...to the credit limit decided by the issuer or [user]..." (Cohen, col. 8, ll. 25-30).
15. The method of claim 1 further comprising defining at least one payment category to include limiting purchases to a limited time interval during which a purchase is permitted.	"In addition, the transactions are preferably, but not necessarily, authorized to be conducted only over a fixed life period of time..." (col. 8, ll. 6-8).	"...each of the disposable credit cards can be given an expiration date...[t]hus, if the credit card is not used within the time limit, it expires" (Cohen, col. 6, ll. 4-7).
16. The method of claim 1 further comprising communicating said transaction code to the customer at the location of the merchant for use in person.	"...the present invention is directed towards a system and method for accomplishing secure credit card purchases. Moreover, these purchases can be 'in person'..." (col. 5, ll. 28-31).	"The vendor could read the number of the disposable or customized card, could scan the number with a bar code scanner, could read a magnetic strip on the disposable card, or so forth" (Cohen, col. 4, ll. 31-35).
17. A method of performing secure credit card purchases, said method comprising:	"...the present invention is directed towards a system and method for accomplishing secure credit card purchases" (col. 5, ll. 28-30).	"It is an object of the present invention to provide improved credit cards and methods for credit card transactions...[i]t is a further object of the present invention to provide methods and apparatus for secure transmission of credit card information"

		(Cohen, col. 1, ll. 48-62).
a) identifying a pre-established account that is used to make credit card purchases;	"...the custodial authorizing entity verifies the credit card status and account identification of the customer..." (col. 6, ll. 15-17).	"...a user dials into her credit card company before making a transaction, and after providing the ordinary credit card number and verification data..." (Cohen, col. 3, ll. 42-45).
b) selecting a predetermined payment category which limits its a nature, of a series of subsequent purchases to one or more merchants,	"The payment category may also include a multi-transaction authorization wherein more than one purchase may be made from one or a plurality of different merchants..." (col. 8, ll. 18-20).	"...a user can indicate in advance of purchase...what the single use or the customized credit card number is to be used for" (Cohen, col. 3, ll. 49-52). "A customized credit card could be issued to the user which is only valid for use for that particular type of charge (computer hardware or software stores)...[or] for use in a particular store itself or a particular chain of stores" (Cohen, col. 8, ll. 25-34).
said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants;	"...each of which may or may not be identified by the customer and pre-coded in associated with the transaction code" (col. 8, ll. 19-22).	"A customized credit card could be issued to the user which is only valid for use for that particular *type* of charge (computer hardware or software stores)..." (Cohen, col. 8, ll. 25-28) (emphasis added).
c) generating a transaction code by a processing computer of a custodial authorizing entity of said pre-established account,	"...the custodial authorizing entity generates a transaction code as at 20" (col. 6, ll. 26-28).	"A user dials into her credit card company before making a transaction, and...is provided with a disposable or customized number" (Cohen, col. 3, ll. 41-45). "These credit cards or credit card numbers are generated..." (Cohen, col. 2, ll. 35-36).
said transaction code associated with at least said pre-established account and the limits of said selected payment category	"...the transaction code is pre-coded to be indicative of a specific credit card account, preferably a merchant or merchants identification and a designated payment category" (col. 6, ll. 33-35).	"A customized credit card could be issued to the user which is only valid for use for that particular type of charge" (Cohen, col. 8, ll. 25-27). "...the credit card can be marked, if desired, to show both that it has been processed to charge money to the person's account..."

		(Cohen, col. 4, ll. 36-38), showing the association of the card with the pre-established account.
and different from said pre-established account;	"The transaction code is used in substitution for the specific credit card number which would normally identify a customer's credit card account..." (col. 6, ll. 28-30).	"No vendor would ever, under one embodiment of the system, receive or have access to the user's permanent credit card number. Rather, the vendor would receive a disposable credit card number from the user's supply" (Cohen, col. 4, ll. 26-31).
d) communicating said transaction code to a merchant to consummate a purchase within defined purchase parameters;	"The verified customer...will directly or through an authorized representative communicate the code to the merchant as at 24" (col. 6, ll. 44-48). "...the merchant proceeds to consummate the purchase..." (col. 7, ll. 27-28).	"...the user transmits his or her credit card information to the vendor. That vendor then verifies the transaction..." (Cohen, col. 5, ll. 36-37).
e) verifying that said defined purchase parameters correspond to said selected payment category;	Inferred, but not directly supported, by the specification. See, col. 7, ll. 13-16 ("Restricted communication between the merchant and the custodial authorizing entity as at 26 is permitted exclusively for purposes of verification of the transaction code...").	"That vendor then verifies the transaction..." (Cohen, col. 5, ln. 37). "A customized credit card...is only valid for use for that particular type of charge...such that if the employee tries to use it for anything else...the charge will be declined" (Cohen, col. 8, ll. 25-32)
f) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said selected payment category and to authorize payment required to complete the purchase; and	No direct support found in specification. See, col. 7, ll. 18-22 ("As a result, the merchant also has a desired verification as to the validity of a transaction and can effectively make arrangements to be paid by the credit card company").	"...the credit card company notes the identity of the vendor, authorizes the transaction (if the credit card number is valid and the purchaser has sufficient funds available), and forwards the authorization code to the vendor" (Cohen, col. 5, ll. 45-49).
g) associating the purchase with said pre-established account.	"...the transaction code is pre-coded to be indicative of a specific credit card account..." (col. 6, ll. 33-34).	"...the credit card can be marked, if desired, to show both that it has been processed to charge money to the person's account..." (Cohen, col. 4, ll. 36-38).

18. The method of claim 17 wherein said step of verifying that said defined purchase parameters correspond to said selected payment category further identifies said merchant as one of said one or more merchants.	"Restricted communication between the merchant and the custodial authorizing entity as at 26 is permitted exclusively for purposes of verification of the transaction code..." (col. 7, ll. 13-16).	"Upon use of the card, the information regarding the transaction is transmitted to the credit card company, as is known in the art" (Cohen, col. 13, ln. 66-col. 14, ln. 1) where merchant identification in transaction details is known in the art.
19. A method of performing secure credit card purchases, said method comprising the steps of:	"...the present invention is directed towards a system and method for accomplishing secure credit card purchases" (col. 5, ll. 28-30).	"It is an object of the present invention to provide improved credit cards and methods for credit card transactions...[i]t is a further object of the present invention to provide methods and apparatus for secure transmission of credit card information" (Cohen, col. 1, ll. 48-62).
a) identifying a pre-established account that is used to make credit card purchases;	"...the custodial authorizing entity verifies the credit card status and account identification of the customer..." (col. 6, ll. 15-17).	"...a user dials into her credit card company before making a transaction, and after providing the ordinary credit card number and verification data..." (Cohen, col. 3, ll. 42-45).
b) selecting a pre-determined payment category which limits its nature of a subsequent purchase to one or more merchants,	"The payment category may also include a multi-transaction authorization wherein more than one purchase may be made from one or a plurality of different merchants..." (col. 8, ll. 18-20).	"...a user can indicate in advance of purchase...what the single use or the customized credit card number is to be used for" (Cohen, col. 3, ll. 49-52). "A customized credit card could be issued to the user which is only valid for use for that particular type of charge (computer hardware or software stores)...[or] for use in a particular store itself or a particular chain of stores" (Cohen, col. 8, ll. 25-34).
said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants;	"...each of which may or may not be identified by the customer and pre-coded in associated with the transaction code" (col. 8, ll. 19-22).	"A customized credit card could be issued to the user which is only valid for use for that particular *type* of charge (computer hardware or software stores)..." (Cohen, col. 8, ll. 25-28) (emphasis added).
c) generating a transaction code by a processing computer of a custodial	"...the custodial authorizing entity generates a transaction code as at 20"	"A user dials into her credit card company before making a transaction, and...is

authorizing entity of said pre-established account,	(col. 6, ll. 26-28).	provided with a disposable or customized number" (Cohen, col. 3, ll. 41-45). "These credit cards or credit card numbers are generated..." (Cohen, col. 2, ll. 35-36).
said transaction code associated with at least said pre-established account and the limits of said selected payment category, and	"...the transaction code is pre-coded to be indicative of a specific credit card account, preferably a merchant or merchants identification and a designated payment category" (col. 6, ll. 33-35).	"A customized credit card could be issued to the user which is only valid for use for that particular type of charge" (Cohen, col. 8, ll. 25-27). "...the credit card can be marked, if desired, to show both that it has been processed to charge money to the person's account..." (Cohen, col. 4, ll. 36-38), showing the association of the card with the pre-established account.
different from said pre-established account;	"The transaction code is used in substitution for the specific credit card number which would normally identify a customer's credit card account..." (col. 6, ll. 28-30).	"No vendor would ever, under one embodiment of the system, receive or have access to the user's permanent credit card number. Rather, the vendor would receive a disposable credit card number from the user's supply" (Cohen, col. 4, ll. 26-31).
d) designating a merchant as one of said one or more merchants;	"...the customer...can designate that only one merchant, whether designated or not, can use the transaction code" (col. 8, ll. 30-34).	"...the user could...if desired, set the places or types of places where the card will be active" (Cohen, col. 9, ll. 27-30).
e) communicating said transaction code to said merchant to consummate a purchase within defined purchase parameters;	"The verified customer...will directly or through an authorized representative communicate the code to the merchant as at 24" (col. 6, ll. 44-48). "...the merchant proceeds to consummate the purchase..." (col. 7, ll. 27-28).	"...the user transmits his or her credit card information to the vendor. That vendor then verifies the transaction..." (Cohen, col. 5, ll. 36-37).
f) verifying that said defined purchase parameters correspond to said selected payment category;	Inferred, but not directly supported, by the specification. See, col. 7, ll. 13-16 ("Restricted communication between the merchant and the custodial authorizing	"That vendor then verifies the transaction..." (Cohen, col. 5, ln. 37). "A customized credit card...is only valid for use for that particular type of charge...such

	entity as at 26 is permitted exclusively for purposes of verification of the transaction code...").	that if the employee tries to use it for anything else...the charge will be declined" (Cohen, col. 8, ll. 25-32)
g) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said selected payment category and to authorize payment required to complete the purchase; and	No direct support found in specification. See, col. 7, ll. 18-22 ("As a result, the merchant also has a desired verification as to the validity of a transaction and can effectively make arrangements to be paid by the credit card company").	"...the credit card company notes the identity of the vendor, authorizes the transaction (if the credit card number is valid and the purchaser has sufficient funds available), and forwards the authorization code to the vendor" (Cohen, col. 5, ll. 45-49).
h) associating the purchase with said pre-established account.	"...the transaction code is pre-coded to be indicative of a specific credit card account..." (col. 6, ll. 33-34).	"...the credit card can be marked, if desired, to show both that it has been processed to charge money to the person's account..." (Cohen, col. 4, ll. 36-38).
21. A method for implementing a system for performing secure credit card purchases, the method comprising:	"...the present invention is directed towards a system and method for accomplishing secure credit card purchases" (col. 5, ll. 28-30).	"It is an object of the present invention to provide improved credit cards and methods for credit card transactions...[i]t is a further object of the present invention to provide methods and apparatus for secure transmission of credit card information" (Cohen, col. 1, ll. 48-62).
a) receiving account information from an account holder identifying an account that is used to make credit card purchases;	"Once contacted, the customer then supplies appropriate identification data to inform the custodial authorizing entity of a specific customer's credit card account as at 15" (col. 5, ln. 66 - col. 6, ln. 2).	"...a user dials into her credit card company before making a transaction, and after providing the ordinary credit card number and verification data..." (Cohen, col. 3, ll. 42-45).
b) receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant, said single merchant limitation being included in said payment category prior to any particular merchant being identified as said single merchant;	"...the customer contacts and supplies a custodial authorizing entity with the requisite information concerning...a requested payment category" (col. 3, ll. 18-25). "The payment category may also include a multi-transaction authorization wherein more than one purchase may be made from one or a plurality of different	"A user dials into her credit card company before making a transaction, and...is provided with a disposable or customized number" (Cohen, col. 3, ll. 41-45). "...a user can indicate in advance of purchase...what the single use or the customized credit card number is to be used for" (Cohen, col. 3, ll. 49-52). "A customized credit card could be issued

	merchants each of which may or may not be identified by the customer and pre-coded in associated with the transaction code" (col. 8, ll. 18-22).	to the user which is only valid...for use in a particular store itself..." (Cohen, col. 8, ll. 25-34).
c) generating a transaction code utilizing a processing computer of a custodial authorizing entity, said transaction code associated with said account	"...the custodial authorizing entity generates a transaction code as at 20" (col. 6, ll. 26-28). "...the transaction code is pre-coded to be indicative of a specific credit card account..." (col. 6, ll. 33-34).	"These credit cards or credit card numbers are generated..." (Cohen, col. 2, ll. 35-36). "...the credit card can be marked, if desired, to show both that it has been processed to charge money to the person's account..." (Cohen, col. 4, ll. 36-38), showing the association of the card with the pre-established account.
and reflecting at least the limits of said payment category, to make a purchase within said payment category;	"...the transaction code is pre-coded to be indicative of a specific credit card account, preferably a merchant or merchants identification and a designated payment category" (col. 6, ll. 33-35).	"A customized credit card could be issued to the user which is only valid for use for that particular type of charge" (Cohen, col. 8, ll. 25-27).
d) communicating said transaction code to said account holder;	"...the transaction code is transmitted exclusively to the customer by the custodial authorizing entity..." (col. 4, ll. 22-23).	"...a user...is provided with a disposable or customized number..." (Cohen, col. 3, ll. 43-45).
e) receiving a request to authorize payment for a purchase using said transaction code;	"Moreover, the merchant 56, through a conventional, yet restricted communication with the custodial authorizing entity 64...can obtain a verification and subsequent payment utilizing the transaction code only" (col. 7, ll. 49-55).	"Upon receiving the request for verification," where the request for verification came from a vendor after receiving the customized credit card from the user (Cohen, col. 5, ll. 35-49).
f) authorizing payment for said purchase if said purchase is within said payment category.	No direct support found in specification. See, col. 7, ll. 18-22 ("As a result, the merchant also has a desired verification as to the validity of a transaction and can effectively make arrangements to be paid by the credit card company").	"...the credit card company notes the identity of the vendor, authorizes the transaction (if the credit card number is valid and the purchaser has sufficient funds available), and forwards the authorization code to the vendor" (Cohen, col. 5, ll. 45-49).

23. The method of claim 21 wherein the step of receiving account information from an account holder identifying an account that is used to make credit card purchases further comprises receiving information identifying a credit card account.	"Once contacted, the customer then supplies appropriate identification data to inform the custodial authorizing entity of a specific customer's credit card account as at 15" (col. 5, ln. 66 - col. 6, ln. 2).	"...a user dials into her credit card company before making a transaction, and after providing the ordinary credit card number and verification data..." (Cohen, col. 3, ll. 42-45).
24. The method of claim 21 wherein the step of generating a transaction code utilizing a processing computer of a custodial authorizing entity further comprises generating a transaction code which reflects at least one of a plurality of predetermined payment categories.	"...the transaction code is pre-coded to be indicative of a specific credit card account, preferably a merchant or merchants identification and a designated payment category" (col. 6, ll. 33-35).	"These credit cards or credit card numbers are generated..." (Cohen, col. 2, ll. 35-36). "A customized credit card could be issued to the user which is only valid for use for that particular type of charge" (Cohen, col. 8, ll. 25-27).
25. The method of claim 21 wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant further comprises receiving a request from said account holder for a transaction code to make a purchase within a payment category that is automatically chosen by a custodial authorizing entity.	"Further, a feature of the transaction code is its ability to indicate any one of preferably a plurality of predetermined payment categories which may be either requested by the customer or automatically chosen by the custodial authorizing entity..." (col. 3, ll. 48-52).	"...a user can indicate in advance of purchase...what the single use or the customized credit card number is to be used for" (Cohen, col. 3, ll. 49-52). The choosing of the payment category inherently would be automatically performed by the credit card company.
29. The method of claim 21 wherein said step of receiving a request to authorize payment for a purchase using said transaction code further identifies said single merchant.	"Moreover, the merchant 56, through a conventional, yet restricted communication with the custodial authorizing entity 64...can obtain a verification and subsequent payment utilizing the transaction code only" (col. 7, ll. 49-55).	"Upon use of the card, the information regarding the transaction is transmitted to the credit card company, as is known in the art" (Cohen, col. 13, ln. 66-col. 14, ln. 1) "...the credit card company notes the identity of the vendor..." (Cohen, col. 5, ll. 45-49).
30. The method of claim 21 wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant further comprises receiving a request from said account	"Once the customer's authorization is confirmed, details of the anticipated transaction are established so as to determine a payment category..." (col. 7, ll. 43-45).	"...a user can indicate in advance of purchase...what the single use or the customized credit card number is to be used for" (Cohen, col. 3, ll. 49-52).

holder for a transaction code to make a purchase within a predetermined payment category that is further limited in accordance with transaction details provided by said account holder.		

Appendix B – '988 Patent Claims and Written Description versus Franklin

'988 Patent Claims	Closest Explanation in '988 Patent	Disclosure in Franklin (5,883,810)
1. A method of performing secure credit card purchases, said method comprising:	"...the present invention is directed towards a system and method for accomplishing secure credit card purchases" (col. 5, ll. 28-30).	"This invention relates to systems and methods for conducting online transactions using an electronically realizable card that has a private, permanent account number...without exposure of the permanent account number" (Franklin, col. 1, ll. 10-16). "To the merchant, the transaction number is treated the same as any regular credit card number" (Franklin, col. 2, ll. 23-25).
a) contacting a custodial authorizing entity having custodial responsibility of account parameters of a customer's account that is used to make credit card purchases;	"...the customer contacts, either by computer, telephone, or in person, a custodial authorizing entity as at 12. The custodial authorizing entity may herein be defined as comprising that entity or institution which has or has been designated by the entity which has custodial responsibility for the financial data and security of a given credit card account of a customer" (col. 5, ll. 51-57).	"...the customer sends a request to the issuing institution..." (Franklin, col. 2, ll. 13-14).
b) supplying said custodial authorizing entity with at least account identification data of said customer's account;	"Once contacted, the customer then supplies appropriate identification data to inform the custodial authorizing entity of a specific customer's credit card account as at 15" (col. 5, ln. 66 - col. 6, ln. 2).	"The customer is prompted by the dialog box to input a password for identification purposes. The password might be the private key...or it may be a separate name or number created by the customer" (Franklin, col. 8, ll. 45-49). The issuing institution "immediately verifies the identity and authenticity of the customer" (Franklin, col. 8, ll. 57-59).
c) defining at least one payment category to include at least limiting a number of transactions to one or more merchants,	[In light of this recitation, the claims are limited to the embodiment described at col. 8, ll. 18-34.] "The payment category may also include a	"...the transaction number can be linked to extra transaction information to ensure that the number is only used for one specific transaction" (Franklin, col. 2, ll. 48-50).

	multi-transaction authorization wherein more than one purchase may be made from one or a plurality of different merchants..." (col. 8, ll. 18-20).	
said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants;	"...each of which may or may not be identified by the customer and pre-coded in associated with the transaction code" (col. 8, ll. 19-22).	"the transaction number can be linked to extra transaction information...for instance, the issuing institution might tie the transaction number to...a particular merchant ID" (Franklin, col. 2, ll. 48-52).
d) designating said payment category;	"Further, a feature of the transaction code is its ability to indicate any one of preferably a plurality of predetermined payment categories which may either be requested by the customer or automatically chosen by the custodial authorizing entity..." (col. 3, ll. 48-52).	"For instance, the issuing institution might tie the transaction number to a specific purchase amount and a particular merchant ID" (Franklin, col. 2, ll. 50-52).
e) generating a transaction code by a processing computer of said custodial authorizing entity,	"...the custodial authorizing entity generates a transaction code as at 20" (col. 6, ll. 26-28).	"The issuing bank generates a random temporary transaction number..." (Franklin, col. 4, ll. 50-51).
said transaction code reflecting at least the limits of said designated payment category to make a purchase within said designated payment category;	"...a merchant identifier is pre-coded in associate within the transaction code, the pre-coding of the transaction code will prohibit an unauthorized use due at least in part to the fact that the merchant is specifically identified and any attempt to use the transaction code other than by the identified merchant will be prohibited" (col. 7, ll. 1-6).	"...the transaction number can be linked to extra transaction information to ensure that the number is only used for one specific transaction" (Franklin, col. 2, ll. 48-50).
f) communicating said transaction code to a merchant to consummate a purchase with defined purchase parameters;	"The verified customer...will directly or through an authorized representative communicate the code to the merchant as at 24" (col. 6, ll. 44-48). "...the merchant proceeds to consummate the purchase..." (col. 7, ll. 27-28).	"The customer receives the transaction number and submits that number to the merchant..." (Franklin, col. 2, ll. 17-18). "The merchant 30 receives the transaction number from the Internet and processes the transaction number using its existing

		computer system" (Franklin, col. 10, ll. 39-41).
g) verifying that said defined purchase parameters are within said designated payment category; and	Inferred, but not directly supported, by the specification. See, col. 7, ll. 13-16 ("Restricted communication between the merchant and the custodial authorizing entity as at 26 is permitted exclusively for purposes of verification of the transaction code...").	"If a record is found, the account manager 60 examines any extra transaction information, such as purchase amount and merchant ID...to double check the accuracy of the request" (Franklin, col. 11, ll. 17-21).
h) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said designated payment category and to authorize payment required to complete the purchase.	No direct support found in specification. See, col. 7, ll. 18-22 ("As a result, the merchant also has a desired verification as to the validity of a transaction and can effectively make arrangements to be paid by the credit card company").	"When the bank computer 32 receives the authorization request, it first examines the transaction number to determine whether it is a valid number" (Franklin, col. 10, ll. 61-63). "The bank computing center 32 then returns the authorization reply to the merchant computer 30..." (Franklin, col. 11, ll. 38-39).
2. The method of claim 1 further comprising the step of designating at least one of said one or more merchants subsequent to generating said transaction code.	"...the customer may designate...that only one merchant, whether designated or not, can use the transaction code" (col. 8, ll. 30-34).	"The issuing institution generates a temporary transaction number...The customer receives the transaction number and submits that number to the merchant..." (Franklin, col. 2, ll. 15-18).
3. The method of claim 1 wherein said step of communicating the transaction code to a merchant to consummate said purchase within defined purchase parameters further comprises designation of said merchant as one of said one or more merchants.	"The verified customer...will directly or through an authorized representative communicate the code to the merchant as at 24" (col. 6, ll. 44-48). "...the merchant proceeds to consummate the purchase..." (col. 7, ll. 27-28).	"The issuing institution generates a temporary transaction number...The customer receives the transaction number and submits that number to the merchant..." (Franklin, col. 2, ll. 15-18). "The merchant 30 receives the transaction number...and processes the transaction number..." (Franklin, col. 10, ll. 39-41).
4. The method of claim 1 wherein said step of generating said transaction code further comprises said customer obtaining said transaction code.	"Once generated, the transaction code is communicated exclusively to the authorized and verified customer by the custodial authorizing entity as at 22" (col. 6, ll. 37-39).	"The customer receives the transaction number..." (Franklin, col. 17-18).
5. The method of claim 1 further	"...the transaction code is pre-coded to be	"...the transaction number can be linked to

comprising generating a transaction code which reflects at least one of a plurality of said payment categories.	indicative of...a designated payment category, selected from the plurality of predetermined payment categories..." (col. 6, ll. 33-36).	extra transaction information..." (Franklin, col. 2, ll. 48-50).
6. The method of claim 1 further comprising defining at least one payment category to include amount parameters for a cost of one or more purchases.	"More specifically, the plurality of payment categories may include a single transaction involving a specific dollar amount for a purchase..." (col. 3, ll. 56-58).	"...the transaction number can be linked to extra transaction information..." (Franklin, col. 2, ll. 48-50). "... extra transaction information, such as purchase amount ..." (Franklin, col. 11, ll. 17-21).
7. The method of claim 1 further comprising defining at least one payment category to include time parameters during which the purchase can be completed.	"More specifically, the plurality of payment categories may include...a specific time period, such as twenty four hours, during which authorization of the purchase remains valid." (col. 3, ll. 56-60).	"The issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses" (Franklin, col. 2, ll. 15-55).
8. The method of claim 1 further comprising defining at least one payment category to include limiting said transaction code to a single transaction for a purchase within a predetermined period of time.	"More specifically, the plurality of payment categories may include a single transaction...for a purchase within a specific time period, such as twenty four hours, during which authorization of the purchase remains valid." (col. 3, ll. 56-60).	"...the transaction number can be linked to extra transaction information to ensure that the number is only used for one specific transaction" (Franklin, col. 2, ll. 48-50). "The issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses" (Franklin, col. 2, ll. 15-55).
9. The method of claim 1 further comprising defining at least one payment category to include limiting purchases to a single transaction at a maximum amount for purchase within a predetermined period of time.	"More specifically, the plurality of payment categories may include a single transaction involving a specific dollar amount for a purchase within a specific time period..." (col. 3, ll. 56-59).	"...the transaction number can be linked to extra transaction information to ensure that the number is only used for one specific transaction" (Franklin, col. 2, ll. 48-50). "The usable limit indicates the maximum limit of electronic money the user can withdraw" (Yanagihara, para. [0019]).
10. The method of claim 1 further comprising defining at least one payment category to include limiting purchases to at least one payment category to at least two purchases at a maximum total amount for items purchased within a predetermined	"Other alternatives would involve one or more of the categories coded to define multiple transactions involving a maximum dollar amount for purchases, as well as a fixed period of time for authorization of such purchases..." (col. 3, ln. 65 to col. 4,	"The usable limit indicates the maximum limit of electronic money the user can withdraw. The aggregate amount indicates a total sum of electronic money read from the electronic money card" (Yanagihara, para. [0019]).

period of time.	ln. 1).	
11. The method of claim 1 further comprising defining at least one payment category to include using said transaction code for at least two purchases for a repeating transaction at a fixed amount payable at each of a fixed number of time intervals.	"Other alternatives would involve one or more of the categories coded to define...a repeating transaction wherein payments may be automatically accessed by a merchant over a predetermined or unspecified time interval (such as every thirty days) for a specific dollar amount or a maximum dollar amount limit" (col. 3, ln. 65 to col. 4, ln. 5).	"The usage identification code indicates what purpose a user uses the electronic money card 106 for...Further, the nonvolatile memory 205 additionally includes a storage area 210...for recording a user's personal ID 223, a transaction date 224, a transaction category 225, an amount transacted 226, and a usage category 227" (Yanagihara, para. [0019-0020]).
12. The method of claim 11 further comprising defining at least one payment category to include limiting purchases to said repeating transaction at said fixed amount payable at each of said fixed number of time intervals.	"Other alternatives would involve one or more of the categories coded to define...a repeating transaction wherein payments may be automatically accessed by a merchant over a predetermined or unspecified time interval (such as every thirty days) for a specific dollar amount or a maximum dollar amount limit" (col. 3, ln. 65 to col. 4, ln. 5).	"The usage identification code indicates what purpose a user uses the electronic money card 106 for...Further, the nonvolatile memory 205 additionally includes a storage area 210...for recording a user's personal ID 223, a transaction date 224, a transaction category 225, an amount transacted 226, and a usage category 227" (Yanagihara, para. [0019-0020]).
13. The method of claim 1 further comprising defining at least one payment category to include using said transaction code for a repeating transaction at a fixed amount payable to each of an unspecified number of time intervals.	"Similarly, a repeating transaction for a stated minimum interval, such as every thirty days may be authorized for a specific amount for an unspecified number of intervals..." (col. 8, ln. 43-45).	"The usage identification code indicates what purpose a user uses the electronic money card 106 for...Further, the nonvolatile memory 205 additionally includes a storage area 210...for recording a user's personal ID 223, a transaction date 224, a transaction category 225, an amount transacted 226, and a usage category 227" (Yanagihara, para. [0019-0020]).
14. The method of claim 1 further comprising defining at least one payment category to include limiting a repeating transaction to a maximum dollar amount.	"Other alternatives would involve one or more of the categories coded to define...a repeating transaction ...for a specific dollar amount or a maximum dollar amount limit" (col. 3, ln. 65 to col. 4, ln. 5).	"The usage identification code indicates what purpose a user uses the electronic money card 106 for...Further, the nonvolatile memory 205 additionally includes a storage area 210...for recording a user's personal ID 223, a transaction date 224, a transaction category 225, an amount transacted 226, and a usage category 227" (Yanagihara, para. [0019-0020]).
15. The method of claim 1 further	"In addition, the transactions are	"Since the transaction number is issued in

comprising defining at least one payment category to include limiting purchases to a limited time interval during which a purchase is permitted.	preferably, but not necessarily, authorized to be conducted only over a fixed life period of time..." (col. 8, ll. 6-8).	place of the customer number...with a limited life..." (Franklin, col. 4, ll. 65-67). "The issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses" (Franklin, col. 2, ll. 15-55).
16. The method of claim 1 further comprising communicating said transaction code to the customer at the location of the merchant for use in person.	"...the present invention is directed towards a system and method for accomplishing secure credit card purchases. Moreover, these purchases can be 'in person'..." (col. 5, ll. 28-31).	"The customer receives the transaction number and submits that number to the merchant..." (Franklin, col. 2, ll. 17-18).
17. A method of performing secure credit card purchases, said method comprising:	"...the present invention is directed towards a system and method for accomplishing secure credit card purchases" (col. 5, ll. 28-30).	"This invention relates to systems and methods for conducting online transactions using an electronically realizable card that has a private, permanent account number...without exposure of the permanent account number" (Franklin, col. 1, ll. 10-16).
a) identifying a pre-established account that is used to make credit card purchases;	"...the custodial authorizing entity verifies the credit card status and account identification of the customer..." (col. 6, ll. 15-17).	"The bank computer 32 receives the signed request and immediately verifies the identity and authenticity of the customer..." (Franklin, col. 8, ll. 57-59). "...the number from the credit card or debit card is the customer account number used to identify the data record for the online commerce card" (Franklin, col. 7, ll. 43-45).
b) selecting a predetermined payment category which limits its a nature, of a series of subsequent purchases to one or more merchants,	"The payment category may also include a multi-transaction authorization wherein more than one purchase may be made from one or a plurality of different merchants..." (col. 8, ll. 18-20).	"The limitations and/or restrictions may include the types of transactions which are allwoed and/or authorized, the goods and/or services which may be purchased with the card, the vendors, stores and/or service provider which may be authorized to accept the card, limits on the dollar amounts of transactions pertaining to each authorized vendor, seller and/or service provider, daily

		spending limits, and/or the geographical area or location wherein authorized card use may be limited, and/or authorized times for card usage (i.e., specific days, dates, time of day, time of month, year, etc.), and/or any other limitation and/or restriction regarding amount of transaction, parties involved, geographical area, and/or times of allowed usage" (Joao, col. 16, ll. 18-30).
said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants;	"...each of which may or may not be identified by the customer and pre-coded in associated with the transaction code" (col. 8, ll. 19-22).	"the transaction number can be linked to extra transaction information...for instance, the issuing institution might tie the transaction number to...a particular merchant ID" (Franklin, col. 2, ll. 48-52).
c) generating a transaction code by a processing computer of a custodial authorizing entity of said pre-established account,	"...the custodial authorizing entity generates a transaction code as at 20" (col. 6, ll. 26-28).	"The issuing bank generates a random temporary transaction number..." (Franklin, col. 4, ll. 50-51).
said transaction code associated with at least said pre-established account and the limits of said selected payment category	"...the transaction code is pre-coded to be indicative of a specific credit card account, preferably a merchant or merchants identification and a designated payment category" (col. 6, ll. 33-35).	"The issuing bank generates a random temporary transaction number and associates it with the permanent account in a data record" (Franklin, col. 2, ll. 15-17). "the transaction number can be linked to extra transaction information... " (Franklin, col. 2, ll. 48-52).
and different from said pre-established account;	"The transaction code is used in substitution for the specific credit card number which would normally identify a customer's credit card account..." (col. 6, ll. 28-30).	"The issuing bank 26 identifies the number as a transaction number, as opposed to a real customer account number" (Franklin, col. 5, ll. 6-8).
d) communicating said transaction code to a merchant to consummate a purchase within defined purchase parameters;	"The verified customer...will directly or through an authorized representative communicate the code to the merchant as at 24" (col. 6, ll. 44-48). "...the merchant	"The merchant 30 receives the transaction number from the Internet and processes the transaction number using its existing computer system" (Franklin, col. 10, ll. 39-

	proceeds to consummate the purchase..." (col. 7, ll. 27-28).	41).
e) verifying that said defined purchase parameters correspond to said selected payment category;	Inferred, but not directly supported, by the specification. See, col. 7, ll. 13-16 ("Restricted communication between the merchant and the custodial authorizing entity as at 26 is permitted exclusively for purposes of verification of the transaction code...").	"If a record is found, the account manager 60 examines any extra transaction information, such as purchase amount and merchant ID...to double check the accuracy of the request" (Franklin, col. 11, ll. 17-21).
f) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said selected payment category and to authorize payment required to complete the purchase; and	No direct support found in specification. See, col. 7, ll. 18-22 ("As a result, the merchant also has a desired verification as to the validity of a transaction and can effectively make arrangements to be paid by the credit card company").	"When the bank computer 32 receives the authorization request, it first examines the transaction number to determine whether it is a valid number" (Franklin, col. 10, ll. 61-63). "The bank computing center 32 then returns the authorization reply to the merchant computer 30..." (Franklin, col. 11, ll. 38-39).
g) associating the purchase with said pre-established account.	"...the transaction code is pre-coded to be indicative of a specific credit card account..." (col. 6, ll. 33-34).	"The issuing bank 26 then swaps the customer account number for the transaction number and processes the authorization request..." (Franklin, col. 5, ll. 10-12).
18. The method of claim 17 wherein said step of verifying that said defined purchase parameters correspond to said selected payment category further identifies said merchant as one of said one or more merchants.	"Restricted communication between the merchant and the custodial authorizing entity as at 26 is permitted exclusively for purposes of verification of the transaction code..." (col. 7, ll. 13-16).	"If a record is found, the account manager 60 examines any extra transaction information, such as purchase amount and merchant ID...to double check the accuracy of the request" (Franklin, col. 11, ll. 17-21).
19. A method of performing secure credit card purchases, said method comprising the steps of:	"...the present invention is directed towards a system and method for accomplishing secure credit card purchases" (col. 5, ll. 28-30).	"This invention relates to systems and methods for conducting online transactions using an electronically realizable card that has a private, permanent account number...without exposure of the permanent account number" (Franklin, col.

		1, ll. 10-16).
a) identifying a pre-established account that is used to make credit card purchases;	"...the custodial authorizing entity verifies the credit card status and account identification of the customer..." (col. 6, ll. 15-17).	"The bank computer 32 receives the signed request and immediately verifies the identity and authenticity of the customer..." (Franklin, col. 8, ll. 57-59). "...the number from the credit card or debit card is the customer account number used to identify the data record for the online commerce card" (Franklin, col. 7, ll. 43-45).
b) selecting a pre-determined payment category which limits its nature of a subsequent purchase to one or more merchants,	"The payment category may also include a multi-transaction authorization wherein more than one purchase may be made from one or a plurality of different merchants..." (col. 8, ll. 18-20).	"the transaction number can be linked to extra transaction information to ensure that the number is only used for one specific transaction...the issuing institution might tie the transaction number to...a particular merchant ID" (Franklin, col. 2, ll. 48-52).
said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants;	"...each of which may or may not be identified by the customer and pre-coded in associated with the transaction code" (col. 8, ll. 19-22).	"the transaction number can be linked to extra transaction information...for instance, the issuing institution might tie the transaction number to...a particular merchant ID" (Franklin, col. 2, ll. 48-52).
c) generating a transaction code by a processing computer of a custodial authorizing entity of said pre-established account,	"...the custodial authorizing entity generates a transaction code as at 20" (col. 6, ll. 26-28).	"The issuing bank generates a random temporary transaction number..." (Franklin, col. 4, ll. 50-51).
said transaction code associated with at least said pre-established account and the limits of said selected payment category, and	"...the transaction code is pre-coded to be indicative of a specific credit card account, preferably a merchant or merchants identification and a designated payment category" (col. 6, ll. 33-35).	"The issuing bank generates a random temporary transaction number and associates it with the permanent account in a data record" (Franklin, col. 2, ll. 15-17). "the transaction number can be linked to extra transaction information... " (Franklin, col. 2, ll. 48-52).
different from said pre-established	"The transaction code is used in substitution for the specific credit card number which would normally identify a	"The issuing bank 26 identifies the number

account;	customer's credit card account..." (col. 6, ll. 28-30).	as a transaction number, as opposed to a real customer account number" (Franklin, col. 5, ll. 6-8).
d) designating a merchant as one of said one or more merchants;	"...the customer...can designate that only one merchant, whether designated or not, can use the transaction code" (col. 8, ll. 30-34).	"If a record is found, the account manager 60 examines any extra transaction information, such as...merchant ID, which is typically included in the authorization request..." (Franklin, col. 11, ll. 17-21).
e) communicating said transaction code to said merchant to consummate a purchase within defined purchase parameters;	"The verified customer...will directly or through an authorized representative communicate the code to the merchant as at 24" (col. 6, ll. 44-48). "...the merchant proceeds to consummate the purchase..." (col. 7, ll. 27-28).	"The merchant 30 receives the transaction number from the Internet and processes the transaction number using its existing computer system" (Franklin, col. 10, ll. 39-41).
f) verifying that said defined purchase parameters correspond to said selected payment category;	Inferred, but not directly supported, by the specification. See, col. 7, ll. 13-16 ("Restricted communication between the merchant and the custodial authorizing entity as at 26 is permitted exclusively for purposes of verification of the transaction code...").	"If a record is found, the account manager 60 examines any extra transaction information, such as purchase amount and merchant ID...to double check the accuracy of the request" (Franklin, col. 11, ll. 17-21).
g) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said selected payment category and to authorize payment required to complete the purchase; and	No direct support found in specification. See, col. 7, ll. 18-22 ("As a result, the merchant also has a desired verification as to the validity of a transaction and can effectively make arrangements to be paid by the credit card company").	"When the bank computer 32 receives the authorization request, it first examines the transaction number to determine whether it is a valid number" (Franklin, col. 10, ll. 61-63). "The bank computing center 32 then returns the authorization reply to the merchant computer 30..." (Franklin, col. 11, ll. 38-39).
h) associating the purchase with said pre-established account.	"...the transaction code is pre-coded to be indicative of a specific credit card account..." (col. 6, ll. 33-34).	"The issuing bank 26 then swaps the customer account number for the transaction number and processes the authorization request..." (Franklin, col. 5, ll.

		10-12).
21. A method for implementing a system for performing secure credit card purchases, the method comprising:	"...the present invention is directed towards a system and method for accomplishing secure credit card purchases" (col. 5, ll. 28-30).	"This invention relates to systems and methods for conducting online transactions using an electronically realizable card that has a private, permanent account number...without exposure of the permanent account number" (Franklin, col. 1, ll. 10-16).
a) receiving account information from an account holder identifying an account that is used to make credit card purchases;	"Once contacted, the customer then supplies appropriate identification data to inform the custodial authorizing entity of a specific customer's credit card account as at 15" (col. 5, ln. 66 - col. 6, ln. 2).	"The customer is prompted to input a password for identification purposes. The password might be a private key (if the customer knows the key value) or it may be a separate name or number created by the customer" (Franklin, col. 8, ll. 45-49). "The bank computer 32 receives the signed request and immediately verifies the identity and authenticity of the customer..." (Franklin, col. 8, ll. 57-59). "...the number from the credit card or debit card is the customer account number used to identify the data record for the online commerce card" (Franklin, col. 7, ll. 43-45).
b) receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant, said single merchant limitation being included in said payment category prior to any particular merchant being identified as said single merchant;	"...the customer contacts and supplies a custodial authorizing entity with the requisite information concerning...a requested payment category" (col. 3, ll. 18-25). "The payment category may also include a multi-transaction authorization wherein more than one purchase may be made from one or a plurality of different merchants each of which may or may not be identified by the customer and pre-coded in associated with the transaction code" (col. 8, ll. 18-22).	"...the customer sends a request to the issuing institution to issue a transaction number..." (Franklin, col. 2, ll. 13-14). "the transaction number can be linked to extra transaction information...for instance, the issuing institution might tie the transaction number to...a particular merchant ID" (Franklin, col. 2, ll. 48-52). "The issuing bank generates a random temporary transaction number and associates it with the permanent account in a data record " (Franklin, col. 2, ll. 15-17).
c) generating a transaction code	"...the custodial authorizing entity	"the transaction number can be linked to

utilizing a processing computer of a custodial authorizing entity, said transaction code associated with said account	generates a transaction code as at 20" (col. 6, ll. 26-28). "...the transaction code is pre-coded to be indicative of a specific credit card account..." (col. 6, ll. 33-34).	extra transaction information... " (Franklin, col. 2, ll. 48-52).
and reflecting at least the limits of said payment category, to make a purchase within said payment category;	"...the transaction code is pre-coded to be indicative of a specific credit card account, preferably a merchant or merchants identification and a designated payment category" (col. 6, ll. 33-35).	"The issuing bank 26 issues the transaction number to the customer..." (Franklin, col. 4, ll. 53-54).
d) communicating said transaction code to said account holder;	"...the transaction code is transmitted exclusively to the customer by the custodial authorizing entity..." (col. 4, ll. 22-23).	"When the bank computer 32 receives the authorization request, it first examines the transaction number..." (Franklin, col. 10, ll. 61-62).
e) receiving a request to authorize payment for a purchase using said transaction code;	"Moreover, the merchant 56, through a conventional, yet restricted communication with the custodial authorizing entity 64...can obtain a verification and subsequent payment utilizing the transaction code only" (col. 7, ll. 49-55).	"...the bank computer 32...first examines the transaction number to determine whether it is a valid number" (Franklin, col. 10, ll. 61-63). "If a record is found, the account manager 60 examines any extra transaction information, such as purchase amount and merchant ID...to double check the accuracy of the request" (Franklin, col. 11, ll. 17-21).
f) authorizing payment for said purchase if said purchase is within said payment category.	No direct support found in specification. See, col. 7, ll. 18-22 ("As a result, the merchant also has a desired verification as to the validity of a transaction and can effectively make arrangements to be paid by the credit card company").	
23. The method of claim 21 wherein the step of receiving account information from an account holder identifying an account that is used to make credit card purchases further comprises receiving information identifying a credit card account.	"Once contacted, the customer then supplies appropriate identification data to inform the custodial authorizing entity of a specific customer's credit card account as at 15" (col. 5, ln. 66 - col. 6, ln. 2).	"The bank computer 32 receives the signed request and immediately verifies the identity and authenticity of the customer..." (Franklin, col. 8, ll. 57-59).
24. The method of claim 21 wherein the step of generating a transaction code	"...the transaction code is pre-coded to be indicative of a specific credit card account,	"the transaction number can be linked to extra transaction information... " (Franklin,

utilizing a processing computer of a custodial authorizing entity further comprises generating a transaction code which reflects at least one of a plurality of predetermined payment categories.	preferably a merchant or merchants identification and a designated payment category" (col. 6, ll. 33-35).	col. 2, ll. 48-52).
25. The method of claim 21 wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant further comprises receiving a request from said account holder for a transaction code to make a purchase within a payment category that is automatically chosen by a custodial authorizing entity.	"Further, a feature of the transaction code is its ability to indicate any one of preferably a plurality of predetermined payment categories which may be either requested by the customer or automatically chosen by the custodial authorizing entity..." (col. 3, ll. 48-52).	"The transaction module 72 executing on the customer computer 28 may require the customer to enter information pertaining to the purchase, like the purchase price, the model or item number, the merchant name, and the like" (Franklin, col. 9, ln. 66 - col. 10, ll. 3). "the transaction number can be linked to extra transaction information...for instance, the issuing institution might tie the transaction number to...a particular merchant ID" (Franklin, col. 2, ll. 48-52).
29. The method of claim 21 wherein said step of receiving a request to authorize payment for a purchase using said transaction code further identifies said single merchant.	"Moreover, the merchant 56, through a conventional, yet restricted communication with the custodial authorizing entity 64...can obtain a verification and subsequent payment utilizing the transaction code only" (col. 7, ll. 49-55).	"If a record is found, the account manager 60 examines any extra transaction information, such as purchase amount and merchant ID...to double check the accuracy of the request" (Franklin, col. 11, ll. 17-21).
30. The method of claim 21 wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant further comprises receiving a request from said account holder for a transaction code to make a purchase within a predetermined payment category that is further limited in accordance with transaction details provided by said account holder.	"Once the customer's authorization is confirmed, details of the anticipated transaction are established so as to determine a payment category..." (col. 7, ll. 43-45).	"The transaction module 72 executing on the customer computer 28 may require the customer to enter information pertaining to the purchase, like the purchase price, the model or item number, the merchant name, and the like" (Franklin, col. 9, ln. 66 - col. 10, ll. 3).

US008036988B2

(12) **United States Patent**
D'Agostino

(10) **Patent No.: US 8,036,988 B2**
(45) **Date of Patent: *Oct. 11, 2011**

(54) **SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD TRANSACTIONS**

(76) Inventor: **John D'Agostino**, Sarasota, FL (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/902,399**

(22) Filed: **Oct. 12, 2010**

(65) **Prior Publication Data**

US 2011/0071945 A1 Mar. 24, 2011

Related U.S. Application Data

(63) Continuation of application No. 11/252,009, filed on Oct. 17, 2005, now Pat. No. 7,840,486, which is a continuation of application No. 10/037,007, filed on Nov. 9, 2001, now abandoned, which is a continuation-in-part of application No. 09/231,745, filed on Jan. 15, 1999, now Pat. No. 6,324,526.

(51) **Int. Cl.**
G06Q 40/00 (2006.01)

(52) **U.S. Cl.** **705/44**

(58) **Field of Classification Search** 705/44
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,376,661 A 4/1968 Hulett
3,938,091 A 2/1976 Atalla et al.
4,016,405 A 4/1977 McCune et al.
4,023,012 A 5/1977 Ano et al.
(Continued)

FOREIGN PATENT DOCUMENTS

CA 2167543 7/1997
(Continued)

OTHER PUBLICATIONS

Lee et al.: Evoluntionary business models for e-cash with smart cards, Korea Advanced Institute of Science and Technology, Korea, http://koasas.kaist.ac.kr/bitstream/10203/4774/1/2000-092.pdf , pp. 352-358.*

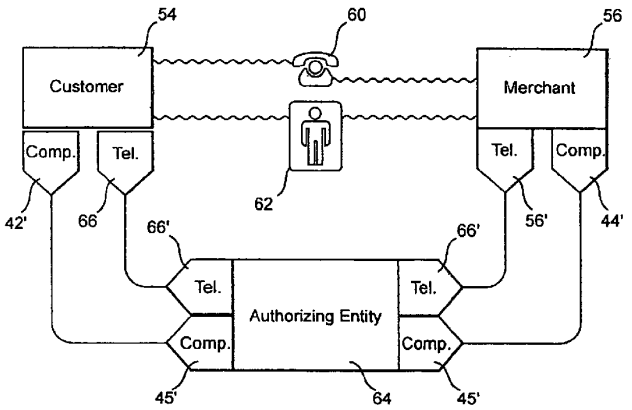
(Continued)

Primary Examiner — Bijendra K Shrestha
(74) *Attorney, Agent, or Firm* — Maxey Law Offices, PLLC; Stephen Lewellyn

(57) **ABSTRACT**

A method and system of performing secure credit card purchases in the context of a remote commercial transaction, such as over the telephone, wherein only the customer, once generally deciding upon a product or service to be purchased, communicates with a custodial authorizing entity, such as a credit card company or issuing bank wherein such entity has previous knowledge of the credit card number as well as custodial control of other account parameters such as interest rate, payment history, available credit limit etc. The customer supplies the custodial authorizing entity with the account identification data such as the credit card number and a requested one of a possible plurality of predetermined payment categories which define the dollar amount for the purchase and specific, predetermined time parameters within which authorization by the custodial authorizing entity will remain in effect. The custodial authorizing entity then generates a transaction code which is communicated exclusively to the customer wherein the customer in turn communicates only the transaction code to the merchant instead of a credit card number. The transaction code is indicative of merchant identification, credit card account identification and a designated one of the plurality of predetermined payment categories.

38 Claims, 2 Drawing Sheets



U.S. PATENT DOCUMENTS

4,048,475	A		9/1977	Yoshida
4,269,874	A		5/1981	Pryor et al.
4,395,628	A		7/1983	Silverman et al.
4,423,316	A		12/1983	Sano et al.
4,599,509	A		7/1986	Silverman et al.
4,629,874	A		12/1986	Pugsley et al.
4,667,087	A		5/1987	Quintana
4,679,236	A		7/1987	Davies
4,707,592	A		11/1987	Ware
4,720,860	A		1/1988	Weiss
4,725,719	A		2/1988	Oncken et al.
4,747,050	A		5/1988	Brachtl et al.
4,797,920	A		1/1989	Stein
4,856,062	A		8/1989	Weiss
4,893,330	A	*	1/1990	Franco 379/91.02
4,941,090	A		7/1990	McCarthy
4,988,849	A		1/1991	Sasaki et al.
4,998,279	A		3/1991	Weiss
5,010,485	A		4/1991	Bigari
5,023,904	A		6/1991	Kaplan et al.
5,093,861	A		3/1992	Graham
5,097,505	A		3/1992	Weiss
5,117,355	A		5/1992	McCarthy
5,130,519	A		7/1992	Bush et al.
5,163,097	A		11/1992	Pegg
5,163,098	A		11/1992	Dahbura
5,192,947	A		3/1993	Neustein
5,193,114	A		3/1993	Moseley
5,196,840	A		3/1993	Leith et al.
5,202,826	A		4/1993	McCarthy
5,231,666	A		7/1993	Matyas
5,239,583	A		8/1993	Parrillo
5,287,268	A		2/1994	McCarthy
5,311,594	A		5/1994	Penzias
5,317,636	A		5/1994	Vizcaino
5,323,338	A		6/1994	Hawthorne
5,326,960	A		7/1994	Tannenbaum
5,343,529	A		8/1994	Goldfine et al.
5,350,906	A		9/1994	Brody et al.
5,361,062	A		11/1994	Weiss et al.
5,363,449	A		11/1994	Bestock
5,420,926	A		5/1995	Low et al.
5,428,684	A		6/1995	Akiyama et al.
5,434,398	A		7/1995	Goldberg
5,457,747	A		10/1995	Drexler et al.
5,466,919	A		11/1995	Hovakimian
5,478,994	A		12/1995	Rahman et al.
5,479,494	A		12/1995	Clitherow
5,479,530	A		12/1995	Nair et al.
5,485,510	A		1/1996	Colbert
5,485,519	A		1/1996	Weiss
5,500,513	A	*	3/1996	Langhans et al. 235/380
5,504,808	A		4/1996	Hamrick, Jr.
5,509,070	A		4/1996	Schull
5,555,497	A		9/1996	Helbing
5,559,313	A		9/1996	Claus et al.
5,577,109	A		11/1996	Stimson et al.
5,583,918	A		12/1996	Nakagawa
5,585,787	A		12/1996	Wallerstein
5,590,038	A		12/1996	Pitroda
5,592,553	A		1/1997	Guski et al.
5,606,614	A		2/1997	Brady et al.
5,621,201	A		4/1997	Langhans et al.
5,627,355	A		5/1997	Rahman et al.
5,649,118	A		7/1997	Carlisle et al.
5,671,279	A		9/1997	Elgamal
5,677,955	A		10/1997	Doggett et al.
5,694,471	A		12/1997	Chen et al.
5,696,908	A		12/1997	Muehlberger et al.
5,715,314	A		2/1998	Payne et al.
5,721,768	A		2/1998	Stimson et al.
5,724,424	A		3/1998	Gifford
5,727,163	A		3/1998	Bezos
5,729,594	A		3/1998	Klingman
5,748,737	A		5/1998	Daggar
5,748,908	A		5/1998	Yu
5,754,653	A		5/1998	Canfield
5,757,917	A		5/1998	Rose et al.
5,768,381	A		6/1998	Hawthorne
5,777,305	A		7/1998	Smith et al.
5,777,306	A		7/1998	Masuda
5,794,221	A		8/1998	Egendorf
5,799,285	A		8/1998	Klingman
5,815,657	A		9/1998	Williams et al.
5,822,737	A		10/1998	Ogram
5,825,881	A		10/1998	Colvin, Sr.
5,826,241	A		10/1998	Stein et al.
5,826,243	A		10/1998	Musmanno et al.
5,826,245	A		10/1998	Sandberg-Diment
5,832,087	A		11/1998	Hawthorne
5,845,267	A		12/1998	Ronen
5,845,281	A	*	12/1998	Benson et al. 1/1
5,864,830	A		1/1999	Armetta et al.
RE36,116	E		2/1999	McCarthy
5,868,236	A		2/1999	Rademacher
5,878,141	A		3/1999	Daly et al.
5,883,452	A		3/1999	Masuda
5,883,810	A		3/1999	Franklin et al.
5,890,137	A		3/1999	Koreeda
5,893,907	A		4/1999	Ukuda
5,899,980	A		5/1999	Wilf et al.
5,903,830	A		5/1999	Joao et al.
5,903,878	A		5/1999	Talati et al.
5,905,736	A		5/1999	Ronen et al.
5,913,203	A		6/1999	Wong et al.
5,914,472	A	*	6/1999	Foladare et al. 235/380
5,953,710	A	*	9/1999	Fleming 705/38
5,955,961	A		9/1999	Wallerstein
5,956,699	A		9/1999	Wong et al.
5,959,699	A		9/1999	Patel et al.
5,984,180	A		11/1999	Albrecht
5,991,749	A		11/1999	Morrill, Jr.
5,991,750	A		11/1999	Watson
6,000,832	A	*	12/1999	Franklin et al. 700/232
6,012,048	A		1/2000	Gustin et al.
6,014,650	A		1/2000	Zampese
6,029,150	A	*	2/2000	Kravitz 705/39
6,029,890	A		2/2000	Austin
6,049,785	A		4/2000	Gifford
6,064,879	A		5/2000	Fujiwara et al.
6,068,192	A		5/2000	McCabe et al.
6,144,948	A		11/2000	Walker et al.
6,154,879	A		11/2000	Pare et al.
6,163,771	A	*	12/2000	Walker et al. 705/18
6,188,761	B1		2/2001	Dickerman et al.
6,195,649	B1		2/2001	Gifford
6,202,055	B1		3/2001	Houvener et al.
6,226,624	B1		5/2001	Watson et al.
6,227,447	B1		5/2001	Campisano
6,240,397	B1		5/2001	Sachs
6,253,188	B1		6/2001	Witek et al.
6,267,292	B1		7/2001	Walker et al.
6,298,335	B1		10/2001	Bernstein
6,324,526	B1		11/2001	D'Agostino
6,330,544	B1		12/2001	Walker et al.
6,339,766	B1		1/2002	Gephart
6,341,724	B2		1/2002	Campisano
6,343,279	B1		1/2002	Bissonette et al.
6,352,205	B1		3/2002	Mullins et al.
6,370,525	B1		4/2002	Kaufman
6,375,084	B1		4/2002	Stanford et al.
6,422,462	B1		7/2002	Cohen
6,456,984	B1	*	9/2002	Demoff et al. 705/40
6,466,901	B1		10/2002	Loofbourrow et al.
6,470,490	B1		10/2002	Hansen
6,484,166	B1		11/2002	Maynard
6,598,031	B1		7/2003	Ice
6,636,833	B1		10/2003	Flitcroft et al.
6,885,857	B1		4/2005	Hanson
2001/0011249	A1	*	8/2001	Yanagihara et al. 705/41
2002/0077837	A1		6/2002	Krueger et al.
2002/0116341	A1		8/2002	Hogan et al.
2002/0120587	A1		8/2002	D'Agostino
2002/0152158	A1		10/2002	Paleiov et al.
2003/0018567	A1		1/2003	Flitcroft et al.
2003/0028481	A1		2/2003	Flitcroft et al.

2003/0097331	A1	5/2003	Cohen	
2003/0216997	A1	11/2003	Cohen	
2010/0012720	A1*	1/2010	Baker-Dean et al.	235/380

FOREIGN PATENT DOCUMENTS

EP	0 081 921	A1	6/1983
EP	0 515 448	A1	12/1992
EP	0 590 861	A2	4/1994
EP	0 590 861	A3	4/1994
EP	0 590 961	A2	4/1994
FR	2 661 996	A1	11/1991
GB	2 145 265	A	3/1985
GB	2 252 270	A	8/1992
GB	2 305 393		4/1997
GB	2 327 831	A	2/1999
GB	2 361 790	A	10/2001
JP	06-282556		10/1994
WO	WO 91/12680		8/1991
WO	WO 91/12693		8/1991
WO	WO 93/14476		7/1993
WO	WO 95/07512		3/1995
WO	WO 96/08756		3/1996
WO	WO 96/42150		12/1996
WO	WO 97/15893		5/1997
WO	WO 97/19549		5/1997
WO	WO 98/26376		6/1998
WO	WO 98/30985		7/1998
WO	WO 99/49424		9/1999
WO	WO 00/42486		7/2000

OTHER PUBLICATIONS

Jones, R.: Prepaid cards, an emerging internet payment mechanism, the Nuvantage Group, Jun. 2001, pp. 1-9.*

Anne Finnigan. *The Safe Way to Shop Online*, Good Housekeeping, pp. 1-2 (Sep. 1998).

Blake Ives & Michael Earl. *Mondex International Reengineering Money*, London Business School Article, isds.bus.lsu.edu/cases/mondex.html, Nov. 1, 2001.

Bob Woods. *New Dell E-Commerce Guarantee Called 'Weak'*, Newsbytes News, pp. 1-2 (Sep. 1998).

CITI.COM, *Total Fraud Protection . . . Solutions for Your Safety and Peace of Mind* (printout) CBSD002144-CBSD002153.

Eran Gabber & Abraham Silberschatz. *A Minimal Distributed Protocol for Electronic Commerce*, www.usenix.org/publications (Article), Oakland, USAa, Nov. 18-21, 1996.

GE Capital Financial Inc., *GE Pre-Authorization System* (GE's website printout).

Jones, R. *Prepaid Cards, An Emerging Internet Payment Mechanism*, The Nuvantage Group, Jun. 2001, pp. 1-9.

Keith Lamond. *Credit Card Transactions Real World and Online*, www.virtualschools.edu/mon/ElectronicProperty/klamond/credit_card.htm, Sep. 11, 2001.

Larry Chase. *Taking Transactions Online*, Target Marketing, pp. 1-4 (Oct. 1998).

Lee, et al. *Evolutionary Business Models of e-Cash with Smart Cards*, Korea Advanced Institute of Science and Technology, Korea, http://koasas.kaist.ac.kr/bitstream/10203/4774/1/2000-092.pdf, pp. 352-358.

Matt Barthel. *Diebold Plans Major Push in Market for Debit-Card Point of Sale Terminals*, American Banker, pp. 1-2 (Sep. 28, 1993).

Netchex—A Short Brief, www.tml.hut.fi/Studies/Tik-110.50/1997/Ecomerce/netchex-5html (Article), Nov. 5, 2002.

Owen Thomas. *Money Changers*, www.ecompany.com (Article), Oct. 2000.

Paul Demery. *Attaching the Smart Card Fortress*, Credit Card Management, pp. 1-4 (Sep. 1998).

Putting Risk in Perspective (Article), *Internet Outlook* (Jul. 20, 1997), vol. 1, No. 3, www.webreference.com.

Re-examination of U.S. Patent No. 6,324,526 granted to John D'Agostino, assigned U.S. Appl. No. 90/007,481, filed Mar. 28, 2005.

Smart Card New Ltd's Information Gateway, www.smartcard.co.uk/articles/electronicmoney.html, Nov. 1, 2001.

Smart Cards, disc.cba.uh.edu (printout), Nov. 1, 2001.

Steven P. Ketchpel & Andreas Paepcke. *Shopping Models: A Flexible Architecture for Information Commerce*, dbpubs.stanford.edu:8090, Oct. 1, 2002 (Stanford, USA).

Vincent Moscaritolo & Robert Hettinga. *Digital Commerce for the Rest of Us Apple in a Geodesic Economy*, www.shipwright.com/rants/rant_15.html (Article), Sep. 4, 1996.

Virtual Credit Card (VCC), www.geocities.com/Eureka/Park/5014/vcc.htm (printout). Jun. 28, 1999.

* cited by examiner

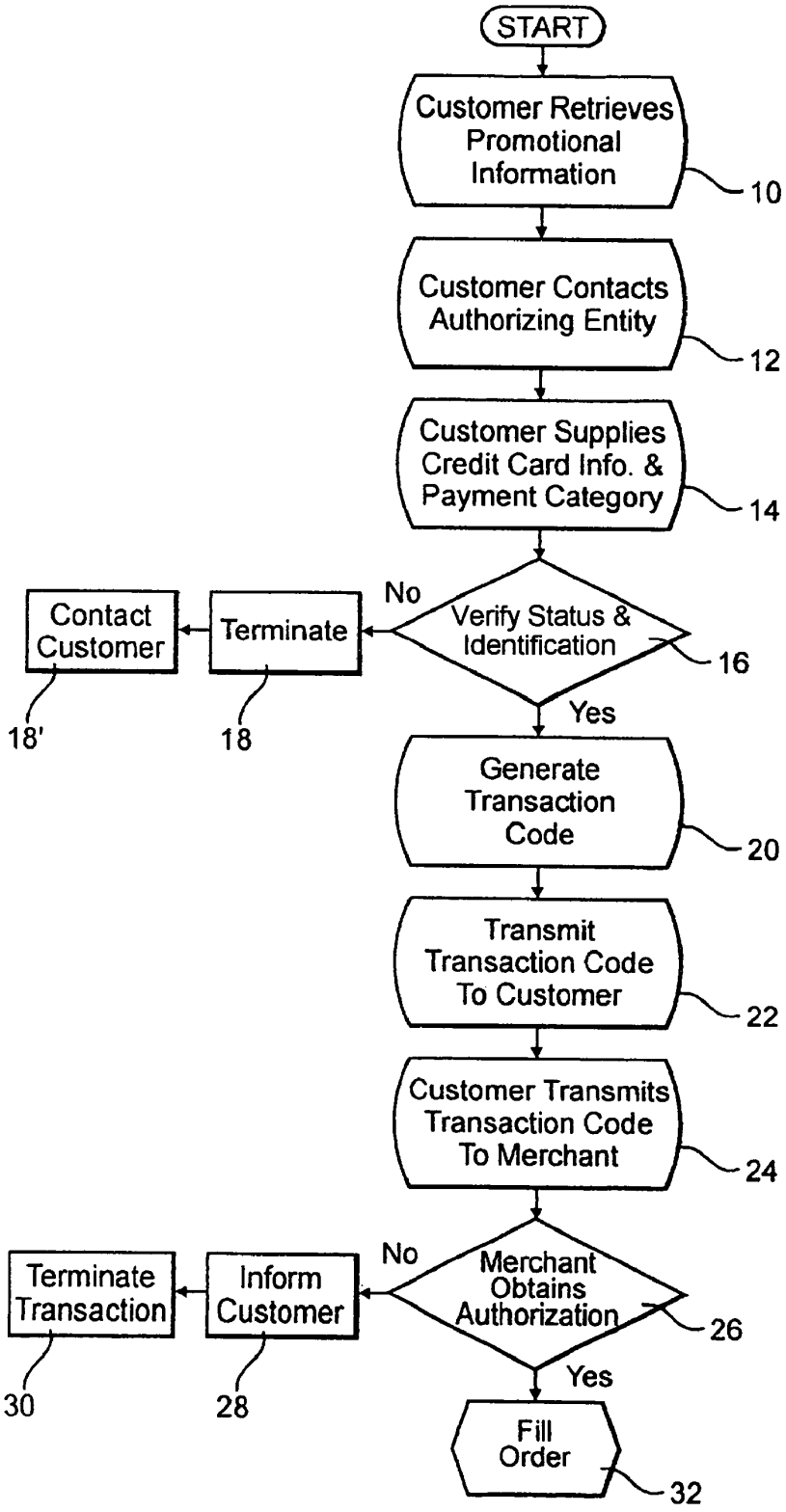

START
Customer Retrieves Promotional Information
10
Customer Contacts Authorizing Entity
12
Customer Supplies Credit Card Info. & Payment Category
14
Verify Status & Identification
16
No
Terminate
18
Contact Customer
18'
Yes
Generate Transaction Code
20
Transmit Transaction Code To Customer
22
Customer Transmits Transaction Code To Merchant
24
Merchant Obtains Authorization
26
No
Inform Customer
28
Terminate Transaction
30
Yes
Fill Order
32

FIG. 1

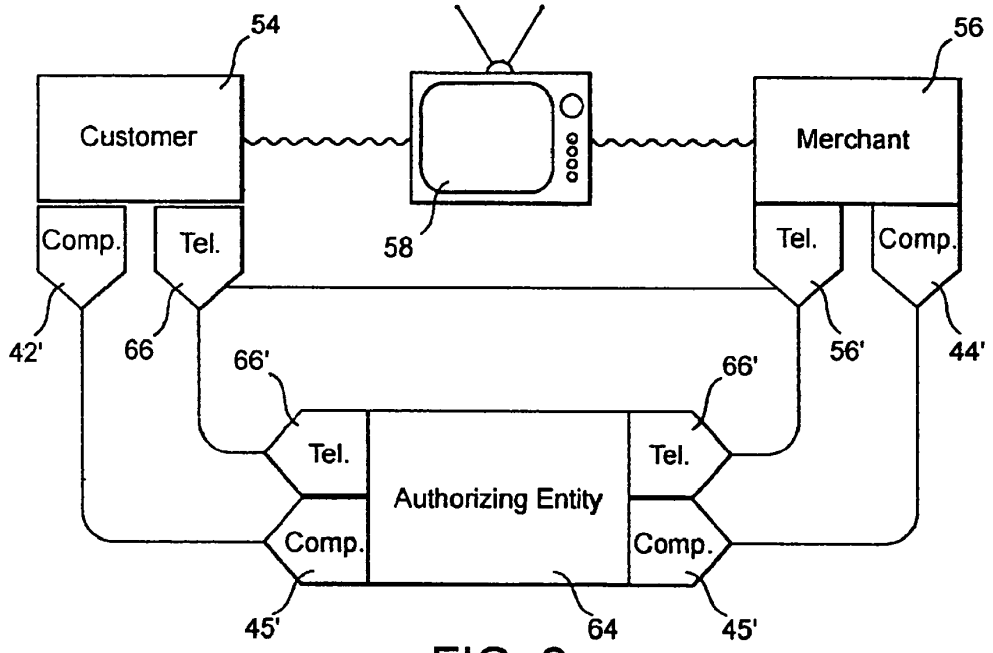

54
56
Customer
Merchant
58
Comp.
Tel.
Tel.
Comp.
42'
66
66'
66'
56'
44'
Tel.
Tel.
Authorizing Entity
Comp.
Comp.
45'
64
45'

FIG. 2

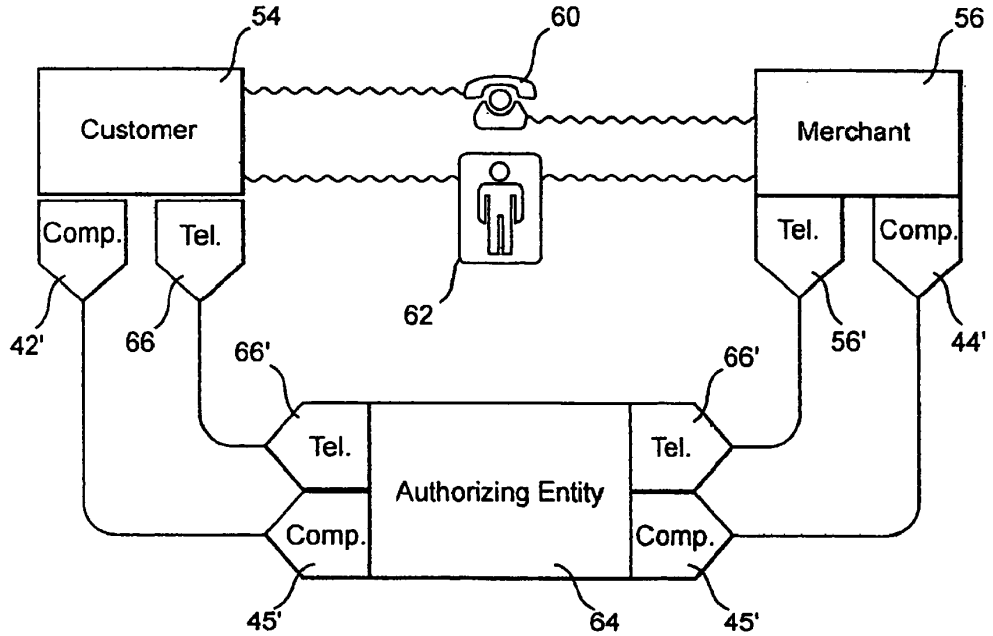

54
60
56
Customer
Merchant
Comp.
Tel.
Tel.
Comp.
62
42'
66
66'
66'
56'
44'
Tel.
Tel.
Authorizing Entity
Comp.
Comp.
45'
64
45'

FIG. 3

SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD TRANSACTIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of pending U.S. patent application Ser. No. 11/252,009, filed on Oct. 17, 2005, which is a continuation of U.S. patent application Ser. No. 10/037,007, filed on Nov. 4, 2001, which is a continuation-in-part of U.S. patent application Ser. No. 09/231,745, filed on Jan. 15, 1999 and now U.S. Pat. No. 6,324,526, issued on Nov. 27, 2001, which the entirety of each are incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to a system and method of performing secure credit card purchases in connection with remote commercial transactions, wherein a credit card holder does not have to reveal their credit card number to a merchant or a mechanism controlled by the merchant in order to accomplish a purchase, and wherein the merchant is still assured of the necessary credit verifications and approvals prior to authorizing and/or completing a credit card transaction, thereby increasing overall security by minimizing any access to credit card numbers without having to substantially modify or deviate from existing, accepted credit card transaction practices.

2. Description of the Related Art

The utilization of credit and debit cards to conduct transactions is ever increasing. This is especially the case with remote or "mail-order" transactions wherein merchants desire to be assured of a payment prior to shipping a product. For example, recent years have seen a substantial increase in the popularity of televised shopping networks to further supplement the popularity of catalogue type sales. Moreover, the increasing use and popularity of distributed computer networks such as the internet has also contributed to the dramatic increase in the number of remote commercial transactions conducted every day.

One primary reason associated with the rapid growth of remote commercial transactions is the ability of a merchant to reach an almost limitless number of potential customers at a substantially insignificant cost and with little or no operating overhead since an actual store is not required. Additionally, such sales techniques permit customers to view the products and services in a greatly expanded marketplace, representing a great number of vendors, without extensive travel and without foregoing the privacy and convenience of their home or other predetermined computer site in some cases. Simply put, a telephone or like communication avenue is all that is needed to place the consumer in contact with the merchant and complete the transaction.

The vast increase in popularity of remote commercial transactions conducted over the telephone or internet is further facilitated by the relatively simple protocols and procedures necessary to conduct such transactions. In particular, in order to complete a valid transaction, a merchant need not physically see the customer or the credit card, but must merely accept and enter a customer's credit card account number and an expiration date thereof to obtain authorization. This same convenience, however, is the primary disadvantage and/or problem associated with conducting commerce in the manners set forth above. Specifically, there is a great reluctance on the part of the customer to transmit the credit card account information, including the credit card number,

because of the proliferation of fraud, and a well recognized lack of security directed to the protection of such account information. Indeed, it has been established that security and privacy concerns are realistic due to the fact that credit card account data is easily readable or interceptable by unauthorized parties, and can be readily used for all types of remote transactions with minimal risk of being physically caught. In fact, unscrupulous individuals have many ways of gaining access to a consumer's legitimate remote transactions and thereby obtaining the credit card information. This information can be obtained from old credit card receipts or even from the unauthorized notation and use of the information by merchants or their employees after a legitimate transaction is made. Naturally, the latter is the most difficult to prevent utilizing known methods and systems unless a consumer is willing to completely forego the use of a credit card for purchases.

In the case of computerized remote transactions, as messages, including account data or other confidential information, move across the internet, they can easily pass through numerous computers, any one of which can be utilized to copy such confidential information or data, thereby leading to a further risk of potential fraud when conducting such transactions. Presently, some companies currently seek to address such security and privacy concerns by the employment of encryption programs and techniques. To this end there is an extensive facility associated with both public and private encryption schemes being deployed in order to guard the private or secured information being transmitted across the internet or like world wide networks. Unfortunately, however, even with such encryption techniques, the account information must usually still ultimately be transmitted to a third party who did not previously have access to that information previously. Even some more sophisticated systems which seek to interpose a separate computer or encryption entity between the consumer and the merchant so as to obtain authorization and forward it to the merchant, that information must still be made available to and/or transmitted to that third party, thereby leaving open an avenue for fraud or theft. Further, such encryption techniques, even if minimally effective for computerized remote transactions, are not truly useable for other conventional types of remote transactions, or even normal in person transactions.

Based on the above, there is an obvious need in the field of art associated with remote commercial transactions for a system and method of performing secure credit card purchases of goods and services which truly reduces the risk of potential fraud and theft by eliminating outside access to a consumer's private credit card information without requiring complex encryption equipment or significantly altering the ease and convenience of current transaction techniques. Further, such a system and method should also be effective for use in conventional, "in person" transactions as well, thereby providing an added measure of security and minimizing the hazards associated with the passing on of account information by unscrupulous merchants. Also, such a system should provide limits to potential loss or liability in a manner which does not impede the transaction.

SUMMARY OF THE INVENTION

The present invention is directed towards a system and method of performing secure credit card purchases, wherein payment for goods or services purchased is efficiently accomplished while eliminating the necessity of disclosure or dissemination of a consumers specific credit card number or other account data which the customer or other individual

may wish to maintain in confidence. The system and method of the present invention incorporates the advantage of consummating the purchase by the customer through the selection of any one of a plurality of predetermined payment categories. Collectively, the payment categories represent a variety of methods for accomplishing payment for a fixed transaction, a multiple transaction and/or a repeating transaction.

One embodiment of the system and method of the present invention comprises a customer receiving information, including specific data necessary for the purchase of any given product or service. This promotional information generated by the merchant can be received by any of a plurality of conventional means including advertisements, catalogues, computer network connections, direct person to person customer and merchant contact, telephone solicitation, mail orders, etc. Once the customer has identified the product or services which he/she wishes to purchase, the customer contacts and supplies a custodial authorizing entity with the requisite information concerning both the identification of a specific credit card or debit card account and a requested payment category. Additionally, security against unauthorized use of confidential account data may also preferably include information relating to the merchant's identification and/or location.

The custodial authorizing entity is preferably defined as the entity which has or has been assigned the custodial responsibility for the financial account data of a customer's credit card account, including a previous knowledge of the credit card number and other information such as credit limits, payment history, available credit amounts and other information which will determine the status of a given credit card account in terms of authorizing a requested payment for a current purchase.

As part of the security system for accomplishing a commercial transaction utilizing credit card or debit card payment, the custodial authorizing entity includes sufficient facilities, preferably including a processing computer or like applicable hardware for the generation of an exclusive transaction code. The transaction code is to be used in substitution for the credit card number and when utilized as authorized, will issue the merchant a credit approval, and will accomplish payment for the goods or services desired in the normal fashion normally associated with a credit or debit card transaction, without the publication or dissemination of an identifying credit card number for a specific customer's account to any entity that is not already aware of that information.

Further, a feature of the transaction code is its ability to indicate any one of preferably a plurality of predetermined payment categories which may be either requested by the customer or automatically chosen by the custodial authorizing entity based on the type of account or the type of purchase or other commercial transaction involved. Each of the payment categories are reflective of a different type of payment desired or required to consummate the intended purchase. More specifically, the plurality of payment categories may include a single transaction involving a specific dollar amount for a purchase within a specific time period, such as twenty four hours, during which authorization of the purchase remains valid. Alternately, a single transaction may be involved wherein a maximum limit or a dollar amount is determined above which the purchase will become invalidated and further wherein a fixed period of time is preferably established for maintaining authorization of such purchase. Other alternatives would involve one or more of the categories coded to define multiple transactions involving a maximum dollar amount for purchases, as well as a fixed period of time for authorization of such purchases, and/or a repeating transaction wherein payments may be automatically accessed by a merchant over a predetermined or unspecified time interval (such as every thirty days) for a specific dollar amount or a maximum dollar amount limit. Also, limits solely as to a specific merchant or a given time period can be effectively established for which the transaction code is valid.

A further feature of the present invention to be described in greater details hereinafter, is the requirement that the transaction code, once received by the customer is transmitted to the merchant by the customer or a person specifically authorized by the customer. Only minimal contact by the merchant and the custodial authorizing entity is provided for purposes of the merchant verifying the validity of the transaction code utilizing a conventional process electronically or otherwise similar to the verification of a credit card number normally offered to a merchant for the purchase of goods or services. There is, therefore, no disclosure, publication or other dissemination of the specific credit card number of a given customer account beyond those entities who already know the information, and the transaction code is transmitted exclusively to the customer by the custodial authorizing entity who has the ability to better identify whether the customer is properly authorized to use the account. Moreover, the transaction code, once given out by the customer, only has a limited usefulness, thereby limiting the risk of misuse and minimizing the potential losses to be experienced by the credit card company and/or the account holder.

Accordingly, it is an object of the present invention to provide a system and attendant method for performing remote commercial transactions utilizing credit cards, which maximizes the security of the transaction and limits the potential liability to be experienced from a fraudulent transaction.

Yet another object of the present invention is to provide a secure system and method for establishing credit card purchases which eliminate the disclosure or dissemination of the actual credit card number to anyone other than a custodial authorizing entity which normally has custodial responsibilities for account information including the previously established credit card number.

It is another object of the present invention to provide a system and method of establishing secure credit card purchases through the generation of a transaction code which renders it extremely difficult or impossible to access or infiltrate a customer's credit card account by unauthorized means.

It is yet another object of the present invention to provide a secure method of completing a remote commercial transaction which eliminates the need to convey actual account information to a merchant, but which allows the merchant to conduct a normal verification of information needed to consummate a given purchase.

It is also an object of the present invention to provide a system and attendant method of accomplishing secure credit card purchases which eliminates the need to disclose or disseminate a given credit card number while providing the customer with the versatility of choosing any one of a plurality of predetermined payment categories.

It is yet another feature of the present invention to provide a system and method of accomplishing secure credit card payments having the versatility of allowing the customer to select any one of a plurality of payment categories which are indicative of a variance in the amount of a purchase as well as the time in which authorization for such payment is valid.

These and other objects, features and advantages of the present invention will become more clear when the drawings as well as the detailed description are taken into consideration.

BRIEF DESCRIPTION OF THE DRAWINGS

For a fuller understanding of the nature of the present invention, reference should be had to the following detailed description taken in connection with the accompanying drawings in which:

FIG. **1** is a schematic representation of a flow chart showing various steps involved in the performance of the system and method of the present invention for the secure credit card purchasing;

FIG. **2** is a schematic representation similar to that of FIG. **1** wherein customer to merchant contact is accomplished by conventional facilities such as television; and

FIG. **3** is a schematic representation similar that of FIG. **2** wherein customer to merchant contact is established either by phone or in person.

Like reference numerals refer to like parts throughout the several views of the drawings.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

As shown in the accompanying Figures, the present invention is directed towards a system and method for accomplishing secure credit card purchases. Moreover, these purchases can be "in person", but preferably include remote commercial transactions such as mail order, purchases over the internet, television solicitations, telephone solicitations, etc. Security is establish by virtue of the elimination of the need to disclose an active credit card number and expiration date to the merchant or any other party other than the original credit card company, issuing bank or like financial institution which already has custodial responsibilities for the financial or account data associated with a given customer's credit card account.

More specifically and with reference to FIG. **1** the system as well as an attendant method is preferably instigated by the customer viewing a product, identifying a desired amount for a transaction and/or receiving promotional information as at **10**, either in person or by any of the electronic or more conventional techniques which will be described in greater detail with reference to FIGS. **2** through **3**. Once the customer reviews the product or promotional information and has sufficient information, such as including price, product or service identification, payment requirement, etc., regarding the remote commercial transaction to be conducted, the customer contacts, either by computer, telephone or in person, a custodial authorizing entity as at **12**. The custodial authorizing entity may herein be defined as comprising that entity or institution which has or has been designated by the entity which has custodial responsibility for the financial data and security of a given credit card account of a customer. As set forth above such custodial authorizing entity can be represented by the credit card company issuing a credit card to a given customer or alternately can be represented by a bank or other financial institution serving to sponsor a credit card or debit card to the extent of processing the debits and credit associated therewith. The authorizing entity's custodial responsibilities of course includes the previous knowledge and/or storage of the credit card number serving to identify a specific customer's credit card account. Once contacted, the customer then supplies appropriate identification data to inform the custodial authorizing entity of a specific customer's credit card account as at **14**. In addition, the customer will supply the custodial authorizing entity with additional required information needed to consummate the purchase as well as ensure the security of the account in order to prevent its unauthorized use. Such additional information may preferably include the identification of the merchant or merchants involved, when such information is deemed necessary, and a requested one of a plurality of predetermined payment categories to facilitate consummation of the purchase of the products or services desired. Such predetermined plurality of payment categories will be discussed in greater detail hereinafter.

Once the appropriate information has been received from the customer as indicated at **16**, the custodial authorizing entity verifies the credit card status and account identification of the customer to determine the viability of the account in terms of dollar amount limits, payment history, available credit balance, etc. If the accessed credit card account is not in good standing, the custodial authorizing entity will permanently or temporarily terminate the transaction as at **18** and/or communicate to the customer directly as at **18'** by any applicable means for purposes of informing the customer of the unacceptable status of the accessed credit card account. If the credit card account is in good standing, based at least in part on the requested payment category, (amount of payment), the custodial authorizing entity generates a transaction code as at **20**. The transaction code is used in substitution for the specific credit card number which would normally identify a customer's credit card account and would allow access thereto by any entity having possession of the credit card number whether or not such possession was authorized or unauthorized. More specifically, the transaction code is pre-coded to be indicative of a specific credit card account, preferably a merchant or merchants identification and a designated payment category, selected from the plurality of predetermined payment categories as set forth above. Once generated, the transaction code is communicated exclusively to the authorized and verified customer by the custodial authorizing entity as at **22**, wherein the system and method of the present invention preferably restricts communication between the custodial authorizing entity and the merchant except to conduct a normal verification as will be explained.

The verified customer thereafter and preferably within a time limit to be determined by the customer and pre-coded in association with the transaction code, will directly or through an authorized representative communicate the transaction code to the merchant as at **24**. The system and method of the preferred embodiment of the present invention contemplates that only the verified customer will transmit the generated transaction code to the merchant in the case of a remote commercial transaction, thereby limiting knowledge of the transaction code to those parties having a need to know. Of course, however, as the transaction code will generally have a limited value as defied by the verified customer when obtained, the verified customer may designate an agent or other entity to act as the customer on his/her behalf, with the amount of potential liability to be experienced by such a transaction to be limited to the amount defined by the verified customer when obtaining the transaction code.

At this point the purchase is consummated at least from the customer standpoint in that the customer has previously established the acceptable status of the account. Therefore the customer feels free to disclose the transaction code to the merchant or merchants instead of the actual credit card number as at **22**, **24** and is relatively unconcerned if the transaction code is published or otherwise disseminated to unauthorized

entities. In a preferred embodiment wherein a merchant identifier is pre-coded in association with the transaction code, the pre-coding of the transaction code will prohibit an unauthorized use due at least in part to the fact that the merchant is specifically identified and any attempt to use the transaction code other than by the identified merchant will be prohibited. In addition, the merchant is prevented from "overcharging" or "extending" the purchase by fixing the dollar amount to satisfy the specific cost or limit of the purchase as well as a specific time limit or time parameters in which the authorization for payment is valid. Such information, as set forth above, is communicated by the requested and subsequently designated payment category as set forth above. Restricted communication between the merchant and the custodial authorizing entity as at **26** is permitted exclusively for purposes of verification of the transaction code in a manner, which may utilize, at least to some extent, conventional facilities for the verification of a credit card number by most merchants or like commercial establishments. As a result, the merchant also has a desired verification as to the validity of a transaction and can effectively make arrangements to be paid by the credit card company.

If for some reason the transaction code is refused verification, the customer may be informed directly by the merchant as at **28** and or the transaction may be terminated as at **30**. Assuming verification of the transaction code by the custodial authorizing entity, the merchant proceeds to consummate the purchase and send the order, as at **32**, in the case of a remote commercial transaction.

FIGS. **2** and **3** are representative of the versatility of the system and method of the present invention wherein the customer **54** may receive the aforementioned promotional information from the merchant **56** by any appropriate means such as television solicitation as at **58**, phone solicitation as at **60** and/or personal solicitation as at **62**. Once the customer receives the promotional information, which may include the viewing of the product itself, or in advance if a general estimate as to the ultimate cost of an anticipate purchase(s) can be made prior to viewing promotional information, the customer contacts the custodial authorizing entity **64** by any appropriate electronic or conventional facilities such as direct phone to phone contact as at **66** and **66'** or direct computer contact as at **46'**, **45'**. Once the customer's authorization is confirmed, details of the anticipated transaction are established so as to determine a payment category, and the a transaction code is issued to the customer. The customer, either directly or through a representative, can then utilize the transaction code to consummate a transaction within the defined parameters of the payment category. Moreover, the merchant **56**, through a conventional, yet restricted communication with the custodial authorizing entity **64** by any of a plurality of conventional or electronic methods using computer to computer linking as at **44'**, **45'** or by telephone transmission as at **56'**, **66'**, can obtain a verification and subsequent payment utilizing the transaction code only.

As emphasized above, an important feature of the present invention is the ability of the customer to request a desired or a required payment category and the ability of the custodial authorizing entity **64** and/or a processing computer **45** of the custodial authorizing entity to issue a transaction code in accordance with the payment category. The payment categories, may be collectively defined as a variety of different types of transactions. Such transactions may include a single transaction for a specific amount of a purchase to be consummated. Alternatively, the payment category may include a single transaction defined by a single purchase having a maximum limit amount, wherein the specific or precise cost of the purchase has not been determined for a variety of reasons, and as such, the customer desires to set a maximum amount for which the single transaction may be made. Accordingly, with such a payment category, the exact amount may not be known in advance, but the customer is assured of not paying over the specifically designated maximum limit. In addition, the transactions are preferably, but not necessarily, authorized to be conducted only over a fixed life period of time, such as within twenty four hours, thereby ensuring that an outstanding transaction code does not remain valid if not used as generally intended. This limited time period can, of course be varied or omitted depending upon the wishes of the customer and/or the policies of the custodial authorizing entity. Also, these or any other payment category transactions may include a specific merchant identification to further restrict use of the transaction code.

The payment category may also include a multi-transaction authorization wherein more than one purchase may be made from one or a plurality of different merchants, each of which may or may not be identified by the customer and pre-coded in association with the transaction code, and wherein a total cost of the plurality of purchases may not exceed a maximum limit amount. This transaction can also be limited to having to take place within a predetermined, designated fixed life span, such as but not limited to twenty four hours. Accordingly, in some instances wherein a customer, or an agent of the customer, such as a child, guardian, or care giver, must make a number of transactions or purchases which are authorized by the customer, the customer may designate a maximum amount which can be spent utilizing a particular transaction code within a predetermined period of time, and/or can designate that only one merchant, whether designated or not, can use the transaction code.

As yet another alternative, the payment category may include a repeating transaction for a specific amount to be paid in each of a fixed number of intervals. For example, the customer may which to join a gym or receive services or products over a fixed number of payment intervals, such as every thirty days. Accordingly, the merchant will be authorized to charge the credit card account designated by the corresponding transaction code a fixed monthly payment. Similarly, a repeating transaction for a stated minimum interval such as every thirty days may be authorized for a specific amount for an unspecified number of intervals wherein the merchant will be authorized to continuously obtain payment on a "monthly" basis until the customer decides to cancel such authorization.

Since many modifications, variations and changes in detail can be made to the described preferred embodiment of the invention, it is intended that all matters in the foregoing description and shown in the accompanying drawings be interpreted as illustrative and not in a limiting sense. Thus, the scope of the invention should be determined by the appended claims and their legal equivalents.

What is claimed is:

1. A method of performing secure credit card purchases, said method comprising:

a) contacting a custodial authorizing entity having custodial responsibility of account parameters of a customer's account that is used to make credit card purchases;

b) supplying said custodial authorizing entity with at least account identification data of said customer's account;

c) defining at least one payment category to include at least limiting a number of transactions to one or more merchants, said one or more merchants limitation being

included in said payment category prior to any particular merchant being identified as one of said one or more merchants;

d) designating said payment category;

e) generating a transaction code by a processing computer of said custodial authorizing entity, said transaction code reflecting at least the limits of said designated payment category to make a purchase within said designated payment category;

f) communicating said transaction code to a merchant to consummate a purchase with defined purchase parameters;

g) verifying that said defined purchase parameters are within said designated payment category; and

h) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said designated payment category and to authorize payment required to complete the purchase.

2. The method of claim **1** further comprising the step of designating at least one of said one or more merchants subsequent to generating said transaction code.

3. The method of claim **1** wherein said step of communicating the transaction code to a merchant to consummate said purchase within defined purchase parameters further comprises designation of said merchant as one of said one or more merchants.

4. The method of claim **1** wherein said step of generating said transaction code further comprises said customer obtaining said transaction code.

5. The method of claim **1** further comprising generating a transaction code which reflects at least one of a plurality of said payment categories.

6. The method of claim **1** further comprising defining at least one payment category to include amount parameters for a cost of one or more purchases.

7. The method of claim **1** further comprising defining at least one payment category to include time parameters during which the purchase can be completed.

8. The method of claim **1** further comprising defining at least one payment category to include limiting said transaction code to a single transaction for a purchase within a predetermined period of time.

9. The method of claim **1** further comprising defining at least one payment category to include limiting purchases to a single transaction at a maximum amount for purchase within a predetermined period of time.

10. The method of claim **1** further comprising defining at least one payment category to include limiting purchases to at least two purchases at a maximum total amount for items purchased within a predetermined time period.

11. The method of claim **1** further comprising defining at least one payment category to include using said transaction code for at least two purchases for a repeating transaction at a fixed amount payable at each of a fixed number of time intervals.

12. The method of claim **11** further comprising defining at least one payment category to include limiting purchases to said repeating transaction at said fixed amount payable at each of said fixed number of time intervals.

13. The method of claim **1** further comprising defining at least one payment category to include using said transaction code for a repeating transaction at a fixed amount payable at each of an unspecified number of time intervals.

14. The method of claim **1** further comprising defining at least one payment category to include limiting a repeating transaction to a maximum dollar amount.

15. The method of claim **1** further comprising defining at least one payment category to include limiting purchases to a limited time interval during which a purchase is permitted.

16. The method of claim **1** further comprising communicating said transaction code to the customer at the location of the merchant for use in person.

17. A method of performing secure credit card purchases, said method comprising:

a) identifying a pre-established account that is used to make credit card purchases;

b) selecting a predetermined payment category which limits a nature, of a series of subsequent purchases to one or more merchants, said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants;

c) generating a transaction code by a processing computer of a custodial authorizing entity of said pre-established account, said transaction code associated with at least said pre-established account and the limits of said selected payment category and different from said pre-established account;

d) communicating said transaction code to a merchant to consummate a purchase within defined purchase parameters;

e) verifying that said defined purchase parameters correspond to said selected payment category;

f) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said selected payment category and to authorize payment required to complete the purchase; and

g) associating the purchase with said pre-established account.

18. The method of claim **17** wherein said step of verifying that said defined purchase parameters correspond to said selected payment category further identifies said merchant as one of said one or more merchants.

19. A method of performing secure credit card purchases, said method comprising the steps of:

a) identifying a pre-established account that is used to make credit card purchases;

b) selecting a pre-determined payment category which limits a nature of a subsequent purchase to one or more merchants, said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants;

c) generating a transaction code by a processing computer of a custodial authorizing entity of said pre-established account, said transaction code associated with at least said pre-established account and the limits of said selected payment category, and different from said pre-established account;

d) designating a merchant as one of said one or more merchants;

e) communicating said transaction code to said merchant to consummate a purchase within defined purchase parameters;

f) verifying that said defined purchase parameters correspond to said selected payment category;

g) providing authorization for said purchase so as to confirm at least that said defined purchase parameters are within said selected payment category and to authorize payment required to complete the purchase; and

h) associating the purchase with said pre-established account.

20. The method of claim 19 wherein said step of verifying that said defined purchase parameters correspond to said selected payment category further identifies said merchant as one of said one or more merchants.

21. A method for implementing a system for performing secure credit card purchases, the method comprising:

a) receiving account information from an account holder identifying an account that is used to make credit card purchases;

b) receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant, said single merchant limitation being included in said payment category prior to any particular merchant being identified as said single merchant;

c) generating a transaction code utilizing a processing computer of a custodial authorizing entity, said transaction code associated with said account and reflecting at least the limits of said payment category, to make a purchase within said payment category;

d) communicating said transaction code to said account holder;

e) receiving a request to authorize payment for a purchase using said transaction code;

f) authorizing payment for said purchase if said purchase is within said payment category.

22. A method for implementing a system for performing secure credit card purchases, the method comprising:

a) receiving account information from an account holder identifying an account that is used to make credit card purchases;

b) receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to one or more merchants, said one or more merchants limitation being included in said payment category prior to any particular merchant being identified as one of said one or more merchants;

c) generating a transaction code utilizing a processing computer of a custodial authorizing entity, said transaction code associated with said account and reflecting at least the limits of said payment category, to make a purchase within said payment category;

d) communicating said transaction code to said account holder;

e) receiving a request to authorize payment for a purchase using said transaction code;

f) authorizing payment for said purchase if said purchase is within said payment category.

23. The method of claim 21 wherein the step of receiving account information from an account holder identifying an account that is used to make credit card purchases further comprises receiving information identifying a credit card account.

24. The method of claim 21 wherein the step of generating a transaction code utilizing a processing computer of a custodial authorizing entity further comprises generating a transaction code which reflects at least one of a plurality of predetermined payment categories.

25. The method of claim 21 wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant further comprises receiving a request from said account holder for a transaction code to make a purchase within a payment category that is automatically chosen by a custodial authorizing entity.

26. The method of claim 21 wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant further comprises receiving a request from said account holder for a transaction code to make a purchase within a payment category that includes limiting a repeating transaction to a maximum dollar amount.

27. The method of claim 21 wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant further comprises receiving a request from said account holder for a transaction code to make a purchase within a payment category that includes limiting purchases to a minimum time interval after which a subsequent purchase is permitted.

28. The method of claim 21 wherein the step of communicating said transaction code to said account holder further comprises communicating said transaction code to said account holder at the location of the merchant for use in person.

29. The method of claim 21 wherein said step of receiving a request to authorize payment for a purchase using said transaction code further identifies said single merchant.

30. The method of claim 21 wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to a single merchant further comprises receiving a request from said account holder for a transaction code to make a purchase within a predetermined payment category that is further limited in accordance with transaction details provided by said account holder.

31. The method of claim 22 wherein the step of receiving account information from an account holder identifying an account that is used to make credit card purchases further comprises receiving information identifying a credit card account.

32. The method of claim 22 wherein the step of generating a transaction code utilizing a processing computer of a custodial authorizing entity further comprises generating a transaction code which reflects at least one of a plurality of predetermined payment categories.

33. The method of claim 22 wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to one or more merchants further comprises receiving a request from said account holder for a transaction code to make a purchase within a payment category that is automatically chosen by a custodial authorizing entity.

34. The method of claim 22 wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to one or more merchants further comprises receiving a request from said account holder for a transaction code to make a purchase within a payment category that includes limiting a repeating transaction to a maximum dollar amount.

35. The method of claim 22 wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to one or more merchants further comprises receiving a request from said account holder for a transaction code to make a purchase within a payment category that includes limiting purchases to a minimum time interval after which a subsequent purchase is permitted.

36. The method of claim 22 wherein the step of communicating said transaction code to said account holder further

comprises communicating said transaction code to said account holder at the location of the merchant for use in person.

37. The method of claim **22** wherein said step of receiving a request to authorize payment for a purchase using said transaction code further identifies a merchant as one of said one or more merchants.

38. The method of claim **22** wherein the step of receiving a request from said account holder for a transaction code to make a purchase within a payment category that at least limits transactions to one or more merchants further comprises receiving a request from said account holder for a transaction code to make a purchase within a predetermined payment category that is further limited in accordance with transaction details provided by said account holder.

* * * * *

US006422462B1

(12) **United States Patent**
Cohen

(10) **Patent No.: US 6,422,462 B1**
(45) **Date of Patent: Jul. 23, 2002**

(54) **APPARATUS AND METHODS FOR IMPROVED CREDIT CARDS AND CREDIT CARD TRANSACTIONS**

(76) Inventor: **Morris E. Cohen**, c/o 757 Third Ave., Suite 2400, New York, NY (US) 10017

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/280,483**

(22) Filed: **Mar. 30, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/079,884, filed on Mar. 30, 1998.

(51) **Int. Cl.**[7] **G06F 7/08**

(52) **U.S. Cl.** **235/381**; 235/380; 705/41

(58) **Field of Search** 235/487, 382, 235/380, 395, 492, 379; 705/35, 38, 39, 1, 20, 26, 41

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,293,424	A *	3/1994	Holtey et al.	380/23
5,696,965	A *	12/1997	Dedrick	395/610
5,705,798	A *	1/1998	Tarbox	235/379
5,706,442	A *	1/1998	Anderson et al.	395/227
5,745,654	A *	4/1998	Titan	395/22
5,749,075	A *	5/1998	Toader et al.	705/14
5,963,643	A *	10/1999	Goreta et al.	380/9
5,970,478	A *	10/1999	Walker et al.	705/35
6,003,134	A *	12/1999	Kuo et al.	713/200
6,014,645	A *	1/2000	Cunningham	705/38
6,145,741	A *	11/2000	Wisdom et al.	235/380

* cited by examiner

Primary Examiner—Thien M. Le

(57) **ABSTRACT**

Customized credit and debit cards for issuance by a person or main cardholder, the cards being limited to use in transactions at selected vendors only. Thus, for example, a parent or corporation can issue a customized card to a person or group, wherein the card is only valid for use at restaurants, airlines, hotels, certain stores, or so forth.

25 Claims, 1 Drawing Sheet

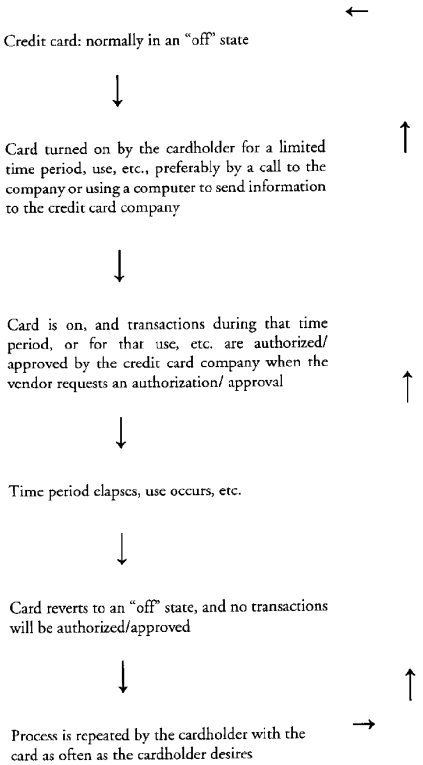
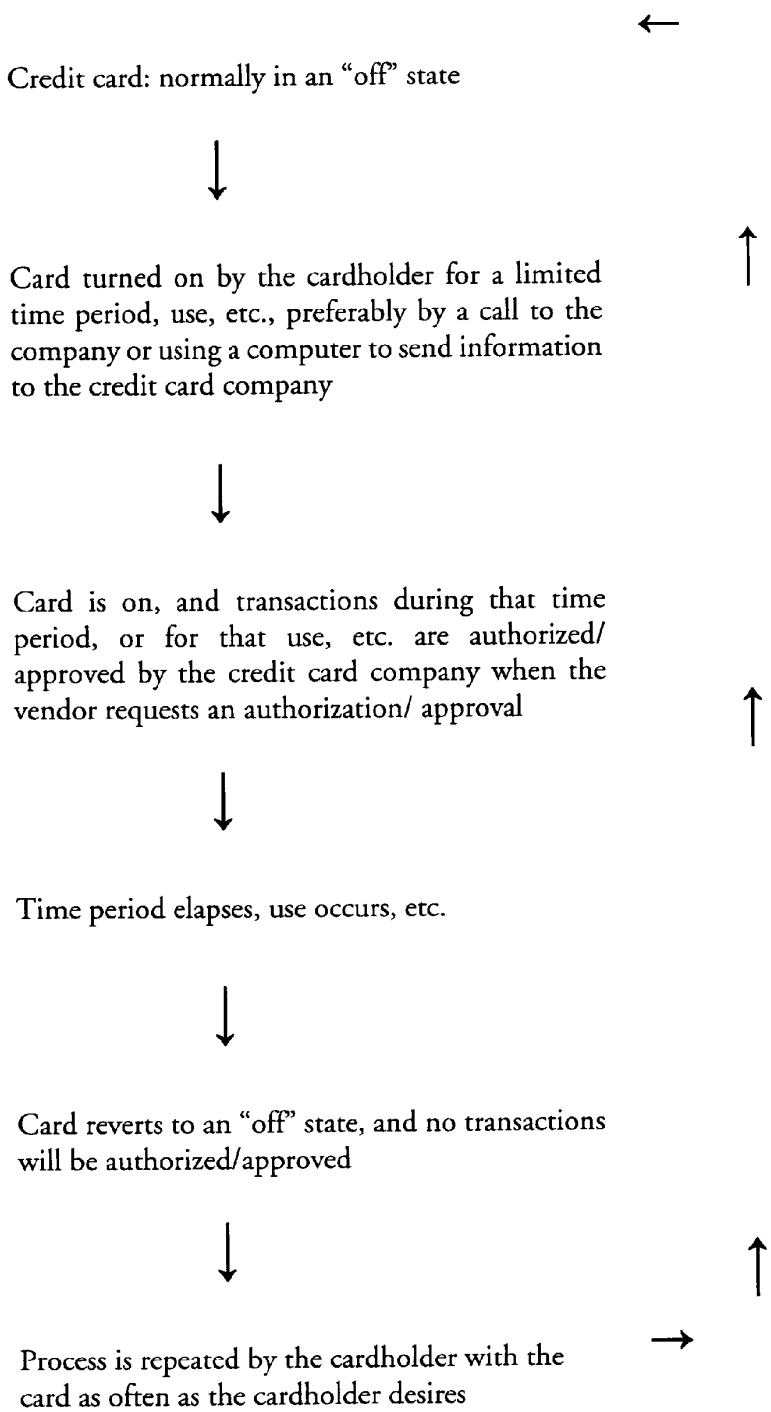


Figure 1


Credit card: normally in an "off" state
Card turned on by the cardholder for a limited time period, use, etc., preferably by a call to the company or using a computer to send information to the credit card company
Card is on, and transactions during that time period, or for that use, etc. are authorized/ approved by the credit card company when the vendor requests an authorization/ approval
Time period elapses, use occurs, etc.
Card reverts to an "off" state, and no transactions will be authorized/approved
Process is repeated by the cardholder with the card as often as the cardholder desires

APPARATUS AND METHODS FOR IMPROVED CREDIT CARDS AND CREDIT CARD TRANSACTIONS

RELATED APPLICATIONS

The present application claims all rights of priority to U.S. Provisional Application Ser. No. 60/079,884 filed Mar. 30, 1998.

BACKGROUND OF THE INVENTION

Credit cards are currently a common financial tool. Yet, credit card fraud is a considerable concern for credit card companies. The problem occurs when an unscrupulous individual obtains a copy of a person's credit card information, and then uses that information to fraudulently charge purchases to the person's card until the theft is noticed and further use of the card is blocked. In addition to being a considerable problem for the card companies themselves, this illegal practice causes inconvenience and annoyance for the innocent user whose card has somehow been compromised.

Such fraud is a potential problem in various contexts, but recently has become of significant concern in Internet transactions in particular. Transmission of credit card information over the Internet has long been suspect due to the risk of individuals monitoring traffic over the network and then using that information for their personal gain. While secure networks and connections have been increasingly available over the past several years, many are nonetheless unwilling to transmit any credit card information over the Internet, due to the possibility that valuable credit card information could be intercepted.

In addition, monitoring, control and regulation of expenditures and finances is a frequent concern of companies and individuals. It is always desirable to provide apparatus and methods which improve the apparatus and methods for such monitoring, control and regulation. Accordingly, there are numerous improvements which have been heretofore unknown in the art, which improve the effectiveness, value, and/or the efficiency of credit cards, either in general or certain types of financial transactions.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide improved credit cards and methods for credit card transactions.

It is a further object of the present invention to provide for customized use credit cards.

It is a further object of the present invention to provide for user-defined credit cards for use in financial transactions.

It is a further object of the present invention to provide for disposable credit cards.

It is a further object of the present invention to provide for limited use credit cards.

It is a further object of the present invention to provide methods and apparatus for secure transmission of credit card information.

It is a further object of the present invention to provide methods and apparatus for minimizing credit card fraud, and the amounts of loss that could occur should card information be intercepted.

It is also an object of the invention to provide methods and apparatus for transmission of credit card information over the Internet with a minimal risk of possible fraud or loss.

In addition to the prevention and reduction of fraud, it is a further object of the invention to provide improved types of credit cards, and improved methods for credit card transactions.

In accordance with the invention, a variety of new forms of credit cards and credit card methods are disclosed herein. In some of the disclosed embodiments, the cards and methods provide improved credit cards and methods providing for customization, limited use, single use (disposability), or so forth. Additionally or alternatively, in some of the disclosed embodiments, the cards and methods include new forms of credit cards designed to reduce or prevent fraud. In addition to, or as an alternative to the prevention of fraud, in some of the embodiments disclosed herein, new credit cards and associated methods are provided for the improvement of credit card transactions and/or for availability of an expanded array of financial products to consumers.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a schematic illustration of the customization of a credit card in accordance with one embodiment of the present invention.

DESCRIPTION OF THE INVENTION

In accordance with the present invention, in one embodiment of the present invention, to address the problem of credit card fraud, a new system of disposable credit card numbers is disclosed herein. These credit cards or credit card numbers are generated for a one time, single transaction basis, after which they are disposed of, or thrown away. The numbers can be used by a user over the Internet or any other communications system, whether open or secure, to effect a single transaction. After a one time use of the credit card number, the number is deactivated by the issuing credit card company such that it is no longer available for use. In this manner, a credit card company need not wait to learn whether a given credit card number has been intercepted, and one or more fraudulent purchases made (with the attendant possible loss of time, money and manpower investigating and resolving such matters) before dealing with the results of the potential theft. Rather, all numbers used over the network, or in a certain context, are assumed insecure, and once used for the first time, are no longer available for use. By doing so, the company, so to speak, "beats the thief to the punch," having already deactivated the number after a single use of the card, even before learning of the fraud.

In other embodiments of the invention, customized or limited use credit cards are provided. These cards are customized, preferably by the user, to suit the user's desires or needs. As a result, they provide methods and apparatus which have been heretofore unknown in the art, but which provide benefits that improve the efficiency, ease and uses of payment for goods and services.

Various embodiments of the inventions are possible consistent with the inventions herein. Although reference is occasionally made to either the disposable credit card embodiment or the customized credit card embodiment

herein, the features disclosed in association with one can likewise be applied to the other, as well.

With respect to the credit card's number itself, in one preferred embodiment, for example, the credit card number is indistinguishable from permanent, ordinary credit card numbers. By making the customized credit card number indistinguishable from regular numbers both users and vendors are encouraged to use the credit card in the same manner as regular credit cards.

Similarly, by making the temporary disposable numbers (or likewise the customized credit card number) indistinguishable in appearance from regular credit card numbers, a potential thief is unable to tell in advance that a particular number is a disposable number, and already not valid. This may in turn enhance the potential of catching the thief by alerting the credit card company the first time someone attempts to illegally use the pilfered number.

With respect to either the disposable or the customized credit card, relevant information (such as the expiration date etc.) can either be printed on the card or verbally transmitted to the user. Likewise, the limited use nature of the card (either in a general sense or the specific limitations), the disposability of the card, the range of dates or validity of the card, etc. may either be printed on the card or transmitted to the user, whether verbally or in writing.

In another embodiment, the customized or the disposable number is the user's regular credit card number with a series of digits or alphanumeric characters either inserted therein, or tacked on at the end. This embodiment allows each customized or disposable card to be easily noted by the user to be a mere extension of his or her regular number.

Many of the embodiments herein could be used in conjunction with a policy by the credit card company (or by the main cardholder or the user) in which purchases from Internet transactions, for example (or purchases over unsecure networks), are only accepted if made in conjunction with a disposable or customized credit card number.

The invention can be practiced according to a wide variety of embodiments. In one embodiment, for example, a user dials into her credit card company before making a transaction, and after providing the ordinary credit card number and verification data, is provided with a disposable or customized number and/or mailed, provided with, or allowed to activate a disposable or customized card for a single or a limited range use.

In one embodiment of the invention, a user can indicate in advance of purchase, on the telephone call with the credit card company, what the single use or the customized credit card number is to be used for. This can be used to provide additional security and/or control the uses of the funds placed on that card.

In another embodiment, a user could be provided, each month or each year, with a set of disposable, one time only, or customized, limited use, numbers and/or cards, which are printed on the credit card statement for use during the next month or year, or which are mailed to the user. With respect to the disposable card, the user is instructed that, after use of the number once, the number may not be used again. With respect to the customized card, the cards can either be preset for certain uses, or the cards can be ready and waiting in the user's office or home for setting to the desired use when the user is ready.

The user could also be provided with a set of paper (or thin plastic) credit cards (preferably with magnetic strips), whether along with the customer's monthly statement, with a credit card encoder, with an encoding device which attaches to the computer and/or the Internet, or otherwise. Each of these credit cards could be used once, or on a limited or customized basis, after which the credit card could be ripped up and discarded. The cards could further have printing or indicia on them to remind the user that they are for one time only or customized use.

In a further variation on this approach, the paper cards and/or the provided numbers must be used in a specific required order, for additional security. These paper credit cards or provided numbers could be unusable until activated by the user, as is the practice with new credit cards that are sent out by mail.

In another embodiment, instead of ripping the credit cards up, the cards could have a portion which the user writes on to record the type of transaction, and the amount of the transaction. Alternatively, the card could have a portion which the user signs upon receipt and a portion which is later countersigned at the vendor, to provide additional security.

These credit cards could even have a portion which the user signs and provides to a vendor in a store. No vendor would ever, under one embodiment of the system, receive or have access to the user's permanent credit card number. Rather, the vendor (for example, a restaurant in which the user has just eaten) would receive a disposable credit card from the user's supply. The vendor could read the number off the disposable or customized card, could scan the number with a bar code scanner, could read a magnetic strip on the disposable card, or so forth. Upon being used once, the credit card can be marked, if desired, to show both that it has been processed to charge money to the person's account, and to show that it is no longer usable. This disposable card could be returned to the cardholder, saved as a receipt by either of the cardholder or the vendor, be returned to the credit card company, destroyed, or so forth. As noted above, signature could be provided once, or two signature lines could be provided, for the user to sign and countersign.

As yet another example, a user could be provided with a "calculator" of sorts, of credit card like thickness, which stores a predetermined number of disposable numbers therein. After using a number once, the user has to go back to the calculator to get the next number for the next transaction. This calculator could also be provided with a PIN number to prevent a party from accessing the numbers should the user's wallet be stolen or lost.

Alternatively, a card with multiple numbers stored thereon (which become activated in a predetermined sequence) can be provided, so that the actual credit card needs to be available (not just the credit card number) to determine the next available number in the sequence. In this way no single number alone is capable of compromising the user's account for more than one transaction, or of compromising the main number in the user's account. This card could have an LED or some other visually readable means to display the next available card number (either automatically or upon activation of a PIN, if desired). As mentioned above, part of the number could be the fixed, base portion (which is a number or portion common to all of the numbers)

and part of the number could be the variable portion (a number or portion which varies). Alphanumeric sequences or any other symbol or series of symbols can be employed for either or both of these portions.

In addition, since they are for use either on a one shot only or on a customized basis, the credit card or number could also be associated with a certain sublimit of the individual's or a corporation's credit limit. Thus, for example, a user with a $500 limit, for example, could call into the credit card company and obtain a disposable or a customized card which itself only has a $50 charge limit (for example, when the individual only intends to charge up to $50 in the next transaction, or to allow someone else to charge up to $50). This further limits the potential losses from a credit card fraud.

The present invention could also be used to provide a disposable card for a single transaction to users in general (or a customized card for a limited use), including users who do not have a permanent credit card. It could also be provided to users on a debit basis, based in whole or in part upon some reserve or funds provided to the issuing company in advance. Alternatively, the user could even identify the general or specific type and amount of transaction in advance, if desired.

The present invention, and the disposable embodiments in particular, is of additional value for use over the Internet. For example, the following system could be employed. Before a user makes a potential purchase over the Internet, he or she accesses one of his or her disposable credit cards or credit card numbers. As noted above, this could be accomplished by dialing into the credit card company, by removing one of a series of disposable cards from the user's monthly statement, or so forth. To effect the transaction over the Internet, the user transmits his or her credit card information to the vendor. That vendor then verifies the transaction and obtains an authorization code from the credit card company authorizing the purchase, as is currently standard practice with credit card transactions. To insure the integrity of the system, the vendor is required to verify the code immediately upon receipt. This prevents undue time from elapsing, which is undesirable from a security standpoint. Upon receiving the request for verification, the credit card company notes the identity of the vendor, authorizes the transaction (if the credit card number is valid and the purchaser has sufficient funds available), and forwards the authorization code to the vendor. At the same time, the credit card company also deactivates the credit card number from any further future use. Thus, if a thief intercepts the credit card information en route, when the thief later attempts to take that information and to use it in an illegal transaction, the transaction will be declined since the number has already been deactivated. After the number has legitimately been used once by the lawful owner, it no longer has any continuing validity.

If desired, to remind the user the vendor can transmit a message indicating both that the credit card number has been accepted, and that it is no longer of validity, and can therefore be ripped up. However, if used, this method runs the risk of also alerting a thief who is monitoring the Internet traffic.

The credit card company can also monitor all second requests for use of that credit card number which are transmitted to the system. This monitoring can be used to attempt to catch the thief during his future attempt to illegally use the card

As additional security, each of the disposable credit cards can be given an expiration date, e.g. the end of the month or the end of the billing cycle. Thus, if the credit card is not used within the time limit, it expires. (This expiration date could be printed on disposable paper credit cards). This approach has been used in a different application by credit card companies with respect to checks that are sent with the statement to the user with a given expiration date. As far as the present inventor is aware, that system has been used by credit card companies with satisfactory results in the past.

The card company can also monitor the time of second requests. If the time of second request is extremely close to that of the first request, then the company can block both transactions on the grounds that a thief may be in the process of attempting to quickly intercept and use a credit card number en route before the user.

To further add to the security of the system, a function can be built into Internet software, such as the popular Internet browsers, in which a server assigns a universal time and date stamp (based for example on Greenwich Mean Time) to each credit card transmission transmitted by a user over the Internet. Thus the authorized user's transaction will be assigned a time and date, such that the credit card company can determine, when the same disposable number is sent twice within a short time frame, which transaction corresponds to the one in which the number was sent first. A function could also be provided in which the Internet address of the sender or some other password is encrypted and transmitted as well.

For example, a password which modifies over time and which is coded to the time/date stamp can also be integrated into the browser. The password is individual to each user, with the data summarizing the algorithm used to encode the password being provided to the user and to the individual's credit card company ahead of time (as part of the security information associated with the account). When the transaction is effected, the browser sends information to the internet provider's server, which sends back the universal time/date stamp. The browser then encodes the password and sends it back to the server with the credit card information to be transmitted to the vendor.

The present invention is not limited to use over open systems. Rather, it is intended that it can also be used over secure systems to provide an additional added level of security. Similarly, the invention can be used for those individuals who own credit cards and wish to purchase items over the telephone, but who are reluctant to give out or release their credit card information over the phone.

Likewise, although a variety of security procedures and methods are disclosed herein, any of the security procedures, protocols, encryption techniques, and so forth, used in the art, can be used in connection with the present disposable and/or customized credit cards.

If the disposable credit cards are stolen or lost, the credit card company can, of course, minimize loss by simply deactivating them upon learning of the theft or loss from the user. In addition, the placement of sublimits on each of the cards, or on the group of cards as a whole, further minimizes potential loss.

Although a disposable credit card number system is preferred, as described above, alternatively, a special, separate (disposable or customized) credit card number could even be assigned specifically for use over the Internet, whose use is subject to higher security measures, whether usable one or more than once. For example, after use, the user would have to call into the credit card company to verify the transaction, or the credit card company would call the user at a predetermined number (e.g. the user's home number) to verify that the user made the transaction. This alternative system could be used for example, exclusively with Internet transactions on secure connections, to provide an additional level of comfort to those users who are uncomfortable with transmission of card information even over secure connections. In the event of problems, this separate Internet credit card number could be deactivated separately from the main credit card number associated with the account.

In accordance with further embodiments of the invention, customized credit cards are also provided herein. These credit cards can be customized by the user such that they are only suitable or usable for particular subuses, for particular subframes of time, or so forth. This differs from the present practice in the art, which is to have credit card numbers which are valid for all uses, and for all periods of time until the card expires.

In the current practice in the art, for example, employees frequently make payments which are later reimbursed by their corporation. In accordance with the present invention, their corporation can issue customized credit cards, or obtain customized credit cards from a credit card company, which can serve certain limited uses, functions or so forth. This card can be customized in any of numerous ways. For example, the customized card could be set to be valid for a certain limited number of dates or until a certain date. For example, if an employee is going on a business trip for two days (or some other amount of time), the card could be set to be valid on only those two days. Thus, the employee is authorized to use the card for charges on only that time that the employee is away on the business trip, but not for any other time. Thus, in accordance with these embodiments, the card can have a user customized range of dates or series of dates. In one embodiment this is a range of dates with a commencement date and expiration date. (This is useful, for example, if an employee is going on a business trip, one or more cards could be issued which are valid for the dates of the trip, with the card not being valid before the trip starts or after the trip ends). In another embodiment the card becomes valid at any specific time (even a time of day) and ceases to be valid at any other specific time. Likewise, the card could become valid for a series of ranges of dates, even dates which are non consecutive or non contiguous. For example, it could be valid for a specific day or series of date in March (for a first business trip), become deactivated once that trip is over, can be reactivated for a specific day or dates in June (for a second business trip), be deactivated once that trip is over, and so forth. It could also be valid for a specific predetermined amount of time. For example, it could be valid for any one week period, beginning from when the user or subuser uses first uses it.

The card can also be customized for only particular uses or groups of uses. In this manner, the main cardholder (e.g. a corporation, a parent, etc.) can determine in advance what the card can or should be used for. For example, the card could be customized so that it is only good for airline reservations, such that if the employee tries to use it for any other type of charge, the charge will be declined, regardless of the amount of the transaction involved. Or the card could be customized so that it can only be used for airline and hotel charges. The types of uses which can be provided include any type of use that is currently charged or could in the future be charged on a credit card, or any combination of the same. Currently, charges which are placed on cards, include airline, hotel and car rental charges, restaurant bills, retail store purchases, and so forth.

The card can also be customized for use only by a specific individual, by certain groups of individuals, or so forth. A parent could provide a customized use card which is for use by his or her son or daughter, a corporation could provide a customized use card which is for use by employees, an organization could provide a customized use card for use by employees and/or members and so forth. Different cards or customization parameters could be provided for officers, board members, executives, or so forth.

As one example, an employee could be given authorization to purchase a new computer system. A customized credit card could be issued to the user which is only valid for use for that particular type of charge (computer hardware and software stores) and to the credit limit decided by the issuer or authorizing party at the corporation, such that if the employee tries to use it for anything else or for a charge in excess of that authorized, the charge will be declined. The card could even customized for use in a particular store itself or a particular chain of stores (such as a particular restaurant, or a particular chain of restaurants). Any of the features in the present application can also be combined —thus, the employee could be given a card for use in any computer store which is good for a total purchase of up to, for example, $2000 in value.

As another example, a parent could give a teenage child a card to go out and make a specific purchase for the child or for the parent. The card could be valid only for purchase on that particular day, to a certain designated purchase limit, and even, if desired only in a certain store, or group of stores or types of stores (e.g. clothing stores), or types of purchases or items. The main account could have, for example, a $1500 credit card limit, but the parent could set a $100 limit for use of the customized card on that particular day. Thus, if the card is lost or stolen, the card can not be used at stores other than the types chosen by the parent. Use in any other type of store or on any day other than that one day will cause the card to be declined. This minimizes the amount of credit card loss which can occur, and increases the chances of catching the thief. Likewise, the sublimit of $100 also minimizes the amount of loss which is possible.

The card could also be customized to be valid only in a particular region. For example, if the employee is going on a business trip from New York to Florida and back, the card could be set to be valid only in the States of New York and Florida, and not to be valid for charges in any other locations. If the card were lost or stolen en route, e.g. in a stopover in Georgia, and the thief attempted to use the card in Georgia, the charge would be declined, irrespective of the amount involved.

The amount of credit on the card could be as high as the credit on the main account, or alternatively, could also be customized. The main cardholder (e.g. the corporation, the parent, etc.) can set how much credit is on the particular card for the subuser (e.g. the employee). This can be done in some fixed manner, on the basis of some formula, or so forth.

Self transfer of funds and customization by the corporation or the user of the card is preferred. In other words, the corporation determines what uses and/or amounts are set on the credit card up to the corporation's total credit card limit.

In one embodiment, with respect to customization, the user receives one or more credit cards, each of which is inactive. Each card has a blank amount of credit, and no predefined use, i.e. the card initially has no credit available on it at all and no use available to it. When the user receives the credit card, or when the user is ready to activate the card, the user determines how much of his or her available credit he or she wants to transfer onto that particular card and what particular uses or types of uses are desired (or even all uses, if desired). For example, the user may decide that he or she wants to go to a particular place or store that day and have a certain amount of money with himself or herself (or wants to send his or her employee with a certain amount). In addition to or in place of carrying cash, the user could carry a card having a predetermined amount on it, and could even, if desired, set the places or types of places where the card will be active.

In another embodiment, a user can designate a single sum for use over a plurality of cards. This method overcomes a variety of problems present with the current methods of the art. For example, if a individual or couple wishes to go on vacation abroad, they often purchase traveller's cheques in any of a predetermined limited number of denominations (e.g. twenty, fifty, one hundred dollars, etc.) When using those cheques to convert money the couple often may not wish to convert the full sum (e.g. the full fifty dollars) at that one time, in that one place, or at that day's exchange rate, etc. Alternatively, the couple may be purchasing an item from a store, and the full cost of the transaction is often some odd number which is less than the denomination on the card. In this case, the individual or may not want to receive change back from the vendor in cash, since the vendor may be providing a disadvantageous exchange rate, or so forth.

Accordingly, in this embodiment, a single sum can be "distributed" over a plurality of cards. In this manner, the user designates a particular sum, and each of the cards in that plurality can draw upon that sum. The use of that card reduces the total sum available for the next cards in the series. In this manner, a user can use the customized or the disposable card for transactions whose sums do not amount to a whole number.

As a security feature, in plurality of card embodiments such as the former, it can be preestablished that not more of a certain percentage of the total sum available can be used on a single card, or can be used without verification of identity. For example, a 50% or 20% single use ceiling (or any other number) can be set by the credit card company or the user, to further guard against loss due to fraud. In this embodiment, if a transaction is attempted with any one card which is in excess of the predetermined ceiling for a single card, the card use can be temporarily blocked or subject to verification of identity, to verify that the card was not stolen and being used illegally for large transactions.

As a further security feature and customization parameter, the card can be set to have a desired level of security which must be comported with by the vendor for the transaction to be authorized. For example, some cards or transactions could require merely a signature, some could require the fingerprinting mentioned herein, some could require a showing of identification (including, if desired, picture ID) or so forth.

As discussed elsewhere herein, all cards in the series can be linked such that, if the cards are stolen, one call will cancel all of the cards.

As another formula, there can be also be a total available credit set by the corporation as customized for the year (or for some period of time, or for a particular trip, etc.) for a person, or for an entire department, or so forth, which can either be on one card, or distributed over several cards, as explained above.

Other combinations can be provided as well. For example, the card can be set such that there are certain combinations of customizations available. For example, each subuse can be associated with a specific credit limit for that subuse on that one credit card. Thus, the user may be told that he or she can spend up to $500 on air travel, $1000 on hotel rooms, $300 on car rentals, and those limits can be programmed into or preset to the card. Other combinations of dates of transactions, types of transactions, amounts for individual and/or total transactions, etc. on a single card, or on multiple cards, can be set as well.

If desired, the customized card could be preset or such that any purchases can only be delivered to a specific shipping address (e.g. the address of the corporation). Likewise, since the card is a customized card, any other special conditions of any sort could be attached to the transaction as desired or needed.

Many other embodiments can be implemented as well. A card can be issued to an individual, or to a department. Or, a group of cards can share a single credit limit. A card can be customized such that, when items are purchased by phone or over the Internet, etc., the only shipping address which will be accepted is a preset shipping address already assigned to the card (e.g. by the main cardholder). A card can be set to have a fixed maximum per transaction limit. It can be set to allow, or disallow cash withdrawals. A card can be set to send out a notification to the main cardholder upon each purchase, or upon each purchase meeting certain criteria (e.g. over a certain limit, pertaining to a certain category, or so forth). The notification could be set to include certain required information, e.g. when it was used and/or where it was used and/or how much credit is left or any other informationi desired. Likewise, a preapproval can be required before every purchase or before certain purchases, such as purchases over a certain limit, or purchases of a certain type.

Likewise, a card can be encoded for multiple uses or types of use. In one such embodiment, the card can be encoded such that it can be used for other magnetic card systems as well. For example, the customized card could be encoded

such that it can also be used in place of some other existing card, e.g. as a metrocard (i.e. a fare card on the New York City subway system), as an EZ Pass (i.e. a card which is used to drive through tolls in New York or elsewhere), or so forth. These multiple use cards could either have a preset amount on them (as a debit card of sorts), or they could interface with the other existing card system (whether the Metrocard system, the EZ Pass system, or so forth) such that upon use of the customized card, the funds are taken out of the user's credit card account.

Or, in another variation on this embodiment, multiple brands of cards can be bundled together on a single customized card for ease of use of the user. The term "brand" is used herein to refer to the general card issuing authorities, whether Visa, Mastercard, American Express, Discover, etc. or to more specific issuing authorities, e.g. Citibank Visa, MBNA Mastercard, etc. In this embodiment, Visa and/or Mastercard and/or American Express etc. card accounts can be bundled together on a single credit card. When the user presents this single card to the vendor he or she has the option to decide which of those brands' account(s) on the card he or she wants to use for the transaction. This reduces the number of cards the individual has to carry. A single transaction could even be broken up among a series of cards if desired with the transaction statement indicating for example that $200 out of the $600 dollar purchase was charged to the Visa account, and an equal amount to the Mastercard and Amex accounts. Or, the main account holder could set up the card to be capable of some fixed total amount of charges (e.g. $1000) with the user free to use any of the accounts on the card in any combination desired to charge up to that amount. This is useful if some establishments accept only one or two of these brands, allowing the user (e.g. the employee, the child, etc.) to use the customized card as establishments that accept any of the brands on the card. Or, for purposes which may be beneficial to the main account holder (e.g. for purposes of frequent flyer mile programs, membership dollar programs, etc.) the customized card could be set up such that all of one or more subtypes of use is charged onto one brand, all of another or more subtype onto a second brand etc. For example, the card could be set such that all airline charges are charged onto the Amex Card, all retail store purchases to the Visa, all hotel reservations to the Mastercard, etc. This could be by the customization of the card which only allow certain types of use of each account, and/or by codes which automatically select the appropriate brand or card account when the user attempts to use the card. This could be in any customization scheme desired. For example, in another embodiment, the first $x amount could be charged to one card account, the next $y dollar amount to another card account, or so forth.

In accordance with a preferred embodiment of present invention, a card could be issued to be always "off", unless the main card or account holder, or the authorized person on the card (i.e. the person given the authority to control the uses of the accounts on the card), authorizes or sets or turns the card and/or a specific use of the card "on" for either a particular time period, or for use until certain conditions are met. For example, the card could be issued to an employee or to a child, and normally be in an "off" state (as opposed to general purpose or regular credit cards which are normally in an "on" state) which can not be used, until the main cardholder authorizes that the card be turned on for the next day (and the next day only). Or, the card could be turned on until one transaction is conducted using the card (or some specified multiple number of transactions are conducted using the card), or a specific use is effected of the card, or turned on in accordance with any of the other customizations of the card described herein. In accordance with this embodiment, the card normally remains "off", but is occasionally or periodically turned "on" for a while to allow the card to be used for a desired purpose. After that purpose has been accomplished, the card goes back "off" again. In this manner, the card can be turned on and off by the user as often as desired or necessary.

In another embodiment of the present invention, the user can maintain a list of available credit card numbers in his or her computer and/or software program, with the list further indicating the specific customized use of each number. Alternatively, the user can maintain a list by hand, or a list can be provided each month with the user's statement. If desired, the uses of each number can vary over time. If an unauthorized user intercepts the first credit card number and attempts to use it for a use that it is not enabled for, the transaction will be declined. For example, a user could maintain 5 separate numbers (or any other desired number), each of which is linked to the main card account. Today, one particular number could be authorized for booking airline tickets for the current business day (but no later), while tomorrow a different number could be authorized for that purpose.

Customization (and activation) of the card or a specific credit card number can be in any of the ways known in the art. In a simple method, for example, the user can call the credit card company and, once his or her identity has been verified, can direct the credit card company to customize the card (or a specific credit card or credit card number on the account) in the manner desired and/or to activate that specific credit card or credit card number. In a variation on this method, the user could be required to call from his or her home phone, with the phone number being verified at the credit card company using "Caller ID".

In another embodiment, the user can use a computer to dial in over a direct connection (or over the world wide web or the Internet on a secure connection) to the credit card company, and program in the desired characteristics using the user's computer. In this embodiment, a software program can be provided to customize and/or activate the card and/or the user can access a web site (i.e. at the credit card company) where a form can be filled out by the main cardholder (or by the authorized person on the card or an authorized card user) to set the desired customization parameters. This form could then be accessed as often as desired to update and/or modify the customization of the card or specific credit card numbers, check the status or usage of the card or specific numbers, etc. In addition, as a further embodiment, authorizations done using this program or connection could be compared (either automatically or upon demand by the user) against actual purchases recorded by the credit card company against the card. In this manner a "cross check" is provided, so that if a limited use, customized or disposable card transaction comes into the credit card

company which was not authorized by the cardholder, it will show up on the cross check. In a further embodiment, this cross check could be effected automatically (e.g. each time the user logs, in), periodically (e.g. once per day or per some set time period), upon the user's activation of this feature, or upon the user's deliberate initiation of a cross check.

In some embodiments, the main cardholder orders or obtains the card from the credit card company. In other embodiments, the main cardholder issues or activates the credit cards off of his or her main account him or herself, after transmitting the necessary customization information to the card company, and obtaining the necessary authorization.

If desired, a customized credit card could be converted to a regular, general purpose credit card, or vice versa, if desired. This can be used to deal with changing circumstances, needs or desires of the main cardholder, the card user, the corporation, etc. By a "regular" or "general purpose" credit card, the present inventor refers to those credit cards currently used in the art, which have no limitations on their use other that the card be valid (e.g. be before the expiration date and be of an account in good standing), that the person using the card be the authorized user, and that the transaction be within the available credit left on the card. Subject to those provisions, such cards can be used at any time for any types of purchases at any vendor accepting that type of card.

Should a card or any of the plurality of cards be stolen, a user can with one call deactivate one or all of the cards at the same time. Moreover, since these cards are preferably all linked to the user's main credit card account, and are thus individually on file with the credit card company under that account, the user does not need to worry about safekeeping or storing the list of separate cards or numbers.

As a further security feature, a disposable or customized credit card can be provided with a "fingerprinting area". During use of the card, the user can be asked to place a particular finger on a certain portion of the card to form a fingerprint which can later be used to verify whether the card was used by the rightful owner or used illegally by someone without authorization. Preferably, this area is covered by a flap (e.g. a plastic cover) which is lifted or removed before fingerprinting, to prevent stray marks or fingerprints from appearing on the area before it is ready for use.

With respect to those which are for a single use only, the user can sign (and/or fingerprint) the back of the card, and the vendor could submit or return the cards to the credit card company if desired. Alternatively, the vendor could be required to scan the cards into an appropriate system, with a record of the scan going to the credit card company.

Alternatively, in a further invention, instead of using a "fingerprinting area" on a disposable or customized card, such an area can be placed on the vendor's bill or documentation which currently in the art is signed by the purchaser.

In accordance with another embodiment of the invention, the cards could each have their own PIN number, or PIN numbers.

Upon use of the card, the information regarding the transaction is transmitted to the credit card company, as is known in the art. In a further embodiment of the invention, the information on each purchase from a vendor is transmitted directly to the user after the transaction is completed so that the user can directly monitor and keep records of his or her usage, without waiting for the credit card statement to come in. This information can be sent to the user in any manner desirable. For example, it can be transmitted over the Internet to the user, to the user's web page, or so forth. Instead of the user, it can be transmitted to a third party, if desired; for example, if the card is being used as an expense card for an employee's expense account at a corporation (as described herein), the information can be transmitted directly to the corporation. This transmission can be done by the credit card company itself. Alternatively, if desired, the system can be set up such that the information is transmitted at the point of sale. This can be done with or without the credit card embodiments described above as a permanent or automatic recordkeeping system.

In the preferred embodiment, these credit cards are can be used, processed, etc. by a credit card company in the same manner as with its regular credit cards, with the exception that the present cards provide the additional features provided herein.

One of the current problems with a regular card, whether it be a credit card, a debit card, or so forth, is that a thief potentially has full access to all of the credit or funds in your account, until the theft or unusual activity is discovered and/or blocked. In the present invention, as described above, a certain set level of funds or type of use of funds can be segregated aside by the user for a desired period, use, or so forth, while maintaining the integrity of the main account intact (and even potentially maintaining the identity or details of the main account secret).

Although the term credit card is used throughout the present application, the intention is to include credit cards, charge cards, and debit cards by that term, unless otherwise stated. In addition, the present inventions can be used with other cards used for purchases or transfers of funds, as well.

Having described the invention with respect to specific embodiments, it is not intended that the description serve as a limitation on the scope of the invention since other variations on the invention are possible, and may be apparent or derived herefrom.

What is claimed is:

1. An item, comprising:

a financial card, said financial card having been provided by a credit card company at the request of a first person, said financial card being provided for use by any person determined by such first person; and,

wherein said financial card is further customized such that it is limited to use for only a particular type of transaction, said type of transaction being purchases at predetermined vendors of a predetermined identity, such that said customized card will be valid at those predetermined vendors, and will not be valid at the other vendors accepting cards from that credit card company.

2. A method as claimed in claim **1**, wherein said credit card is an American Express® brand credit card.

3. A method as claimed in claim **1**, wherein said credit card is a Visa® brand credit card.

4. A method as claimed in claim **1**, wherein said credit card is a Mastercard® brand credit card.

5. An item as claimed in claim 1, wherein said credit card is a card comprising a magnetic strip.

6. An item as claimed in claim 1, wherein said credit card is not a smart card.

7. An item comprising:

a website on the world wide web, said website being the website of a credit card company where requests can be made for a financial card, wherein said financial card is a card requested by a first person and which is provided by the credit card company for use by any person of the first person's choice; and,

wherein said credit card is further customized such that it is limited to use for only a particular type of transaction, said type of transaction being purchases at predetermined vendors of a predetermined identity, such that said customized card will be valid at those predetermined vendors, and will not be valid at the other vendors accepting cards from that credit card company.

8. An item as claimed in claim 7, wherein said website comprises a form to be filled out by the first person to request said activation of said credit card.

9. An item as claimed in claim 7, wherein said credit card is a card comprising a magnetic strip.

10. An item as claimed in claim 7, wherein said credit card is not a smart card.

11. A method comprising:

requesting a financial card from a credit card company via a website on the world wide web, said requesting of said credit card being by a first person, said financial card being provided by the credit card company for use by any person of the first person's choice; and,

wherein said request is for said financial card to be customized to be limited to use for a particular type of transaction, said type of transaction being purchases at predetermined vendors of a predetermined identity, such that said card will be valid at those predetermined vendors and will not be valid at the other vendors accepting cards from that credit card company.

12. An item as claimed in claim 11, wherein said credit card is a card comprising a magnetic strip.

13. An item as claimed in claim 11, wherein said credit card is not a smart card.

14. A method, comprising:

providing a financial card, said financial card being activated by a credit card company, said card being a card requested from the credit card company by a first person, said financial card being provided by the credit card company for use by any second person of the first person's choice, said card being a card provided in response to a request from the first person via a website over the world wide web for said card; and,

providing said card as a customized card which can only be used for a particular type of transaction, said type of transaction being purchases at predetermined vendors of a predetermined identity, such that said card will be valid at those predetermined vendors, and will not be valid at the other vendors accepting cards from that credit card company.

15. A method as claimed in claim 14, wherein said credit card is an American Express® brand credit card.

16. A method as claimed in claim 14, wherein said credit card is a Visa® brand credit card.

17. A method as claimed in claim 14, wherein said credit card is a Mastercard® brand credit card.

18. An item as claimed in claim 14, wherein said credit card is a card comprising a magnetic strip.

19. An item as claimed in claim 14, wherein said credit card is not a smart card.

20. An item as claimed in claim 1, wherein those predetermined vendors are limited to restaurants.

21. An item as claimed in claim 1, wherein the spending limit on said card is set by the first person.

22. An item as claimed in claim 1, wherein said card is provided to the second person based on funds provided to the credit card company in advance.

23. An item as claimed in claim 7, wherein said card is customized such that it is limited for use only at restaurants.

24. A method as claimed in claim 11, wherein said card is customized such that it is limited for use only at restaurants.

25. A method as claimed in claim 14, wherein said card is customized such that it is limited for use only at restaurants.

* * * * *

US005883810A

United States Patent [19]

Franklin et al.

[11] **Patent Number: 5,883,810**

[45] **Date of Patent: Mar. 16, 1999**

[54] **ELECTRONIC ONLINE COMMERCE CARD WITH TRANSACTIONPROXY NUMBER FOR ONLINE TRANSACTIONS**

[75] Inventors: **D. Chase Franklin**, Seattle; **Daniel Rosen**, Bellevue, both of Wash.

[73] Assignee: **Microsoft Corporation**, Redmond, Wash.

[21] Appl. No.: **935,486**

[22] Filed: **Sep. 24, 1997**

[51] **Int. Cl.**[6] **G06F 17/00**

[52] **U.S. Cl.** **364/479.02**; 235/379; 235/380

[58] **Field of Search** 235/379, 380; 364/479.02

[56] **References Cited**

U.S. PATENT DOCUMENTS

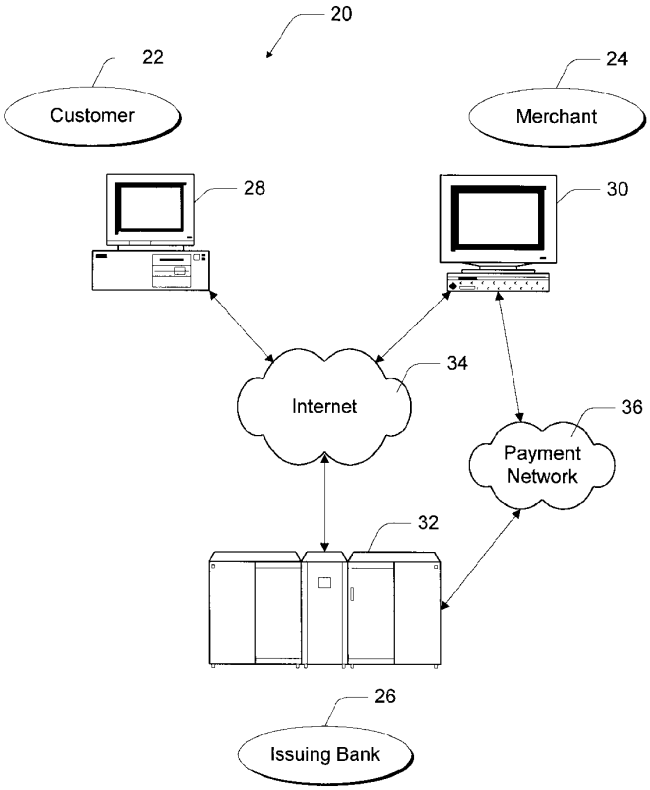
5,831,862 11/1998 Hetrick et al. 364/479.02

Primary Examiner—Harold I. Pitts
Attorney, Agent, or Firm—Lee & Hayes, PLLC

[57] **ABSTRACT**

An online commerce system facilitates online commerce over a public network using an online commerce card. The "card" does not exist in physical form, but instead exists in digital form. The online commerce card is issued electronically to a customer by an issuing institution. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer at the issuing institution to remove the risk of the number being lost or s stolen. When the customer desires to conduct an online transaction, the customer asks the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number. The transaction number looks like a real card number and the merchant handles the transaction number in the same manner as any regular credit card number. When the merchant submits an request for authorization, the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number, using the transaction number as an index, and processes the authorization request using the real customer account number in place of the proxy number. Once the authorization request is processed, the issuing institution once again exchanges the transaction number for the customer account number and sends an authorization reply back to the merchant under the transaction number.

45 Claims, 5 Drawing Sheets



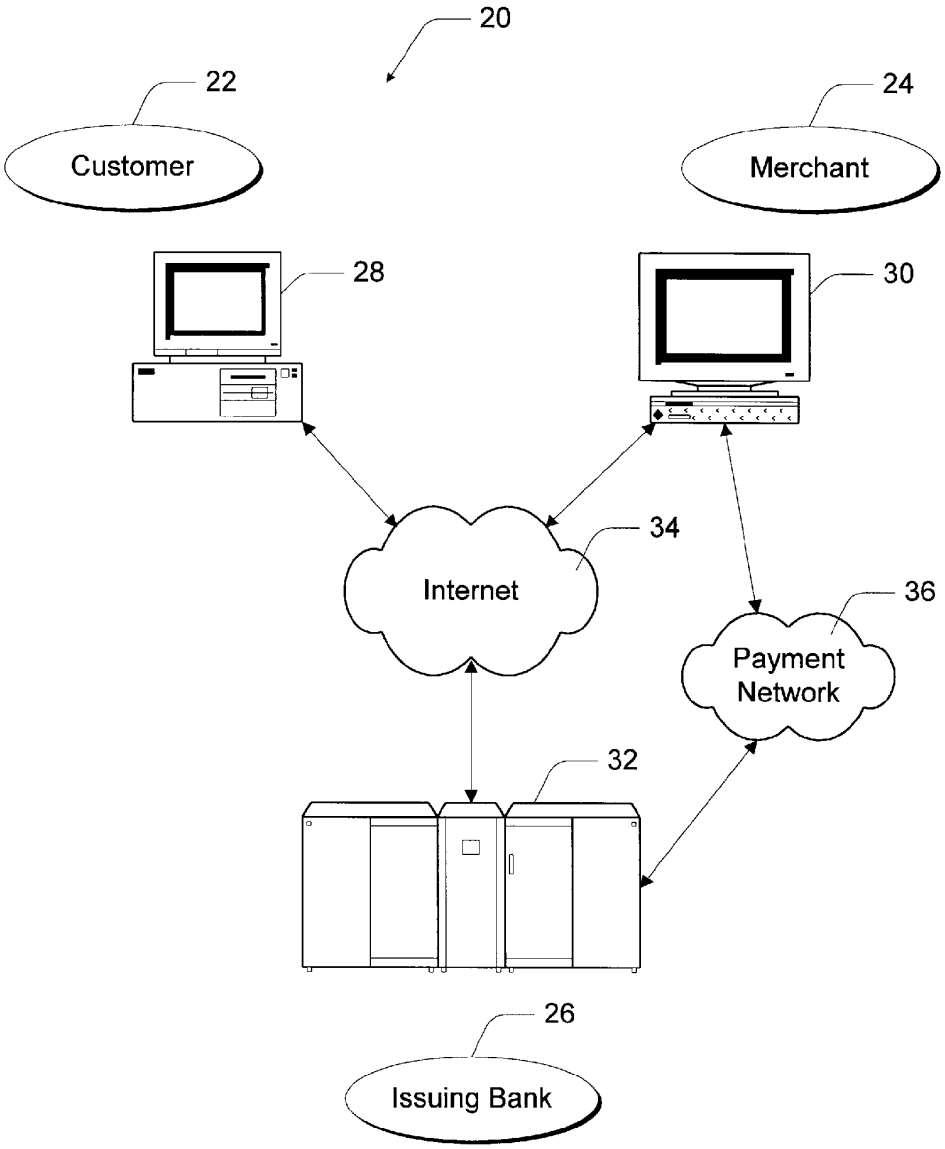
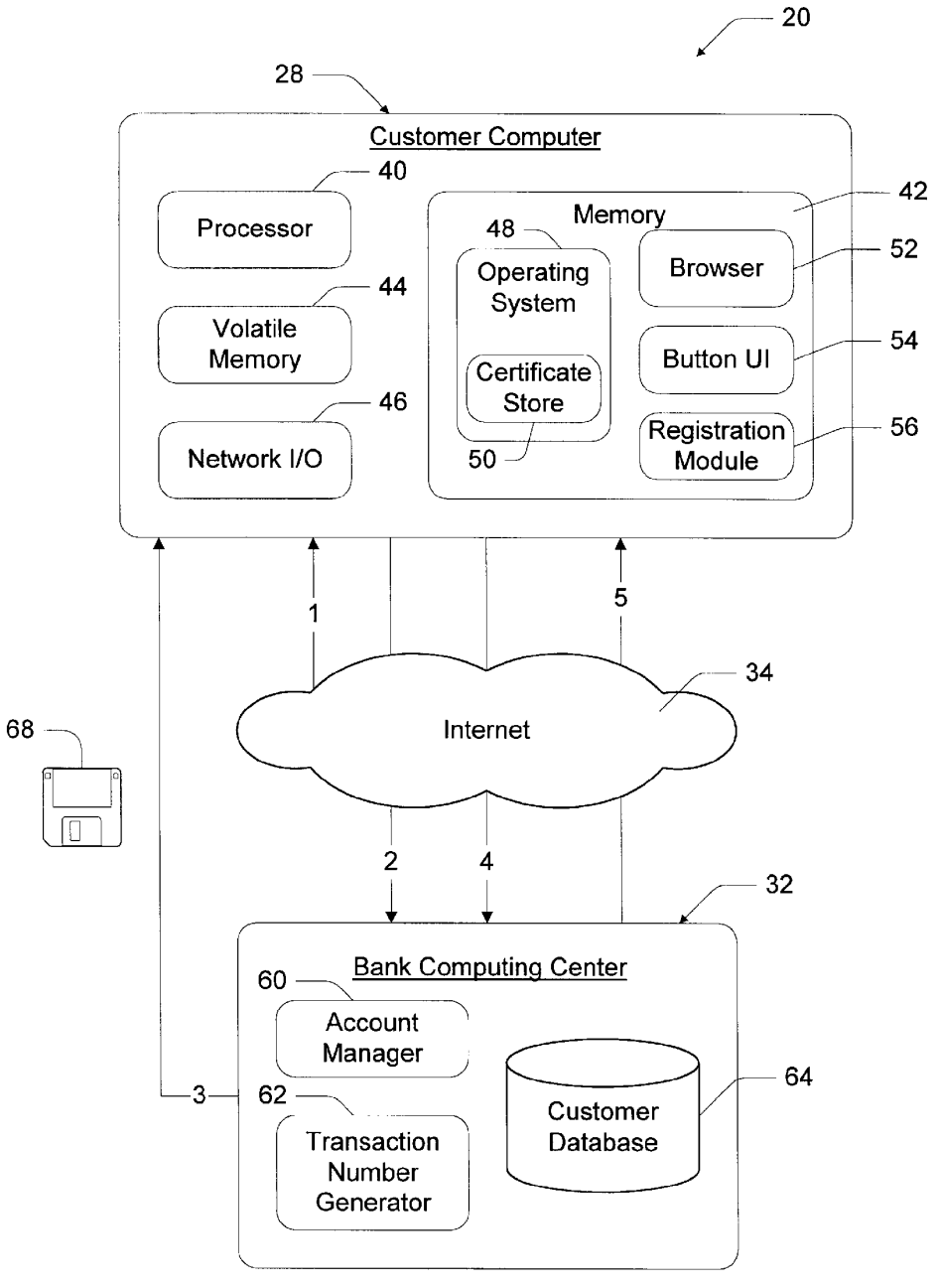
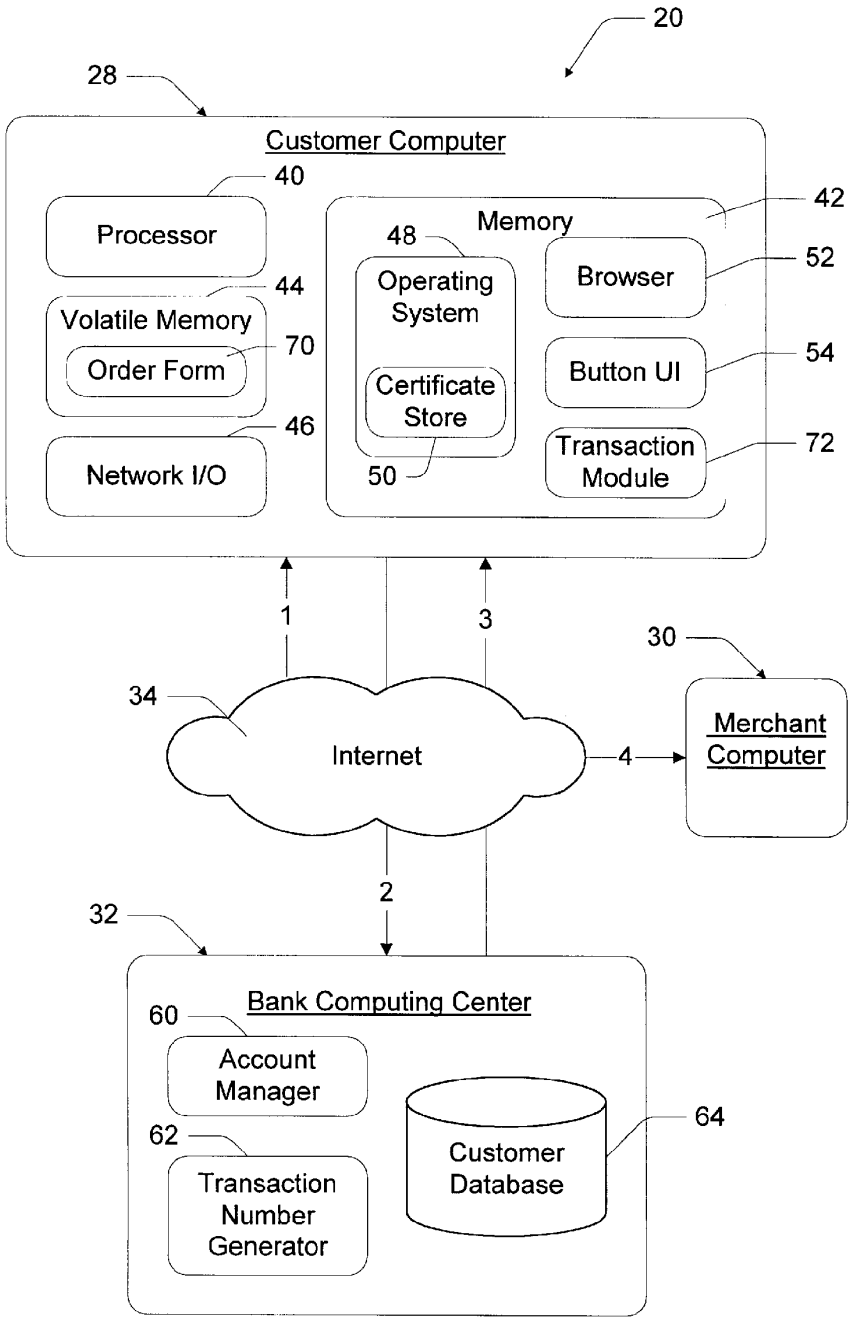

20
22
Customer
24
Merchant
28
30
34
Internet
36
Payment Network
32
26
Issuing Bank

Fig. 1



REGISTRATION PHASE

Fig. 2



TRANSACTION PHASE

Fig. 3

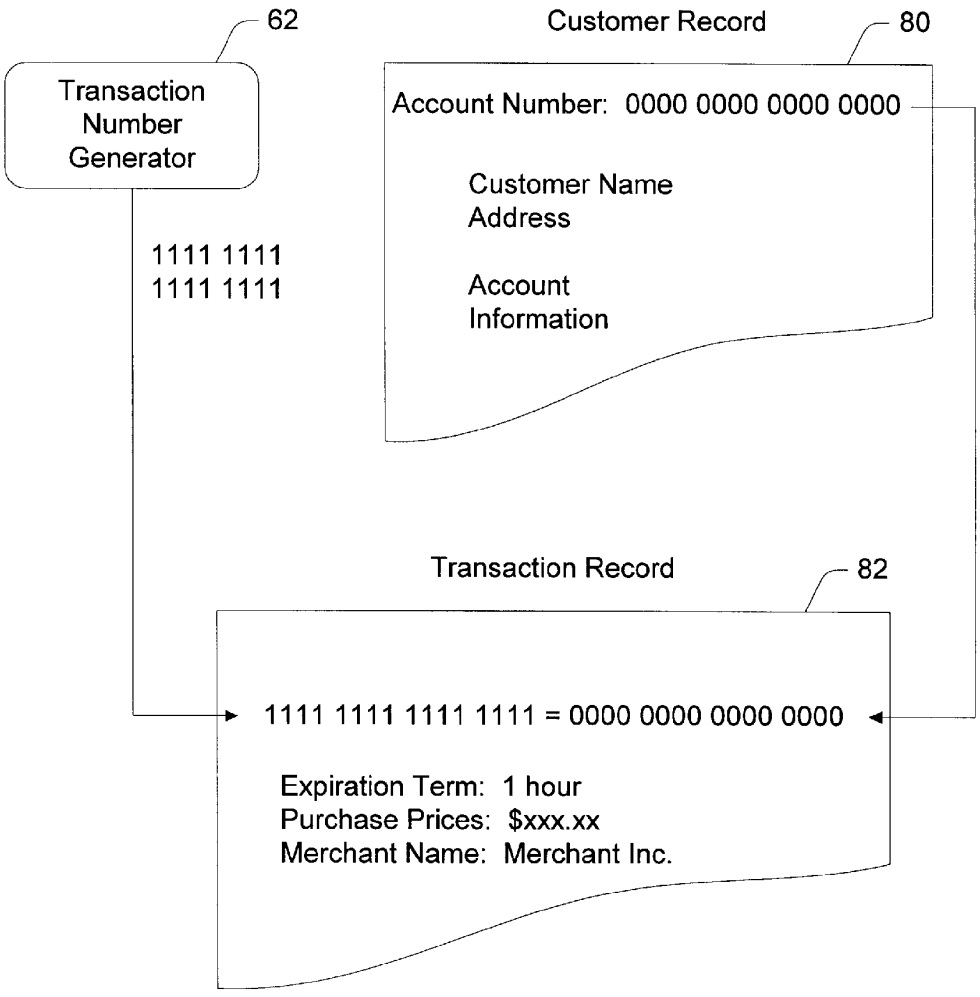
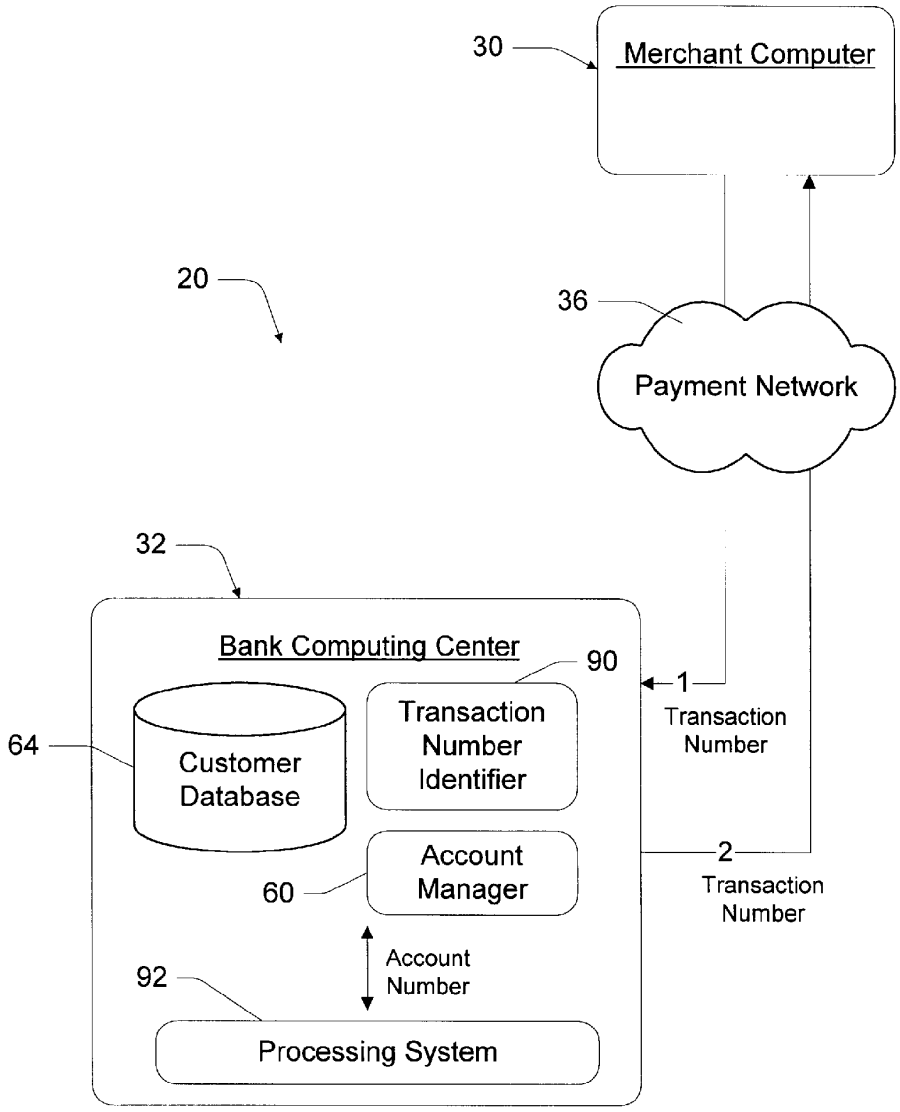

62
Transaction Number Generator
1111 1111
1111 1111
Customer Record
80
Account Number: 0000 0000 0000 0000
Customer Name
Address
Account
Information
Transaction Record
82
1111 1111 1111 1111 = 0000 0000 0000 0000
Expiration Term: 1 hour
Purchase Prices: $xxx.xx
Merchant Name: Merchant Inc.

Fig. 4



AUTHORIZATION PHASE

Fig. 5

ELECTRONIC ONLINE COMMERCE CARD WITH TRANSACTIONPROXY NUMBER FOR ONLINE TRANSACTIONS

TECHNICAL FIELD

This invention relates to systems and methods for facilitating online commerce over a public network (such as the Internet or an Interactive TV/Cable Network) using credit cards, debit cards, and other types of financial/banking cards. More particularly, this invention relates to systems and methods for conducting online transactions using an electronically realizable card that has a private, permanent account number maintained on behalf of a customer by an issuing institution and temporary transaction numbers issued to the customer on a transactional basis without exposure of the permanent account number.

BACKGROUND OF THE INVENTION

Online commerce is experiencing dramatic growth in recent years. More merchants are developing sites on the World Wide Web (or simply "WWW" or "Web") that consumers can access and order goods and/or services. It is fairly common for a consumer to browse a merchant's catalog, select a product, place an order for the product, and pay for the product all electronically over the Internet.

Typically, the consumer pays for the goods and/or services ordered over the Internet with a credit card. During the online transaction, the merchant sends an order form and requests the consumer to enter personal data (e.g., name, address, and telephone number) and credit card information (e.g., account number and expiration date). The consumer returns the completed order form containing the credit card information to the merchant over the Internet. The merchant verifies that the credit card number is valid and can be charged the payment amount. The card verification is usually conducted on a well-established card network, such as the VisaNet® network or the Veriphone® network.

One problem with this traditional online commerce model concerns the security of the credit card data as it travels over the Internet. The credit card information can be intercepted in route, copied into a database, and used to make unauthorized purchases. In an automated environment, an imposter can repeatedly use the stolen credit card data to conduct many online transactions before the consumer ever becomes aware that the credit card data has been stolen.

It would be desirable to develop a new online commerce model that reduces or eliminates the incentive for stealing credit card data. Ideally, a secure online commerce model would render the credit card data hard to steal, and if stolen, worthless to the thief.

Another concern is that any new online commerce model should integrate well with existing proprietary card network systems. There are well-established systems that verify credit card purchases and subsequently settle accounts. These systems and associated protocols are entrenched in the merchant and banking communities and experience a high level of acceptance and trust. A new online commerce model should not usurp these systems, nor require merchants to change their existing practices to implement completely different systems and protocols.

The inventor has developed a card-based online commerce system that improves security and integrates with existing card verification and settlement systems.

SUMMARY OF THE INVENTION

This invention concerns a system and method for facilitating online commerce over a public network (such as the Internet or Interactive TV/Cable Network) using an online commerce card. The "card" of this system does not exist in physical form, but instead exists in a digital form that can be electronically realized for online commerce.

The online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen.

When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction.

The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number.

During the authorization phase, the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth. Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number.

As a result, the merchant never needs to know if the number is a legitimate account number, or a proxy number for an account number. The merchant does not need to implement any new devices, software, or protocols to participate in the new online commerce system.

For added security, the transaction number can be linked to extra transaction information to ensure that the number is only used for one specific transaction. For instance, the issuing institution might tie the transaction number to a specific purchase amount and a particular merchant ID. The issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses.

The online commerce system substantially reduces the value of a stolen number since the transaction number that is transmitted over the Internet (or other network) is only a proxy number for a single purchase. Stealing the proxy number would not greatly benefit a thief because it cannot be repeatedly used for other purchases or transactions. In addition, the system seamlessly integrates with existing card verification and settlement protocols. Software modules are implemented at the customer and issuing institution, but no additional components are implemented at the merchant, settlement participants, or any other member in the online commerce transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

The same reference numbers are used throughout the figures to reference like components and features.

FIG. **1** is diagrammatic illustration of an online commerce system.

FIG. **2** is a block diagram of a customer computing unit and bank computing center. FIG. **2** shows an information exchange between the customer computing unit and the bank computing center during an online commerce card registration phase.

FIG. **3** is the same as FIG. **2**, but shows an information exchange between the customer computing unit and the bank computing center during a transaction request phase.

FIG. **4** is a diagrammatic illustration of data records maintained at the bank computing center to associate a permanent customer account number to a temporary transaction number used in an online commerce transaction.

FIG. **5** is a block diagram of the bank computing center and a merchant computing unit. FIG. **5** shows an information exchange between the merchant computing unit and the bank computing center during a payment authorization phase.

DETAILED DESCRIPTION

The following discussion assumes that the reader is familiar with cryptography. For a basic introduction of cryptography, the reader is directed to a text written by Bruce Schneier and entitled "Applied Cryptography: Protocols, Algorithms, and Source Code in C," published by John Wiley & Sons with copyright 1994 (with a second edition in 1996), which is hereby incorporated by reference.

FIG. **1** shows an online commerce system **20** for conducting online commerce transactions. For general discussion purposes, three participants to an online commerce transaction are shown: a customer **22**, a merchant **24**, and an issuing bank **26**. These three participants play the primary roles in the online commerce transaction. The customer and merchant may represent individual people, entities, or businesses. Although labeled as a "bank", the issuing bank **26** may represent other types of card-issuing institutions, such as credit card companies, card sponsoring companies, or third party issuers under contract with financial institutions. It is further noted that other participants may be involved in some phases of the transaction, such as an intermediary settlement institution, but these participants are not shown.

Each participant is equipped with a computing system to facilitate online commerce transactions. The customer **22** has a computing unit **28** in the form of a personal computer, although other types of computing units may be used including laptops, notebooks, handheld computers, set-top boxes, and the like. The merchant **24** has a computing unit **30** implemented in the form of a computer server, although other implementations are possible. The bank **26** has a computing center **32** shown as a mainframe computer. However, the bank computing center **32** may be implemented in other forms, such as a minicomputer, a PC server, a networked set of computers, and the like.

The computing units **28**, **30**, and **32** are connected with each other via a data communication network **34**. The network **34** is a public network and assumed to be insecure and open to eavesdroppers. In the illustrated implementation, the network is embodied as the Internet. In this context, the computers may or may not be connected to the Internet **34** at all times. For instance, the customer computer **28** may employ a modem to occasionally connect to the Internet **34**, whereas the bank computing center **32** might maintain a permanent connection to the Internet **34**. It is noted that the network **34** may be implemented as other types of networks, such as an interactive television (ITV) network.

The merchant computer **30** and the bank computer **32** are interconnected via a second network, referred to as a "payment network" **36**. The payment network **36** represents existing proprietary networks that presently accommodate transactions for credit cards, debit cards, and other types of financial/banking cards. The payment network **36** is closed network that is assumed to be secure from eavesdroppers. Examples of the payment network **36** include the VisaNet® network and the Veriphone® network.

The electronic commerce system **20** is implemented at the customer **22** and issuing bank **26**. In the preferred implementation, the electronic commerce system **20** is implemented as computer software modules loaded onto the customer computer **28** and the bank computing center **32**. The merchant computer **30** does not require any additional software to participate in the online commerce transaction supported by the online commerce system **20**.

General Operation

There are three distinct phases supported by the online commerce system **20**: a registration phase, a transaction phase, and a payment authorization phase. During the registration phase, the customer **22** requests an online commerce card from the issuing bank **26**. The issuing bank **26** creates an online commerce card for the customer and assigns a permanent customer account number to the card. The permanent customer account number is retained in a data record at the issuing bank **26** and not given to the customer **22**. This prevents the customer account number from being stolen while being transferred over the Internet **34** or stored on the customer's computer **28**.

The "online commerce card" does not exist in physical form, but in digital form for use in online transactions. The issuing bank **26** issues the card to the customer **22** in the form of a signed digital certificate binding the customer to the bank and a software module that can be invoked when using the commerce card to conduct a transaction on the Internet **34**. The commerce card is configured to be used by the customer in one or more areas of commerce in which the customer typically employs a credit card, a debit card, a bank card, or other type of financial services card. The registration phase is described below in more detail with reference to FIG. **2**.

During the transaction phase, the customer **22** invokes the software module, which submits a request for a secure card number to the issuing bank **26**. The issuing bank generates a random temporary transaction number and associates the transaction number with the permanent customer account number in a data record. The issuing bank **26** issues the transaction number to the customer to use as a proxy for the real customer account number. The transaction number resembles a real account number. In the case of a credit card, for example, the transaction number and real customer account number are both 16-digit, mod **10**, numbers identically formatted with four spaced sets of 4-digits. To the customer (and every other participant in the transaction), the transaction number appears to be a valid credit card number. Only the issuing bank **26** differentiates the transaction numbers from the real customer account numbers. The customer **22** uses the proxy transaction number in the transaction with the merchant **24**. Since the transaction number is issued in place of the customer number for only a single transaction and with a limited life, a thief that

intercepts the transaction number is prevented from using it for illicit gain. The transaction phase is described below in more detail with reference to FIG. **3**.

During the payment authorization phase, the merchant **24** submits the transaction number over the conventional payment network **36** to the issuing bank **26** for approval. The issuing bank **26** identifies the number as a transaction number, as opposed to a real customer account number. The issuing bank **26** uses the transaction number to retrieve the data record linking the transaction number to a customer account number. The issuing bank **26** then swaps the customer account number for the transaction number and processes the authorization request using its conventional processing system. After the processing, the issuing bank **26** substitutes the transaction number back for the customer account number and returns the authorization reply to the merchant **24** under the transaction number. In this manner, only the issuing bank is aware that the transaction number is a proxy for the customer account number. The merchant **24** need not be aware that the transaction number is not a true customer account number, but simply handles the number as it would any other card number. The authorization phase is described below in more detail with reference to FIG. **5**.

Registration Phase

FIG. **2** shows the online commerce system **20** during a registration phase. This phase involves the customer **22** requesting an online commerce card from the issuing bank **26**, and the issuing bank creating and issuing the online commerce card to the customer. The information exchange between the customer computer **28** and the bank computer **32** during the registration phase are illustrated as enumerated lines between the two entities.

The customer computer **28** has a central processing unit comprising a processor **40**, a volatile memory **42** (e.g., RAM), and a non-volatile memory **44** (e.g., ROM, hard disk drive, floppy disk drive, CD-ROM, etc.). The customer computer **28** also has a network I/O **46** (input/output) for accessing the Internet **34**. The network I/O **46** can be implemented, for example, as a dial-up modem or as a permanent network connection.

The customer computer **28** runs an operating system **48** that supports multiple applications. The operating system **76** is preferably a multitasking operating system that allows simultaneous execution of multiple applications in a graphical windowing environment. One preferred operating system is a Windows® brand operating system sold by Microsoft Corporation, such as Windows® 95, Windows® NT, Windows® CE, or other derivative versions of Windows®. It is noted, however, that other operating systems that provide windowing environments may be employed, such as the Macintosh operating system from Apple Computer, Inc.

The operating system **48** includes a certificate store **50** to securely hold digital certificates. The certificate store **50** holds a signed certificate received from the issuing bank as part of the online commerce card.

Several software components are stored in memory **42** including a browser **52**, a button user interface (UI) **54**, and a registration module **56**. These software components load into volatile memory when launched and execute on the processor **40** atop the operating system **48**. The browser software **52** originally exists on the customer computer **28**, whereas the button UI **54** and registration module **56** are downloaded to the customer computer **28** during the registration process. It is further noted that the button UI **54** may be integrated into, or rely on, the graphical user interfaces supported by the operating system **48**, but is shown separately for explanation purposes.

The bank computer **32** has an account manager **60**, a transaction number generator **62** and a customer database **64**. The account manager **60** and transaction number generator **62** are preferably implemented in software that executes on the bank computer **32**. The transaction number generator **62** is preferably a random number generator that creates random numbers in the same format as the customer account number. The software modules **60** and **62** may be executed individually or integrated into the same software program, such as a relational database program that manages the relational database **64**.

The registration phase between the customer and issuing bank will now be described with respect to FIG. **2**. During normal operation on the Web, the customer comes across a banner advertising an online commerce card sponsored by the issuing bank. The banner may be part of the bank's Web site, or part of a statement to its customers, or included as advertisement in other Web content. The customer activates the banner by clicking the banner icon with a mouse pointer. This action submits a request for an online commerce card application. In response, the customer downloads the registration module **56** from the Web to the customer computer **28**. This initial registration step is illustrated by flow arrow **1** from the Internet **34** to the customer computer **28**.

The registration module **56** automatically launches to aid the customer in the completion of the online application. The registration module is preferably configured to provide step-by-step instructions, such as a Help Wizard. The customer fills out various fields related to personal and financial matters, such as name, address, telephone number, social security number, presently owned credit cards, bank affiliations, and the like.

The customer completes the online commerce card application using the registration wizard and submits the application to the issuing bank (flow arrow **2** in FIG. **2**). The registration module **56** facilitates this communication and all future interaction between the consumer and the issuing bank. The application itself, or the registration module **56**, contains the necessary routing information to direct the application over the Internet **34** to the bank computing center **32**. The issuing bank reviews the application to determine whether the customer is credit worthy **19** and pending the analysis, whether to grant or deny a commerce card. If a new card is denied, the issuing bank returns a message to the customer indicating that the card application has been denied and no card will be issued. Conversely, if a new card is to be granted, the issuing bank returns a message indicating that a card will be granted assuming the remaining registration steps are satisfied.

Assuming that a card account is granted, the issuing bank creates a temporary customer account record in the customer database **64** and assigns a temporary PIN (personal identification number) or other type of customer identifier to that account. The bank supplies the PIN and any additional software needed to complete the formal application process to the customer. In the preferred implementation, the bank supplies the PIN and software using some means other than online transmission. FIG. **2** shows the PIN and software being stored on a floppy disk **68** and mailed to the customer using conventional postal carriers (flow arrow **3** in FIG. **2**).

Using regular mail provides an added level of security in that the bank can verify through the mailing address that a customer having the registered name and address truly lives at the place inscribed on the online registration form. This increases the bank's confidence that the customer did not submit a fraudulent application. Another benefit is that the software on floppy disk **68** might contain cryptographic

modules to secure communication between the customer and issuing bank. Providing the cryptography on a disk that is mailed to a U.S. address avoids the problem of unknowingly supplying cryptographic code to foreigners in a manner contrary to U.S. export laws.

The customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module **56** and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard **56** generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations.

The pair of public and private keys is unique to the customer. The public/private keys form the foundation of public cryptography systems and are based upon a mathematical relationship in which one key cannot be calculated (at least in any reasonable amount of time) from the other key. The holder distributes the public key to other parties and maintains the private key in confidence. Public key cryptography is well known. An example of an asymmetric cipher is the well-known RSA cryptographic algorithm named for the creators Rivest, Shamir, and Adleman.

The customer computer **28** submits the certificate request to the issuing bank (flow arrow **4** in FIG. **2**). The certificate request contains the public/private key pair and the temporary PIN, which serves as a baseline authentication of the customer requesting the certificate.

If the bank still desires to grant an online commerce card to the customer, the account manager **60** at the issuing bank converts the temporary customer account record to a permanent account record in the database **64**. The bank's account manager **60** assigns a permanent customer account number to the customer account record.

The customer account number uniquely associates all relevant database records to a specific customer. The customer account number may exist in many different forms. For instance, if the customer already possesses a real credit card or debit card from the bank, the number from the credit card or debit card is the customer account number used to identify the data record for the online commerce card. In this manner, the customer can use the digital online commerce card concurrently with the physical credit or debit card. As another implementation, the public key, private key, or a mathematical derivation of one or both keys (e.g., a hash value of one or both keys) might be employed to represent the customer account number. Another alternative is for the bank to generate an internal number that is used for solely for record keeping purposes.

The issuing bank digitally signs a certificate containing the public/private key pair and places the customer's public key in the customer account record in the database **64**. One technique for forming this digital signature is to hash the certificate and encrypt the resulting hash value using the bank's private signing key. The issuing bank returns the signed certificate to the customer via the Internet **34** (flow arrow **5** in FIG. **2**).

The certificate is deposited in the certificate store **50** on the customer computer **28**. The certificate and customer's private key act as a password for all future authenticated conversations between customer and issuing bank. Along with the certificate, the issuing bank also downloads the button UI **54**, which can be added to the browser's toolbar (and/or toolbars of other applications). The button UI **54** enables the customer to invoke the wizard to communicate with the issuing bank during future commerce transactions. At this point, the customer has been issued an "online commerce card".

The registration process is described as an interaction between the customer and an issuing bank. It is noted that a third party may handle some or all of the registration tasks on behalf of the bank. Such third parties are often referred to as "certifying authorities", "credential binders," "binding authorities," or simply "binders." However, for discussion purposes, the issuing bank is assumed to perform all of the functions of a bank and an issuing institution.

Transaction Phase

FIG. **3** shows the online commerce system **20** during a transaction phase. This phase involves the customer **22** engaging in an online commerce transaction with the merchant **24**. As part of the process, the customer **22** requests a transaction number from the bank **26** to be used in the commerce transaction. The information exchange between the customer computer **28**, the merchant computer **30**, and the bank computer **32** during the transaction phase are illustrated as enumerated lines.

The customer invokes the browser **52** to surf the Web for a particular product or service, or to visit a Web site of a particular merchant. Suppose that the customer decides to commence an online transaction with the merchant, such as purchasing a product from the merchant. The customer downloads an order form **70** from the Web and stores it in volatile memory **44** (flow arrow **1** in FIG. **3**). The order form **70** is typically configured as an HTML (hypertext markup language) form. The customer fills out the order form **70** to purchase a desired product from the merchant. The order form **70** includes a payment section that requires the customer to enter a credit card number for payment of the goods.

Upon reaching this method of payment field, the customer clicks the card button UI **54** on the browser toolbar to invoke a card transaction module **72**. The transaction module **72** is the wizard software created as a result of the registration process of FIG. **2** and is employed to guide the customer through a request for a transaction number.

Upon clicking the button UI **54**, a dialog box appears on the display to inform the customer that they have requested a secure card number. The customer is prompted by the dialog box to input a password for identification purposes. This password might be the private key (if the customer knows the key value) or it may be a separate name or number created by the customer. The operating system **48** checks the password prior to allowing access to the certificate store **50**. If the password is approved, the transaction module **72** prepares a request for a transaction number, digitally signs the request using the customer's private key, and submits the signed request to the issuing bank's computer **32** via the Internet **34** (flow arrow **2** in FIG. **3**). The request contains the certificate originally issued by the bank.

The bank computer **32** receives the signed request and immediately verifies the identity and authenticity of the customer by applying the customer's public key to the digital signature and examining the certificate. Assuming the signature and request are valid and the customer's account is in good standing, the account manager **60** instructs the transaction number generator **62** to create a transaction number to be used as a proxy for the customer account number during the online commerce transaction. The account manager **60** associates the transaction number with the customer account number in a data record on the

customer database **64**. As a result, the online commerce card now has two numbers associated therewith: a permanent customer account number and a transaction number that serves as a proxy for the customer account number.

FIG. **4** shows one exemplary implementation of creating a transaction number and associating that number with the customer's account number. A customer record **80** for the requesting customer is stored in the customer database **64** and contains a customer account number. Suppose, for example, the customer account number is a 16-digit credit card number. Credit card numbers comply with a standardized format having four spaced sets of numbers, as represented by the number "0000 0000 0000 0000". The first five-to-seven digits are reserved for processing purposes. It identifies the issuing bank, the card type, and so forth. The last 16^{th} digit is used as a sum check for the 16-digit number. The intermediary eight-to-ten digits are used to uniquely identify the customer.

The transaction number generator **62** generates a transaction number for the online commerce card that is formatted identically to the customer account number. In this example, the number generator **62** creates a 16-digit transaction number having four spaced sets of numbers, as represented by the number "1111 1111 1111 1111". The transaction number resembles a credit card number in all respects, except that the first five-seven-digits are coded by the issuing bank to identify the number as a fictitious electronic proxy number, rather than a real credit card number.

The account manager **60** associates the temporary transaction number with the permanent customer account number by relating the two numbers in a data record **82**. More particularly, the account manager creates data record **82** in a proxy/customer account cross-reference database. The data record **82** is keyed with the customer account number to identify the customer record **80**. The transaction number is then written to the data record **82**. In this manner, the customer account record **80** can be cross-referenced via the transaction record **82** using the transaction number as an index. The issuing bank will use the transaction record **82** at a later time when the merchant submits the transaction number for payment authorization.

The transaction number is designed to have a finite life, as determined by the issuing bank. The shorter the duration, the less likelihood of fraud resulting from the transaction number being stolen and reused prior to the end of its life. The chief requirement of the expiration term is that it be sufficiently greater than the anticipated worst case time for returning the authorization request response to the merchant, plus overhead to account for customer and merchant handling prior to submittal of the authorization request. The networks operated by Visa and MasterCard allegedly handle submission and return of an authorization request (round trip from the merchant to the issuing bank and back to the merchant) in less than four seconds, which is essentially negligible compared to the time reserved for customer and merchant handling. Accordingly, a suitable expiration term for a transaction number can be one-half hour to two hours. In FIG. **4**, the account manager **60** assigns an expiration term of one hour to the transaction number in record **82**. When the expiration term lapses, the transaction number is no longer valid.

The transaction number is valid for only one transaction. For added security, the transaction number can be linked to transaction information to ensure that the number is only used for one specific transaction. The transaction module **72** executing on the customer computer **28** may require the customer to enter information pertaining to the purchase, like the purchase price, the model or item number, the merchant name, and the like. The issuing bank can then tie the transaction number to this specific transaction data within the transaction record **82**.

Once the transaction record **82** is created and related to the customer record **80**, the issuing bank computer **32** sends the transaction number to the customer computer **28** (flow arrow **3** in FIG. **3**). The real customer account number is not sent to the customer, but is retained at the issuing bank in secrecy. In the credit card case, this means that the true credit card number is never sent over the Internet **34**, thereby eliminating the possibility of interception and illicit use by a thief.

At the customer computer, the transaction number is presented in a graphical window by the transaction module **72**. If the order form is compatible, the customer can click on an icon to have the number automatically entered into the merchant order form **70**. Otherwise, in a worst case scenario, the customer manually enters the proxy transaction number into the merchant's HTML order form **70**. Since the transaction number has the identical 16-digit format as a real credit card number, the customer enters the 16-digit number as if it were his/her real credit card number.

The user may also be required to enter an expiration date, which may or may not be sent from the issuing bank. Essentially, the expiration date can be any future date that is not too far in the distant future, such as less than two to three years. The customer then submits the completed order form **70** over the Internet **34** to the merchant computer **30**.

Authorization Phase

FIG. **5** shows the online commerce system **20** during a payment authorization phase. This phase involves the merchant **24** seeking authorization from the issuing bank **26** to honor the customer's transaction number received by the merchant in the commerce transaction with the customer. The information exchange between the merchant computer **30** and the bank computer **32** during the authorization phase are illustrated as enumerated lines.

The merchant **30** receives the transaction number from the Internet and processes the transaction number using its existing computer system. There is no software components added to the merchant computer as part of the online commerce system **20**. Rather, the merchant computer **30** treats the transaction number of the online commerce card no differently than it treats a standard credit card number. In fact, the merchant computer **30** most likely will not be able to distinguish between the two types of numbers.

In FIG. **5**, the merchant computer submits a request for authorization over a payment network **36** to the bank computing center **32** (flow arrow **1** in FIG. **5**). This illustration is simplified for discussion purposes, as other participants will most likely be involved. For instance, the merchant computer **30** typically submits the request for authorization to its acquiring bank (not shown) by conventional means. The acquiring bank validates the authorization request by verifying that the merchant is a valid merchant and that the credit card number represents a valid number. The acquiring bank then forwards the authorization request to the issuing bank. The routing to the issuing bank via the payment network is handled through conventional techniques.

When the bank computer **32** receives the authorization request, it first examines the transaction number to determine whether it is a valid number. A transaction number identifier **90** executing at the bank computer **32** examines all incoming account numbers to segregate proxy transaction numbers from real credit card numbers. On a daily basis, it is likely for the bank computer **32** to handle many account

numbers on the order of tens or hundreds of thousands. Most of the numbers are expected to be real credit card account numbers. Only a small percentage is anticipated to be temporary transaction numbers. The transaction number identifier **90** filters out authorization requests that pertain to transaction numbers from authorization request that pertain to real customer account numbers. In the continuing example, the transaction number identifier **90** recognizes the number submitted by the merchant computer **30** as a transaction number based on the first five-to-seven digits.

The transaction number identifier **90** passes the transaction number to the account manager **60**. The account manager **60** uses the transaction number as an index to transaction records in the customer database **64**. If no records are found, the number is deemed invalid and the bank computer **32** returns a message disapproving the transaction to the merchant computer **30**. If a record is found, the account manager **60** examines any extra transaction information, such as purchase amount and merchant ID, which is typically included in the authorization request to double check the accuracy of the request.

Once a valid transaction record **82** is located, the account manager **60** cross-references to the associated customer account number and uses this number to index the customer record **80**. The account manager **60** substitutes the customer account number in place of the transaction number in the merchant authorization request. The account manager **60** then submits the authorization request to the bank's traditional processing system **92** for normal authorization processing (e.g., confirm account status, credit rating, credit line, etc.).

After the request is processed, the processing system **92** returns an authorization response to the account manager **60**. The account manager fetches the transaction number from the cross-referenced data records **80** and **82** in the database **64** and substitutes the transaction number in place of the customer account number in the bank's authorization reply. The bank computing center **32** then returns the authorization reply to the merchant computer **30** via the payment network **36** (flow arrow **2** in FIG. **5**).

The preceding steps assume the authorization request was successful. If that is the case, the credit limit of the customer's account is drawn down in the amount of the authorization, and the transaction is logged for future posting.

Settlement

During settlement, batches of transactions are submitted to a card association, which performs the following operations:

- Edit/balance the batch transactions
- Calculate the interchange fees
- Verify the fees
- Route chargeback transactions
- Calculate net settlement
- Distribute interchange files to the issuers
- Transmit settlement advisements to the clearing (issuer) banks
- Transmit settlement to the settlement (card association) bank

The issuing bank receives a daily interchange file that contains all transactions submitted by merchants against customer accounts owned by the issuing bank for that day. In addition, the issuing bank also receives other settlement transactions such as chargebacks, retrieval requests, re-presentments, etc. The settlement process thus far is conventional.

When the settlement file references a transaction number, however, the account manager **60** performs essentially the same lookup-and-substitute process described above with respect to the authorization request. That is, the account manager fetches the customer account number from the cross-referenced records **80, 82** in the database **64**, replaces the transaction number in the batch with the customer account number, and processes the batch using conventional means.

The online commerce system has many advantages. One advantage is that it substantially reduces the value of a stolen number since the number is only a proxy number for a single purchase. Stealing the proxy number would not greatly benefit a thief because it cannot be repeatedly used for other purchases or transactions. Another benefit is that the system integrates with existing card verification and settlement protocols. All parties, except the issuing bank, are able to treat the transaction number of the online commerce card in the same manner in which they process a Visa® or MasterCard® transaction today. No additional processing software is needed at the merchants or settlement participants.

Although the invention has been described in language specific to structural features and/or methodological steps, it is to be understood that the invention defined in the appended claims is not necessarily limited to the specific features or steps described. Rather, the specific features and steps are disclosed as preferred forms of implementing the claimed invention.

We claim:

1. A method for facilitating online commerce, comprising the following steps:

issuing an electronic commerce card to a customer during a registration phase, the commerce card having a permanent number associated therewith to identify the customer; and

during an online commerce transaction phase, issuing a proxy number that is associated with the permanent number for use in an online commerce transaction in place of the permanent number on the commerce card.

2. A method as recited in claim **1**, wherein the issuing steps comprise issuing permanent and proxy numbers that are formatted with an equal number of digits.

3. A method as recited in claim **1**, wherein the issuing steps are performed online.

4. A method as recited in claim **1**, wherein the step of issuing the commerce card comprises the step of supplying to the customer a signed digital certificate and software code that supports a user interface button that invokes a user interface for requesting the proxy number.

5. A method as recited in claim **1**, wherein the step of issuing the proxy number comprises the step of issuing a proxy number having a finite period of time within which the proxy number can be used.

6. A method as recited in claim **1**, further comprising the step of using the proxy number during the online commerce transaction.

7. A method as recited in claim **1**, wherein prior to the step of issuing an electronic commerce card, the method comprises the following additional steps:

initiating, from the customer, a request for the commerce card from an issuing authority; and

downloading software code to the customer to assist in a card registration process.

8. A method as recited in claim **1**, wherein prior to the step of issuing an electronic commerce card, the method comprises the following additional steps:

initiating, from the customer, a request for the commerce card from an issuing authority;

supplying a preliminary identifier to the customer; and

using the preliminary identifier to request a certificate from the issuing authority, the certificate being part of the commerce card.

9. A method as recited in claim **8**, wherein the step of issuing the commerce card comprises the step of supplying to the customer a signed digital certificate and software code that supports a user interface button that invokes a user interface for requesting the proxy number.

10. A graphical user interface embodied on a computer-readable medium that presents the user interface button as recited in claim **9**.

11. An electronic commerce card embodiment on a computer-readable medium that is created as a result of the steps in the method as recited in claim **1**.

12. A computer-readable medium having computer-executable instructions for performing the steps in the method as recited in claim **1**.

13. A computer programmed to perform the steps in the method as recited in claim **1**.

14. A method for registering for an online commerce card, comprising the following steps:

initiating, at the customer, a request for an online commerce card application;

downloading software code to the customer to assist in completing the card application;

submitting the application for the commerce card from the customer to the issuing authority; supplying a preliminary customer identifier to the customer;

submitting a request for a certificate from the issuing authority, the request including the preliminary customer identifier to identify the customer;

associating a customer account number with the customer; and

downloading a signed digital certificate from the issuing authority to the customer, the signed digital certificate comprising part of the commerce card.

15. A method as recited in claim **14**, wherein the supplying step comprises the step of providing the preliminary customer identifier to the customer through means other than online transmission.

16. A method as recited in claim **14**, wherein the step of submitting the request for a certificate comprises the following steps:

composing a public key;

generating a private key that is associated with the public key; and

submitting a request for certificate that includes the public and private keys.

17. A method as recited in claim **16**, further comprising the step of using the signed digital certificate and the private key as a password for communication between the customer and issuing authority.

18. A method as recited in claim **14**, further comprising downloading to the customer software code that supports a user interface button to invoke a user interface for facilitating commerce transactions.

19. A graphical user interface embodied on a computer-readable medium that presents the user interface button as recited in claim **18**.

20. Computer-readable media resident at the customer and the issuing authority having computer-executable instructions for performing the steps in the method as recited in claim **14**.

21. A method for utilizing an online commerce card in conducting online commerce transactions between a customer and a merchant, the commerce card having a permanent customer number associated therewith to identify the customer, comprising the following steps:

submitting a request for a proxy number from the customer to an authority;

generating the proxy number at the authority;

associating the proxy number with the permanent customer number;

issuing the proxy number to the customer; and

sending the proxy number, rather than the permanent customer number, to the merchant to commence the online commerce transaction.

22. A method as recited in claim **21**, further comprising the following steps:

generating a request that comprises a password unique to the customer;

digitally signing the request at the customer;

submitting the digitally signed request from the customer to the authority; and

authenticating the customer from the digitally signed request.

23. A method as recited in claim **21**, further comprising the step of displaying the proxy number returned from the authority.

24. Computer-readable media resident at the customer and the authority having computer-executable instructions for performing the steps in the method as recited in claim **21**.

25. A computer-implemented method for handling a request for an online commerce transaction number that can be used by a customer in conducting an online commerce transaction, comprising the following steps:

generating a transaction number;

associating the transaction number with a customer number that identifies the customer; and

transmitting the transaction number to the customer for use as a proxy for the customer number during the online commerce transaction.

26. A computer-implemented method as recited in claim **25**, wherein the associating step comprises the step of creating a record in a database, the record linking the transaction number to the customer number.

27. A computer-implemented method as recited in claim **25**, further comprising the step of assigning an expiration time to the transaction number that specifies when the transaction number expires.

28. A computer-readable medium having computer-executable instructions for performing the steps in the computer-implemented method as recited in claim **25**.

29. A computer programmed to perform the steps in the computer-implemented method as recited in claim **25**.

30. At an authority responsible for authorizing an online commerce transaction involving payment by an electronically transmitted account number, a computer-implemented method for handling an authorization request to honor the account number and accept payment, comprising the following steps:

determining whether the authorization request involves a permanent customer account number or a transaction number that is used as a proxy for the customer account number;

in an event that the authorization request involves a transaction number, performing the following steps:

using the transaction number to cross-reference to an associated customer account number;

substituting the associated customer account number in place of the transaction number; and

processing the authorization request using the associated customer account number.

31. A computer-implemented method as recited in claim **30**, further comprising the step of accessing a database containing customer account numbers and using the transaction number as an index to the database for locating the associated customer account number.

32. A computer-implemented method as recited in claim **30**, wherein after the processing step, the method further comprising the following steps:

substituting the transaction number in place of the customer account number; and

replying to the authorization request using the transaction number in lieu of the customer account number.

33. A computer-implemented method as recited in claim **30**, further comprising the step of adjusting an account associated with the customer account number to reflect the payment made in the online commerce transaction.

34. A computer-readable medium having computer-executable instructions for performing the steps in the computer-implemented method as recited in claim **30**.

35. A computer programmed to perform the steps in the computer-implemented method as recited in claim **30**.

36. A method for facilitating online commerce, comprising the following steps:

(A) conducting a registration phase between a customer and an issuing authority comprising the following steps:

(1) initiating, at the customer, a request for an online commerce card application;

(2) downloading software code to the customer to assist in completing the card application;

(3) submitting the application for the commerce card from the customer to the issuing authority;

(4) supplying a preliminary customer identifier to the customer;

(5) submitting, from the customer, a request for a certificate from the issuing authority, the request including the preliminary customer identifier to identify the customer; and

(6) associating a customer account number with the customer; and

(7) downloading a signed digital certificate from the issuing authority to the customer and software code that supports a user interface button to invoke a user interface for facilitating online commerce transactions, the signed digital certificate and user interface button forming the online commerce card having the customer account number associated therewith;

(B) utilizing the online commerce card to conduct an online commerce transaction phase between the customer and a merchant comprising the following steps:

(1) submitting a request to use the commerce card from the customer to the issuing authority;

(2) generating a transaction number;

(3) associating the transaction number with the customer account number; and

(4) transmitting the transaction number to the customer for use as a proxy for the customer account number during the online commerce transaction;

(5) sending the transaction number, rather than the permanent customer number, to the merchant to commence the online commerce transaction;

(C) conducting a payment authorization phase at the issuing authority in response to receiving an authorization request from the merchant to honor the transaction number and accept payment, comprising the following steps:

(1) identifying the authorization request as involving a transaction number that is used as a proxy for the customer account number;

(2) using the transaction number to cross-reference to the associated customer account number;

(3) substituting the associated customer account number in place of the transaction number;

(4) processing the authorization request using the associated customer account number;

(5) substituting the transaction number in place of the customer account number; and

(6) replying to the merchant using the transaction number in lieu of the customer account number.

37. A system for facilitating online commerce, comprising:

a customer computing unit resident at a customer site, the customer computing unit being configured with an online commerce card for use in online commerce transactions, the online commerce card being associated with a customer account number;

an authority computing system resident at an authority site, the authority computing system having a database to hold the customer account number, the authority computing system being configured to generate a transaction number, associate the transaction number with the customer account number in the database and electronically issue the transaction number to the customer computing unit;

the customer computing unit being configured to use the transaction number in an online commerce transaction with a merchant; and

the authority computing system being configured to receive from the merchant an authorization request for approval of the transaction number, the authority computing system using the transaction number to cross-reference in the database the associated customer account number and to process the authorization request with the customer account number.

38. A system as recited in claim **37**, wherein the customer account and transaction numbers are formatted with an equal number of digits.

39. A system as recited in claim **37**, wherein the authority computing system assigns an expiration term to the transaction number so that the transaction number is not valid after the expiration term elapses.

40. A system for issuing online commerce cards used in online commerce transactions, comprising:

a customer account manager to establish a customer account number for a customer and to associate the customer account number to a digital certificate that is unique to the customer, the digital certificate being in embodied in an electronically transmittable form which can be downloaded to the customer for use as an online commerce card;

a transaction number generator to generate a transaction number for an online commerce transaction in which the customer desires to engage; and

the customer account manager being configured to associate the transaction number with the customer account number, the transaction number being embodied in an electronically transmittable form which can be downloaded to the customer so that the customer can use the transaction number in the online commerce transaction as a proxy for the customer account number.

41. A software program embodied on a computer-readable medium incorporating the system as recited in claim **40**.

42. In an online commerce system, a system for handling an authorization request to approve an electronically transmittable number, comprising:

a transaction number identifier to identify the number as a transaction number that is used as a proxy for a customer account number; and

a customer account manager to cross-reference the customer account number using the transaction number and to substitute the transaction number for the customer account number for further processing.

43. A system as recited in claim **42**, wherein the customer account manager is configured to reverse substitute the transaction number back for the customer account number after the processing.

44. A software program embodied on a computer-readable medium incorporating the system as recited in claim **42**.

45. An electronically realizable commerce card embodied on a computer-readable medium comprising:

a first data field to hold a permanent customer account number having N digits and a predefined format that is recognized as an acceptable card number format;

a second data field to hold a temporary transaction number that serves as a proxy for the customer account number, the transaction number having the N digits and the format identical to the customer account number; and

wherein the first and second data fields are related to associate the customer account number with the transaction number.

* * * * *

US005903830A

United States Patent [19]

Joao et al.

[11] Patent Number: 5,903,830

[45] Date of Patent: May 11, 1999

[54] **TRANSACTION SECURITY APPARATUS AND METHOD**

[76] Inventors: **Raymond Anthony Joao**, 122 Bellevue Pl., Yonkers, N.Y. 10703; **Robert Richard Bock**, 27 Sumner Ave., Yonkers, N.Y. 10704

[21] Appl. No.: **08/874,051**

[22] Filed: **Jun. 12, 1997**

Related U.S. Application Data

[63] Continuation of application No. 08/694,199, Aug. 8, 1996.

[51] **Int. Cl.**[6] **H04Q 7/08**; H04Q 7/10; H04Q 7/32

[52] **U.S. Cl.** **455/406**; 455/408; 455/405; 455/410; 455/31.3

[58] **Field of Search** 455/410, 411, 455/405, 406, 407, 408, 409, 426; 379/91.01, 91.02, 93.17, 93.23, 93.02; 340/825.33, 825.34, 825.44, 825.3, 825.32; 705/38

[56] **References Cited**

U.S. PATENT DOCUMENTS

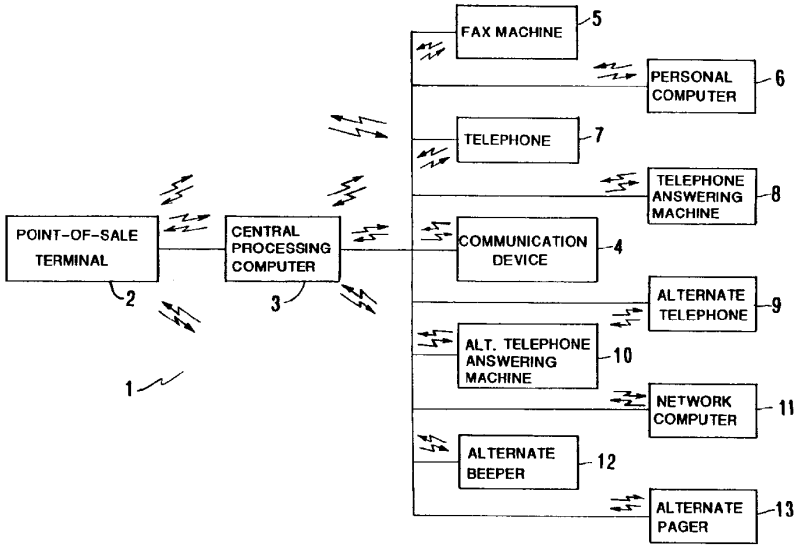
3,723,655	3/1973	Zucker et al. .	
3,938,090	2/1976	Borison et al. .	
4,485,300	11/1984	Peirce .	
4,758,714	7/1988	Carlson et al. .	
4,947,027	8/1990	Golightly .	
5,173,594	12/1992	McClure .	
5,177,342	1/1993	Adams	340/825.33
5,243,645	9/1993	Bissell et al. .	
5,335,278	8/1994	Matchett et al.	455/410
5,345,595	9/1994	Johnson et al.	455/410
5,357,563	10/1994	Hamilton et al. .	
5,406,619	4/1995	Akhteruzzaman et al. .	
5,444,616	8/1995	Nair et al. .	
5,444,763	8/1995	Lazaridis et al. .	
5,473,667	12/1995	Neustein .	
5,479,510	12/1995	Olsen et al. .	
5,485,510	1/1996	Colbert .	
5,513,250	4/1996	McAllister .	
5,526,407	6/1996	Russell et al. .	
5,530,438	6/1996	Bickham et al.	340/825.32
5,615,110	3/1997	Wong .	
5,631,947	5/1997	Wittstein et al. .	
5,655,007	8/1997	McAllister .	
5,661,285	8/1997	Elrick et al. .	
5,699,528	12/1997	Hogan .	
5,708,422	1/1998	Blonder et al.	340/825.34

Primary Examiner—Wellington Chin
Assistant Examiner—Keith Ferguson
Attorney, Agent, or Firm—Raymond A. Joao

[57] **ABSTRACT**

A transaction security apparatus which comprises a receiver for receiving one of a limitation and a restriction on an account usage, wherein the one of a limitation and a restriction on an account usage are received in real-time from an individual account holder, a memory for storing the one of a limitation and a restriction on an account usage, and a central processing device for processing an authorization request for a transaction on an account in conjunction with the one of a limitation and a restriction on an account usage. The central processing device generates a first signal, wherein the first signal contains information for one of authorizing and disallowing the transaction. A method for transaction security which comprises receiving one of a limitation and a restriction on an account usage, wherein the one of a limitation and a restriction on an account usage are received in real-time from an individual account holder, storing the one of a limitation and a restriction on an account usage, processing an authorization request for a transaction on an account in conjunction with the one of a limitation and a restriction on an account usage, and determining whether the transaction is one of authorized and unauthorized.

20 Claims, 14 Drawing Sheets



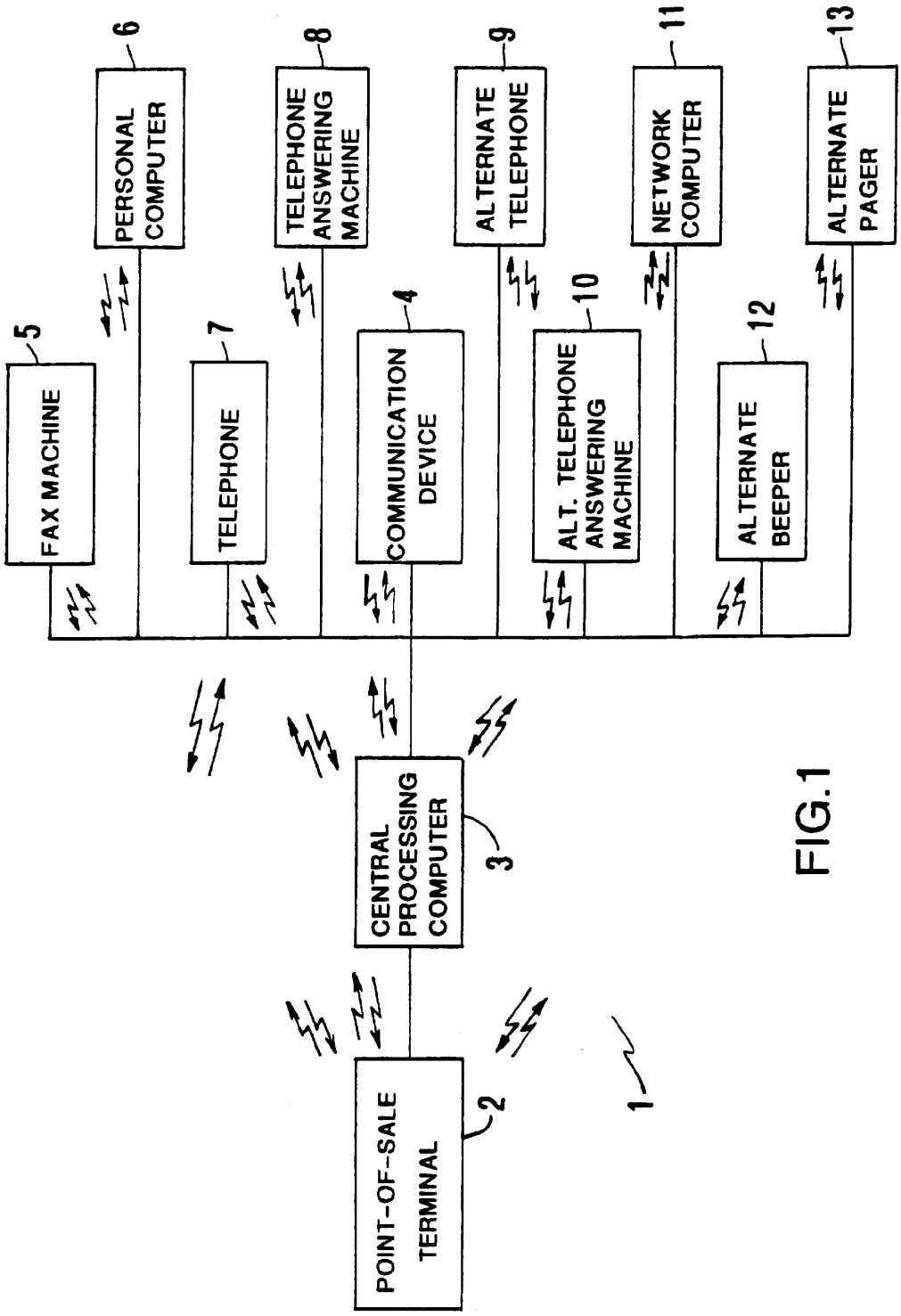

POINT-OF-SALE TERMINAL
2
CENTRAL PROCESSING COMPUTER
3
COMMUNICATION DEVICE
4
FAX MACHINE
5
PERSONAL COMPUTER
6
TELEPHONE
7
TELEPHONE ANSWERING MACHINE
8
ALTERNATE TELEPHONE
9
ALT. TELEPHONE ANSWERING MACHINE
10
NETWORK COMPUTER
11
ALTERNATE BEEPER
12
ALTERNATE PAGER
13
1

FIG.1

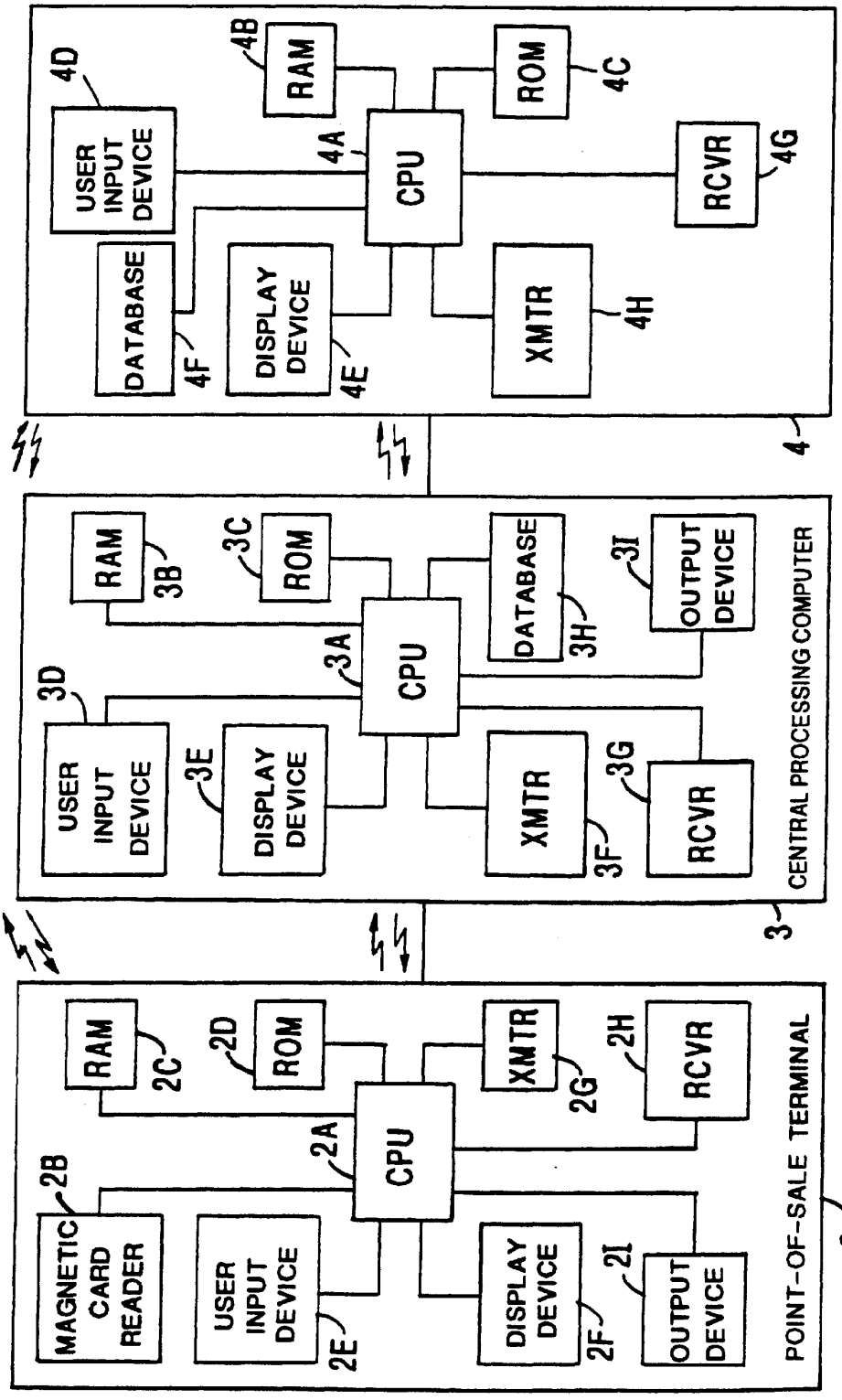

4D
USER INPUT DEVICE
4B
RAM
ROM
4C
4A
CPU
RCVR
4G
DATABASE
4F
DISPLAY DEVICE
4E
XMTR
4H
4
3C
ROM
RAM
3B
DATABASE
3H
3I
OUTPUT DEVICE
3A
CPU
3D
USER INPUT DEVICE
3E
DISPLAY DEVICE
XMTR
3F
3G
RCVR
CENTRAL PROCESSING COMPUTER
3
RAM
2C
2D
ROM
XMTR
2G
2H
RCVR
2A
CPU
2B
MAGNETIC CARD READER
USER INPUT DEVICE
2E
DISPLAY DEVICE
2F
2I
OUTPUT DEVICE
POINT-OF-SALE TERMINAL
2

FIG.2

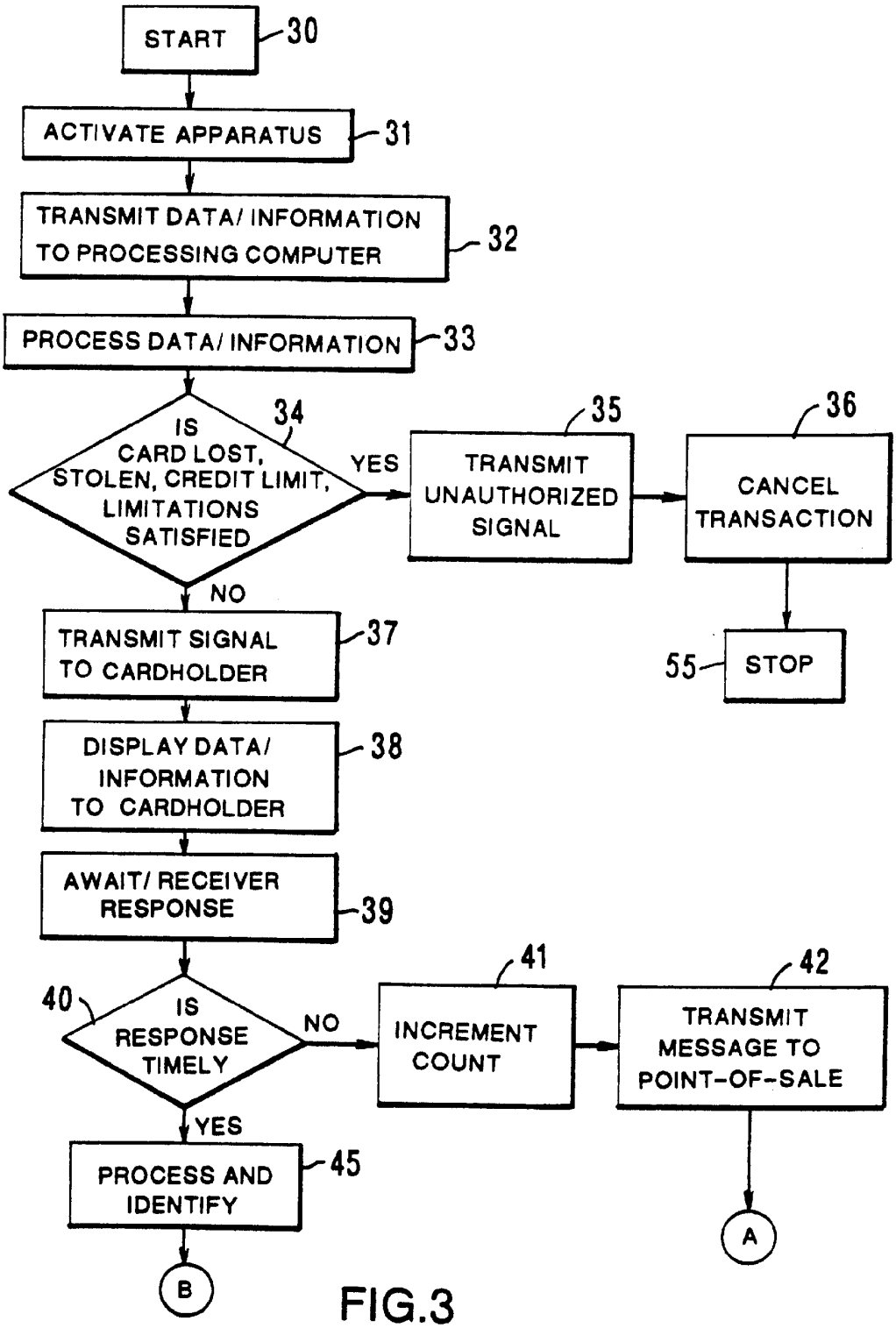

START
30
ACTIVATE APPARATUS
31
TRANSMIT DATA/ INFORMATION TO PROCESSING COMPUTER
32
PROCESS DATA/ INFORMATION
33
IS CARD LOST, STOLEN, CREDIT LIMIT, LIMITATIONS SATISFIED
34
YES
35
TRANSMIT UNAUTHORIZED SIGNAL
36
CANCEL TRANSACTION
55
STOP
NO
TRANSMIT SIGNAL TO CARDHOLDER
37
DISPLAY DATA/ INFORMATION TO CARDHOLDER
38
AWAIT/ RECEIVER RESPONSE
39
40
IS RESPONSE TIMELY
NO
41
INCREMENT COUNT
42
TRANSMIT MESSAGE TO POINT-OF-SALE
YES
PROCESS AND IDENTIFY
45
A
B

FIG.3

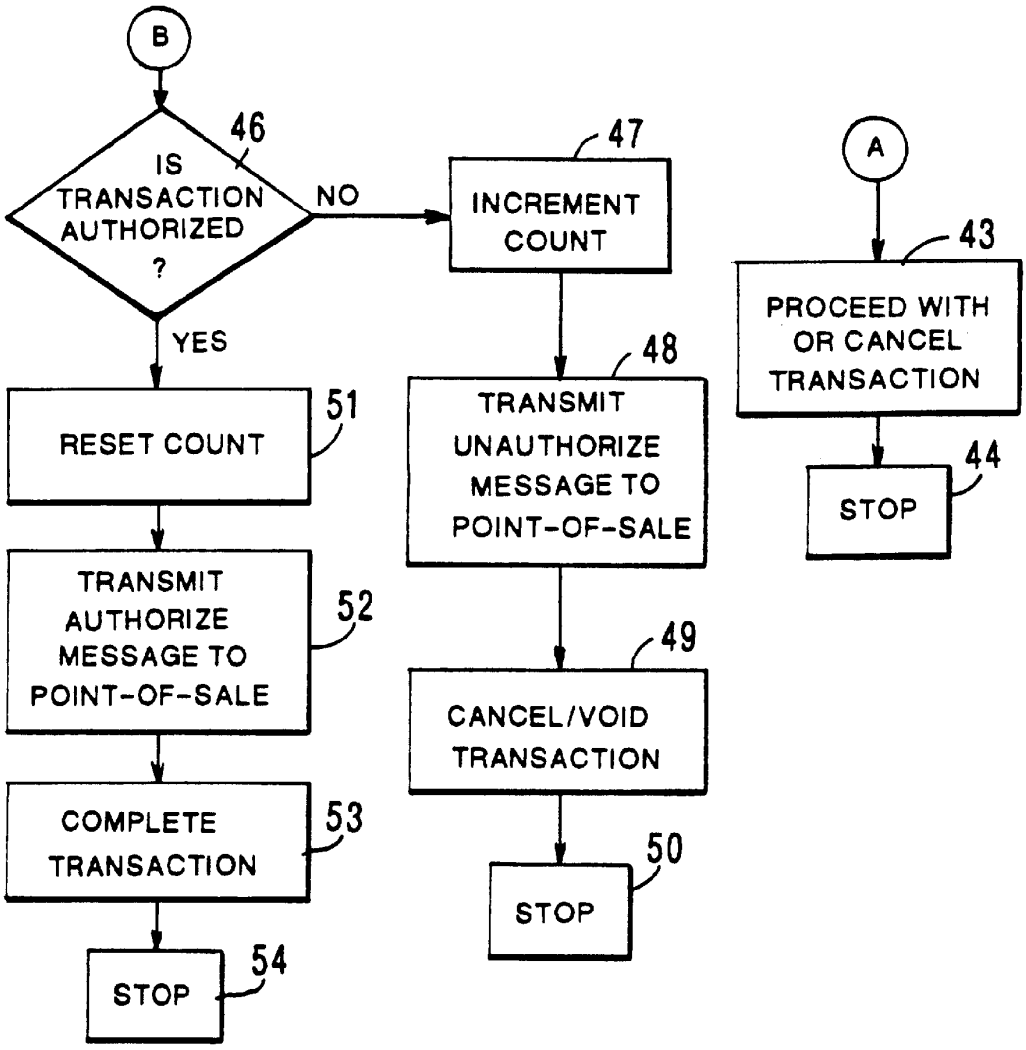

B
46
IS TRANSACTION AUTHORIZED ?
NO
YES
47
INCREMENT COUNT
48
TRANSMIT UNAUTHORIZE MESSAGE TO POINT-OF-SALE
49
CANCEL/VOID TRANSACTION
50
STOP
A
43
PROCEED WITH OR CANCEL TRANSACTION
44
STOP
51
RESET COUNT
52
TRANSMIT AUTHORIZE MESSAGE TO POINT-OF-SALE
53
COMPLETE TRANSACTION
54
STOP

FIG.3 (CONT.)

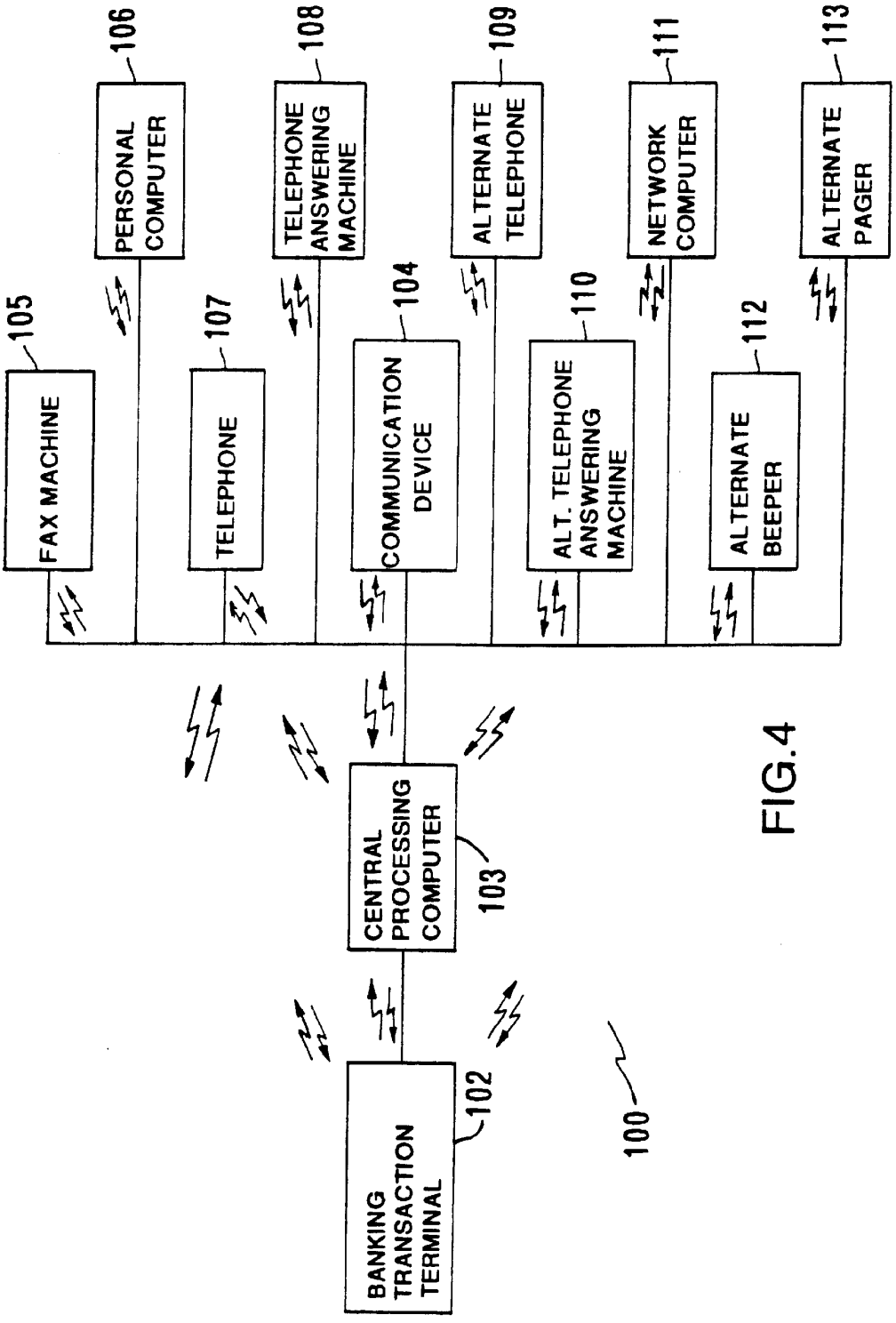

BANKING TRANSACTION TERMINAL
102
CENTRAL PROCESSING COMPUTER
103
100
COMMUNICATION DEVICE
104
FAX MACHINE
105
PERSONAL COMPUTER
106
TELEPHONE
107
TELEPHONE ANSWERING MACHINE
108
ALTERNATE TELEPHONE
109
ALT. TELEPHONE ANSWERING MACHINE
110
NETWORK COMPUTER
111
ALTERNATE BEEPER
112
ALTERNATE PAGER
113

FIG.4

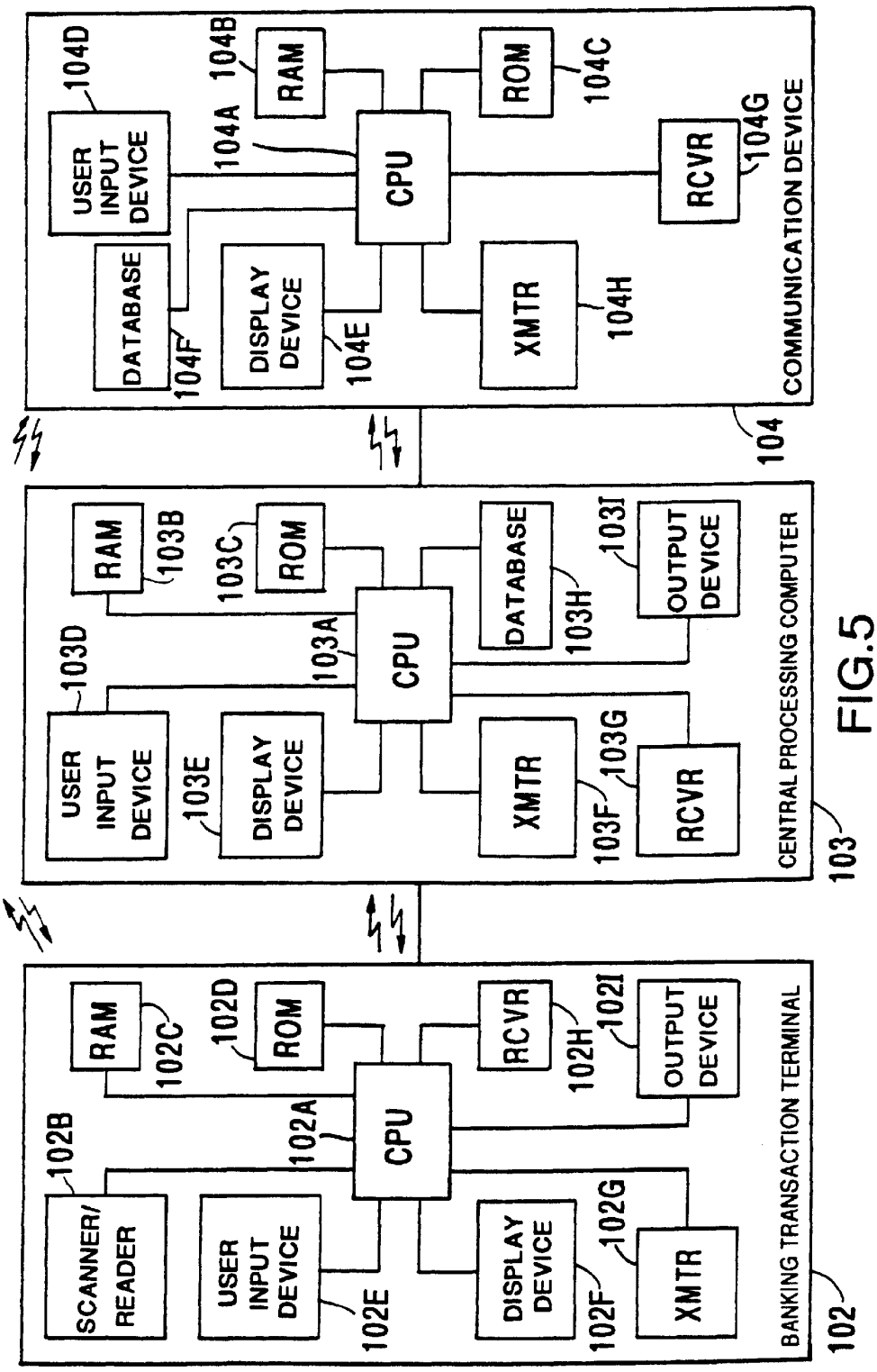

BANKING TRANSACTION TERMINAL
102
SCANNER/ READER
102B
USER INPUT DEVICE
102E
DISPLAY DEVICE
102F
XMTR
102G
CPU
102A
RAM
102C
ROM
102D
RCVR
102H
OUTPUT DEVICE
102I
CENTRAL PROCESSING COMPUTER
103
USER INPUT DEVICE
103D
DISPLAY DEVICE
103E
XMTR
103F
RCVR
103G
CPU
103A
RAM
103B
ROM
103C
DATABASE
103H
OUTPUT DEVICE
103I
COMMUNICATION DEVICE
104
USER INPUT DEVICE
104D
DATABASE
104F
DISPLAY DEVICE
104E
XMTR
104H
CPU
104A
RAM
104B
ROM
104C
RCVR
104G

FIG.5

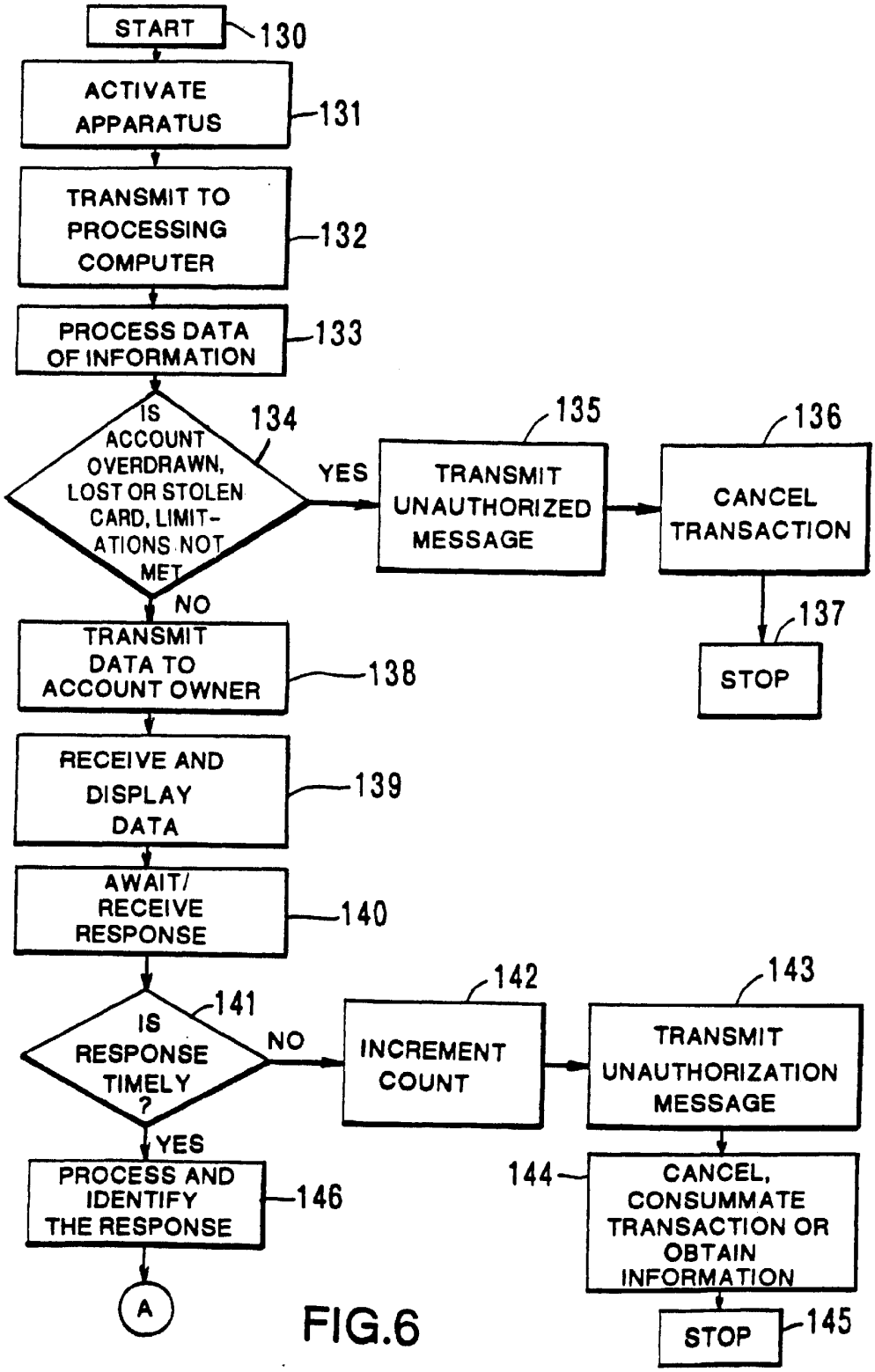

START
130
ACTIVATE APPARATUS
131
TRANSMIT TO PROCESSING COMPUTER
132
PROCESS DATA OF INFORMATION
133
IS ACCOUNT OVERDRAWN, LOST OR STOLEN CARD, LIMIT-ATIONS NOT MET
134
YES
135
TRANSMIT UNAUTHORIZED MESSAGE
136
CANCEL TRANSACTION
137
STOP
NO
TRANSMIT DATA TO ACCOUNT OWNER
138
RECEIVE AND DISPLAY DATA
139
AWAIT/ RECEIVE RESPONSE
140
IS RESPONSE TIMELY ?
141
NO
142
INCREMENT COUNT
143
TRANSMIT UNAUTHORIZATION MESSAGE
144
CANCEL, CONSUMMATE TRANSACTION OR OBTAIN INFORMATION
145
STOP
YES
PROCESS AND IDENTIFY THE RESPONSE
146
A

FIG.6

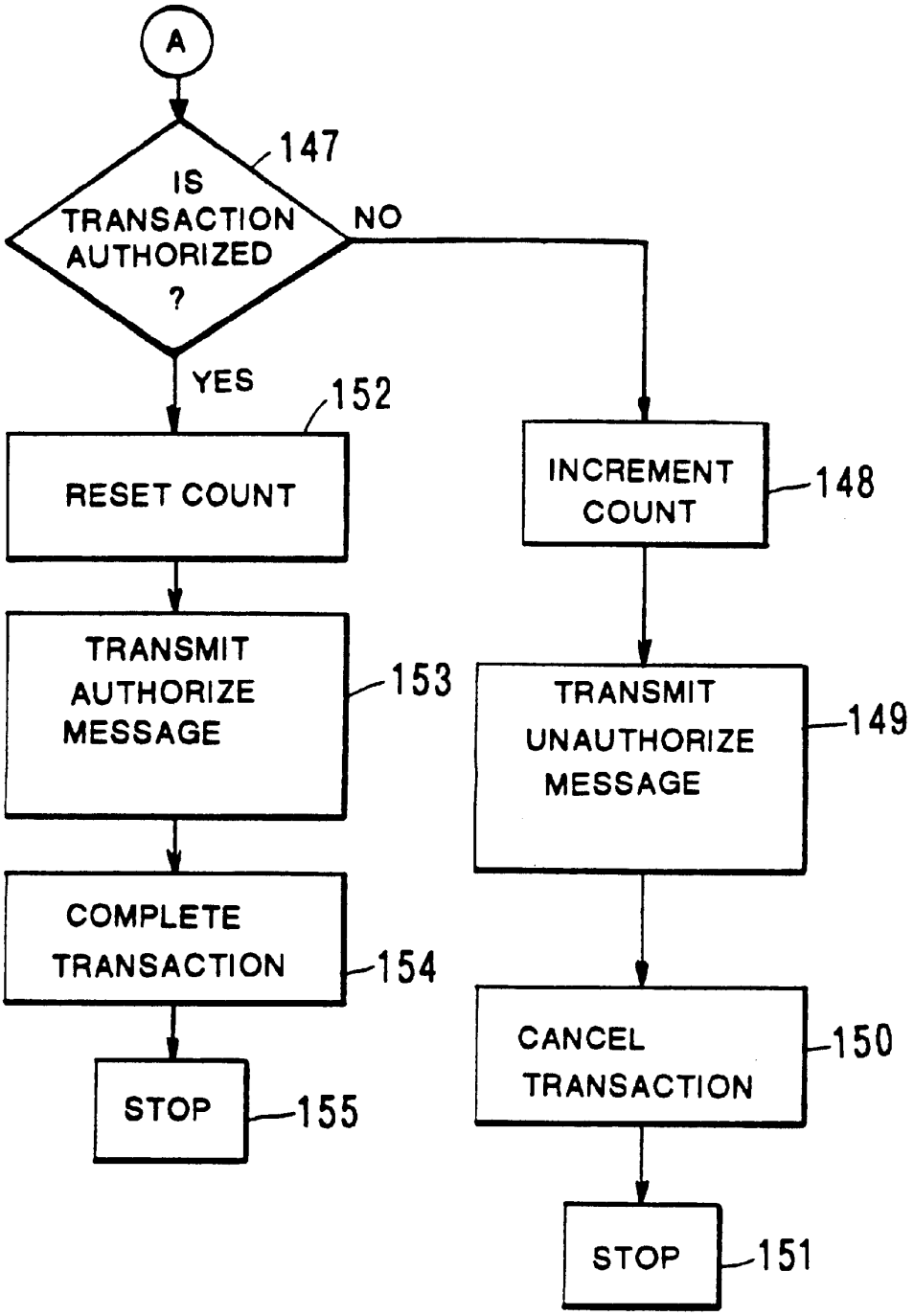

A
147
IS TRANSACTION AUTHORIZED ?
NO
YES
152
RESET COUNT
INCREMENT COUNT
148
TRANSMIT AUTHORIZE MESSAGE
153
TRANSMIT UNAUTHORIZE MESSAGE
149
COMPLETE TRANSACTION
154
CANCEL TRANSACTION
150
STOP
155
STOP
151

FIG.6 (CONT.)

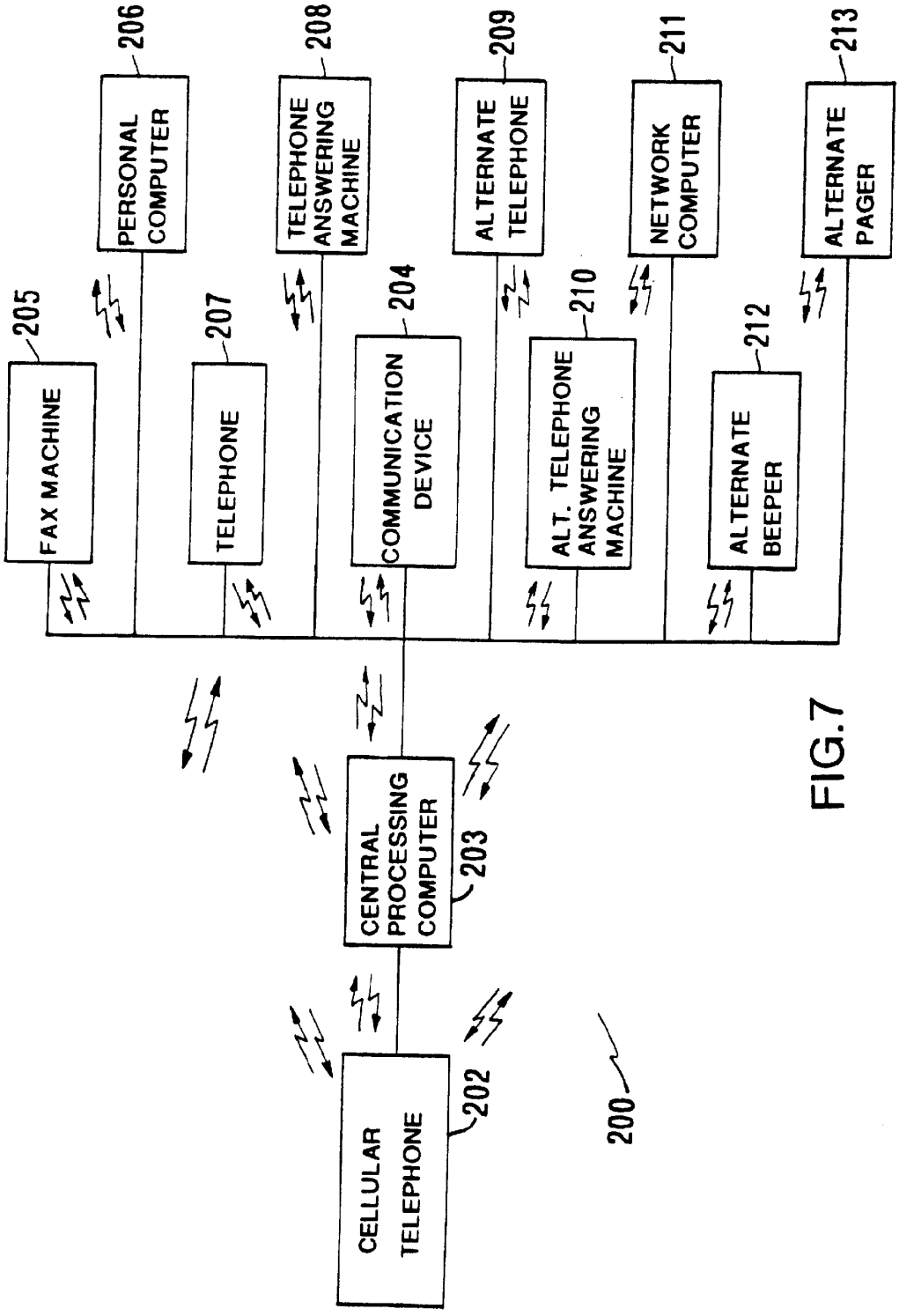

206
PERSONAL COMPUTER
208
TELEPHONE ANSWERING MACHINE
209
ALTERNATE TELEPHONE
211
NETWORK COMPUTER
213
ALTERNATE PAGER
205
FAX MACHINE
207
TELEPHONE
204
COMMUNICATION DEVICE
210
ALT. TELEPHONE ANSWERING MACHINE
212
ALTERNATE BEEPER
CENTRAL PROCESSING COMPUTER
203
CELLULAR TELEPHONE
202
200

FIG.7

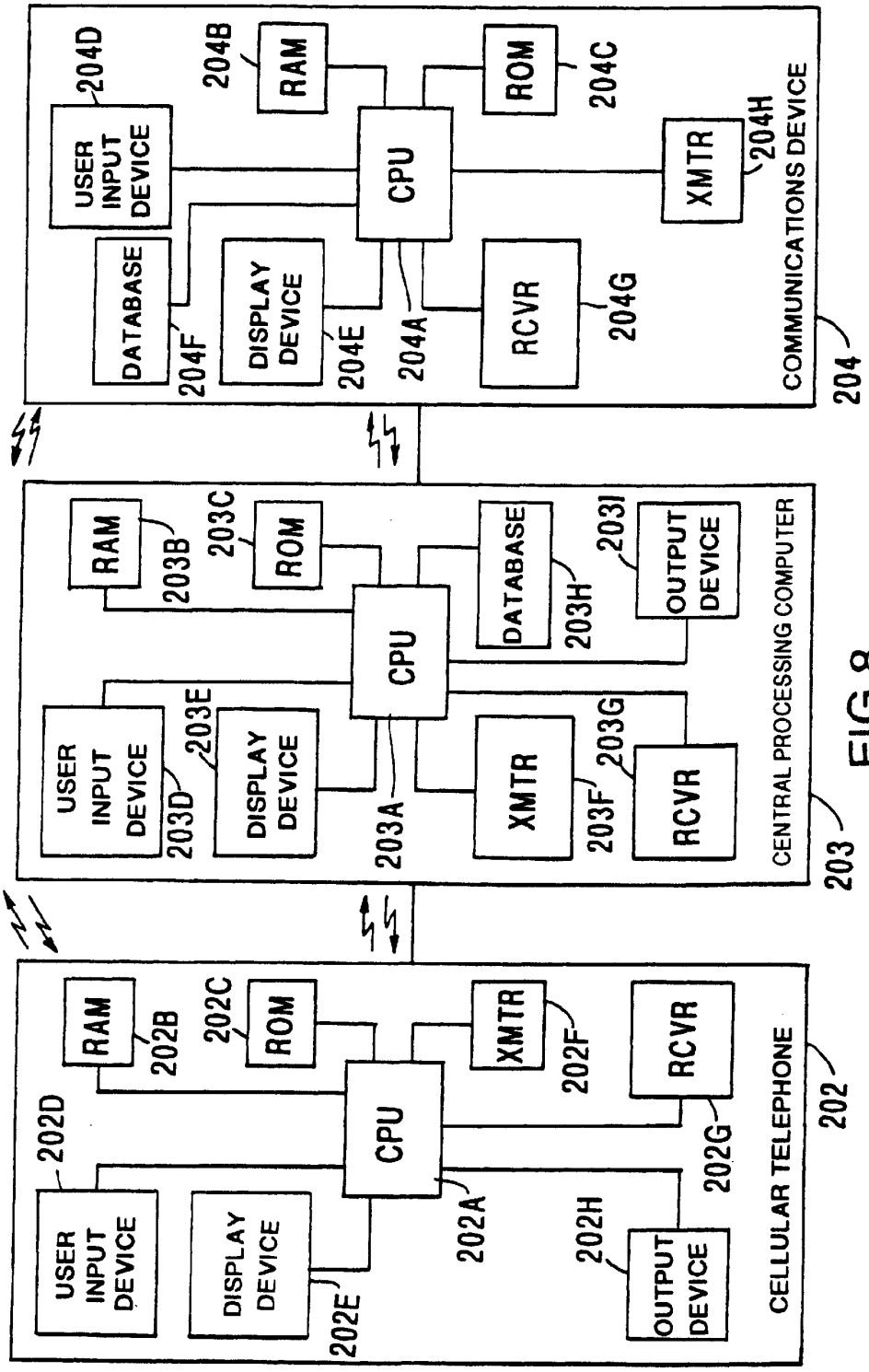

CELLULAR TELEPHONE
202
RAM
202B
ROM
202C
CPU
202A
XMTR
202F
RCVR
202G
USER INPUT DEVICE
202D
DISPLAY DEVICE
202E
OUTPUT DEVICE
202H
CENTRAL PROCESSING COMPUTER
203
RAM
203B
ROM
203C
CPU
203A
DATABASE
203H
OUTPUT DEVICE
203I
USER INPUT DEVICE
203D
DISPLAY DEVICE
203E
XMTR
203F
RCVR
203G
COMMUNICATIONS DEVICE
204
RAM
204B
ROM
204C
CPU
204A
USER INPUT DEVICE
204D
DATABASE
204F
DISPLAY DEVICE
204E
XMTR
204H
RCVR
204G

FIG.8

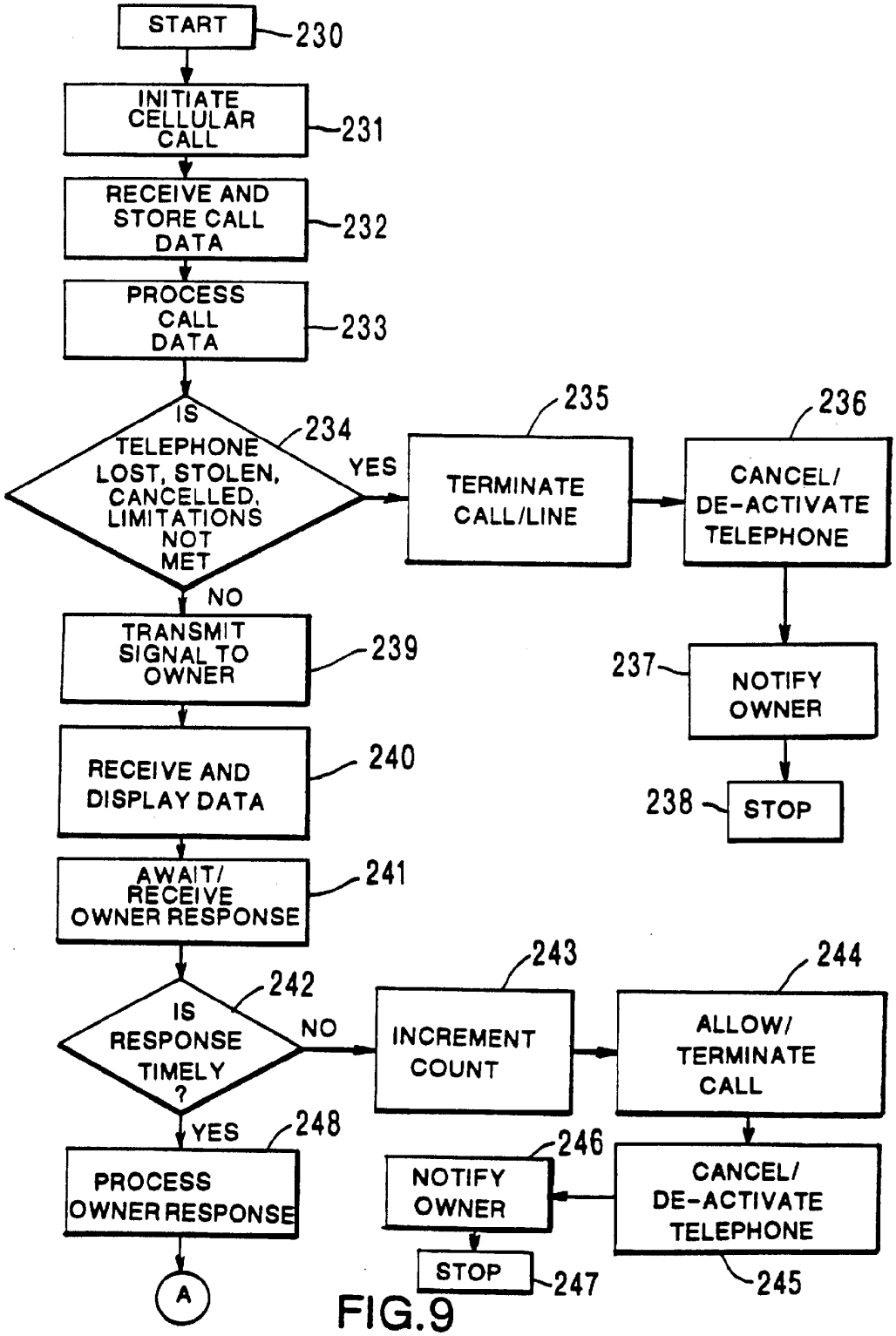

START
230
INITIATE CELLULAR CALL
231
RECEIVE AND STORE CALL DATA
232
PROCESS CALL DATA
233
IS TELEPHONE LOST, STOLEN, CANCELLED, LIMITATIONS NOT MET
234
YES
NO
235
TERMINATE CALL/LINE
236
CANCEL/ DE-ACTIVATE TELEPHONE
237
NOTIFY OWNER
238
STOP
TRANSMIT SIGNAL TO OWNER
239
RECEIVE AND DISPLAY DATA
240
AWAIT/ RECEIVE OWNER RESPONSE
241
IS RESPONSE TIMELY ?
242
NO
YES
243
INCREMENT COUNT
244
ALLOW/ TERMINATE CALL
245
CANCEL/ DE-ACTIVATE TELEPHONE
246
NOTIFY OWNER
247
STOP
248
PROCESS OWNER RESPONSE
A

FIG.9

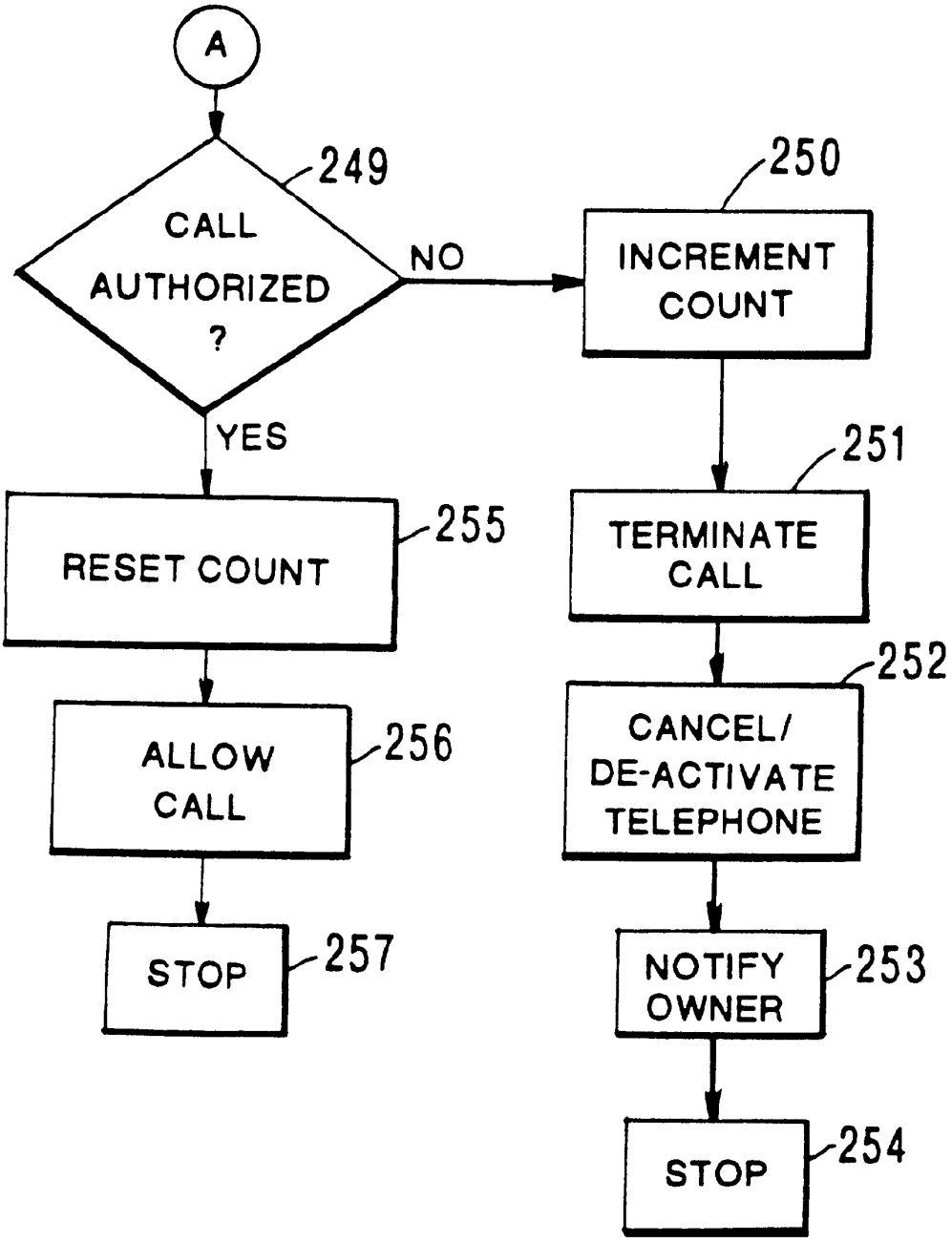

A
249
CALL AUTHORIZED ?
NO
YES
250
INCREMENT COUNT
251
TERMINATE CALL
252
CANCEL/ DE-ACTIVATE TELEPHONE
253
NOTIFY OWNER
254
STOP
255
RESET COUNT
256
ALLOW CALL
257
STOP

FIG.9 (CONT.)

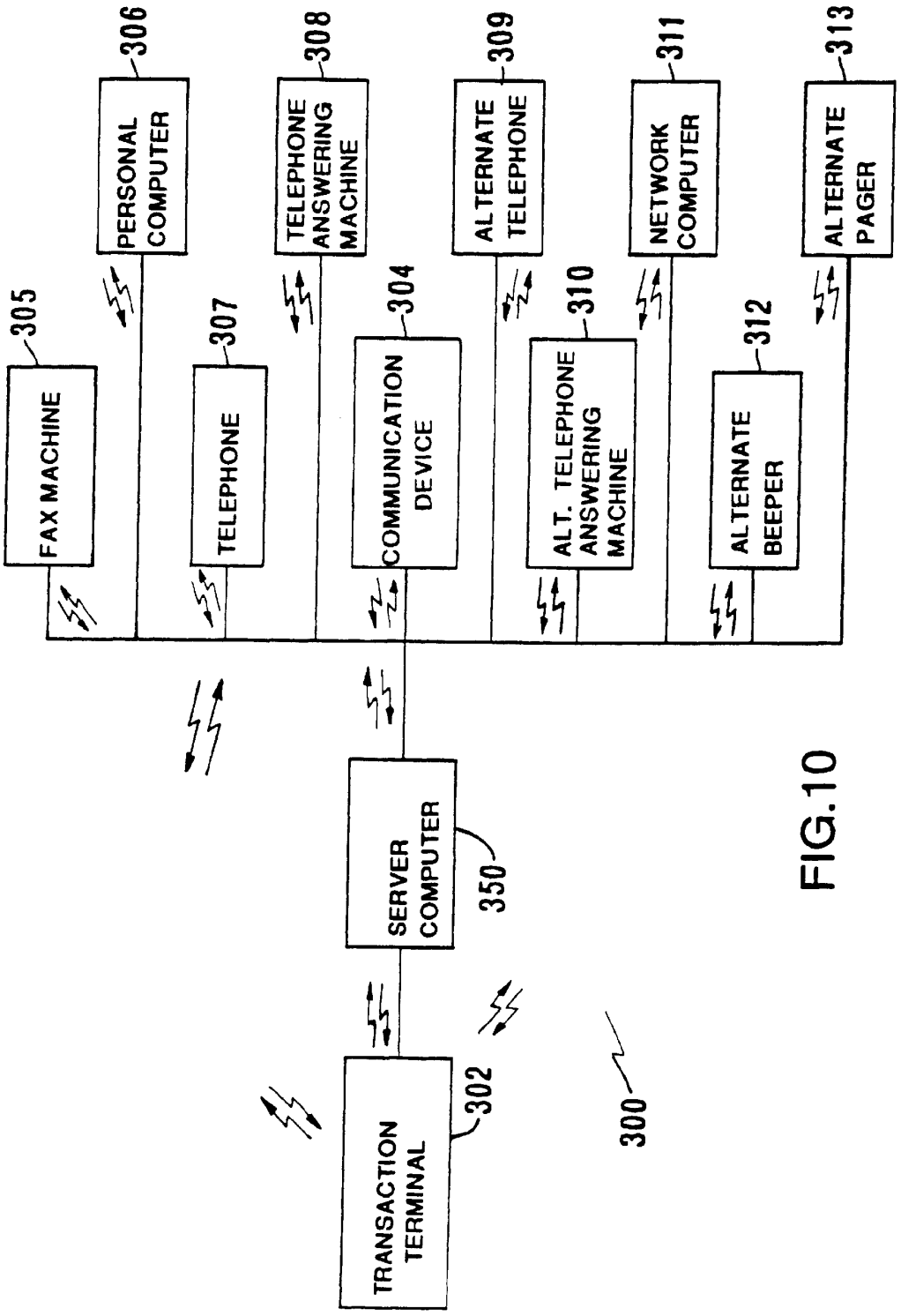

306
PERSONAL COMPUTER
308
TELEPHONE ANSWERING MACHINE
309
ALTERNATE TELEPHONE
311
NETWORK COMPUTER
313
ALTERNATE PAGER
305
FAX MACHINE
307
TELEPHONE
304
COMMUNICATION DEVICE
310
ALT. TELEPHONE ANSWERING MACHINE
312
ALTERNATE BEEPER
SERVER COMPUTER
350
TRANSACTION TERMINAL
302
300

FIG.10

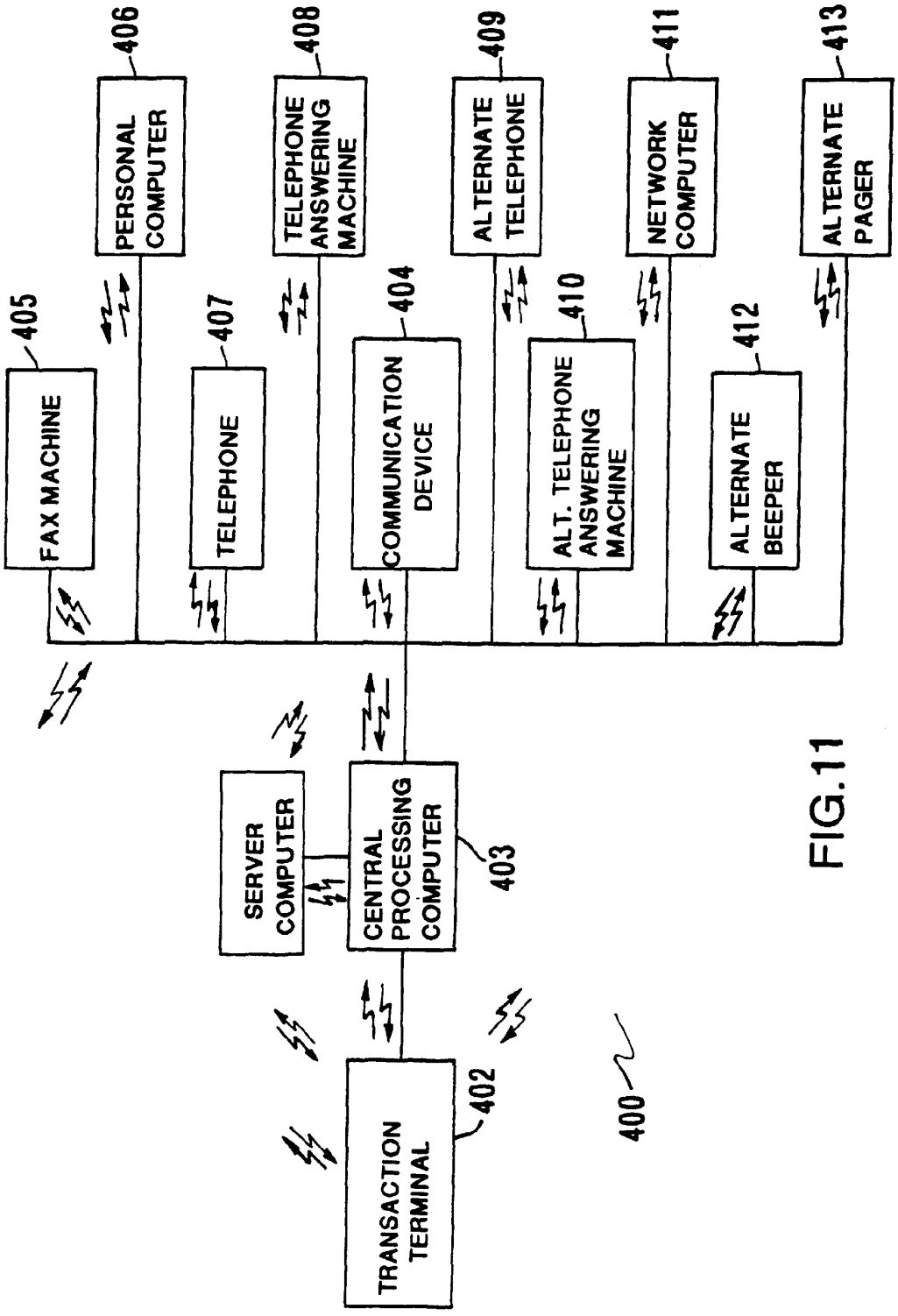

406
PERSONAL COMPUTER
408
TELEPHONE ANSWERING MACHINE
409
ALTERNATE TELEPHONE
411
NETWORK COMPUTER
413
ALTERNATE PAGER
405
FAX MACHINE
407
TELEPHONE
404
COMMUNICATION DEVICE
410
ALT. TELEPHONE ANSWERING MACHINE
412
ALTERNATE BEEPER
SERVER COMPUTER
CENTRAL PROCESSING COMPUTER
403
TRANSACTION TERMINAL
402
400

FIG.11

TRANSACTION SECURITY APPARATUS AND METHOD

This is a continuation application of application Ser. No. 08,694,199, filed Aug. 8, 1996.

FIELD OF THE INVENTION

The present invention pertains to a financial transaction and/or wireless communication device authorization, notification and/or security apparatus and method, and, in particular to a financial transaction and/or wireless communication device authorization, notification and/or security apparatus and method for use in providing authorization, notification and/or security in conjunction with credit card, charge card and/or debit card use, savings and/or checking account activity and/or cellular telephone use.

BACKGROUND OF THE PRESENT INVENTION

Millions of individuals enjoy the convenience of utilizing credit cards, charge cards, debit cards, and/or currency or "smart" cards as a convenient way in which to purchase goods and/or services. By utilizing credit cards, charge cards, debit cards, and/or currency or "smart" cards, an individual may enter into a transaction without having to have cash or currency in hand or otherwise. In the case of credit cards, charge cards and debit cards, the individual, in effect obtains an instant loan of the funds needed to make a purchase and/or enter into a transaction. In the case of currency or "smart" cards, the individual may "store" an amount of money on the card(s) and, thereafter, utilize the card(s), instead of cash or currency, in order to make purchases and/or enter into transactions.

Millions of individuals also enjoy the benefits of having savings accounts, checking accounts and/or automated teller machine accounts which allow then to enjoy the security of saving their money in accounts which are usually insured and which allow them to, in some instances, earn interest on their money. In the case of checking accounts, individuals enjoy the convenience of writing checks and/or other transaction instruments which allow them to draw against their money without having to undergo the inconvenience of going to the bank or financial institution to withdraw their money, in currency form, and traveling to, in some cases, a distant location to either make a purchase, payment and/or to otherwise settle an account. In this regard, the ability to write checks, drafts and/or other instruments against an account is a very convenient manner in which to conduct transactions of any kind.

In the case of automated teller machines, individuals may conveniently withdraw and/or deposit money into a bank of other financial account.

Many individuals also enjoy the convenience of owning and/or using wireless, mobile or cellular telephones or devices as a means by which to make telephone calls when a conventional line or permanent telephone is not within reach and/or when the individual is "on the go", such as in an automobile, on foot, and/or in any other type of environment, such as away from home, when a conventional line or permanently fixed telephone is not available.

Unfortunately, with the convenience of each of the above credit cards, charge cards, debit cards, and/or currency or "smart" cards, savings accounts, checking accounts, automated teller machine accounts, and cellular telephones or cellular communications devices, comes many disadvantages and the opportunity for theft and/or fraud. In the case

of credit cards, charge cards and/or debit cards, hundreds of millions, if not billions, of dollars a year are lost as a result of the theft of, and/or the fraudulent use of, credit cards, charge cards and/or debit cards, or the account numbers which correspond thereto.

A lost or stolen card may be utilized by an unauthorized individual to spend upwards of thousands of dollars before the unauthorized use is detected and/or before the cardholder can ascertain, and/or be notified, either by the card issuer or servicing institution or when the cardholder detects the unauthorized transaction on his or her monthly account statement, that the card is lost or stolen. Similarly, even in the absence of the physical card, an unauthorized individual may utilize the account number which corresponds to the card in order to make certain transactions.

While card holders are usually protected by various coverages which shield them from the liabilities associated with the fraudulent use of a card or the corresponding account number, the card issuers, credit, charge and/or debit card issuing companies and/or institutions, and/or their insurance companies, end up paying for the above described thefts and/or fraudulent and/or unauthorized uses. Ultimately, the consumer also shoulders the burden of the costs associated with these thefts and/or fraudulent and/or unauthorized uses in the form of increased prices.

While authorization terminals and/or devices are utilized at a point-of-sale and/or at the vendor's, the seller's, or the service provider's, location, these authorization terminals and/or devices typically are utilized to obtain an authorization from the card issuer or account servicing institution which, usually entails a screening of whether the card has been lost, stolen, cancelled, de-activated and/or whether the cardholder has exceeded and/or will exceed his or her credit limit. This current authorization practice fails to prevent the use of a lost or stolen card, or the unauthorized use of either the card or the account number corresponding thereof, if the card has not been reported, and/or discovered, to be lost, stolen or used without authorization and/or if the account credit limit has not yet been reached.

Current practices do not entail and/or do not include the provision for obtaining an authorization, and/or for providing notice to the cardholder before, during and/or shortly after a transaction, which cardholder authorization and/or notification procedure would be helpful and prove to be essential in preventing the fraudulent use and/or unauthorized use of a card and/or the account number corresponding thereto in a unauthorized transaction and/or shortly thereafter an unauthorized transaction has occurred, thereby minimizing the fraudulent and/or unauthorized use of the card and/or the account number corresponding thereto.

In the case of currency or "smart" cards, which typically may serve as bearer instruments, the monetary credit on these cards may be completely depleted before the card owner even discovers same to be lost or stolen.

In the case of savings accounts, checking accounts, and/or automated teller machine accounts, these accounts may be accessed, and funds be withdrawn, without the account owner's notification and/or knowledge. In the case of savings accounts and checking accounts, these accounts may be accessed, and/or funds may be withdrawn therefrom, when checks drawn on insufficient funds are returned, and/or when the account number is inadvertently and/or fraudulently utilized in an endorsement, or otherwise, by an individual attempting to cash or perform a transaction with a fraudulent instrument, a forged instrument and/or an otherwise "bad" check. In these instances, the accounts and/or funds involved

are usually accessed, invaded, and/or withdrawn from the account involved without the account owner being notified and/or having a say in the matter.

The account owner is typically notified of the above-described activity involving his or her account days later when he or she either receives a mailed notice and/or when they receive and review their monthly or periodic statement, which notice may be received at a time when it may be too late for the account owner to stop or reverse the transaction and/or, in the case of a check or draft returned for insufficient funds, at a time which is too late for the account owner to attempt to collect the funds. In the case of automated teller machine accounts, these accounts may be accessed, such as with a lost, stolen, or counterfeit card and/or with a card account number(s) and/or associated personal identification number(s), by a thief or by any other unauthorized person who could then make an unauthorized withdrawal(s) therefrom.

Once again, the account owner would not receive notification and/or have knowledge of the unauthorized transaction until they are notified by the bank or financial institution either via a monthly and/or periodic statement, and/or when they attempt a transaction at the automated teller machine and, at that time, discover that funds are missing and/or have been withdrawn. In the case of savings accounts, checking accounts and/or automated teller machine accounts, there is no present apparatus or method by which to provide notification to an account owner at the time of the unauthorized transaction and/or account activity and/or shortly thereafter same.

In the case of cellular telephones, recent practices involving "cloning" cellular telephones, which entails intercepting telephone transmissions from a cellular telephone, which transmissions contain the phone number of the transmitting phone and/or the associated personal identification number (PIN), and utilizing the intercepted information to program a different cellular phone which by then be utilized in conjunction with the account of the "cloned" cellular telephone, has also resulted in widespread theft and fraudulent use of cellular telephones and/or cellular communications devices The "cloned" telephones are typically sold on the "black" market. In these instances, the cellular telephone owner has no way of knowing whether, or when, his or her cellular transmissions are being intercepted and/or if and when a "cloned" cellular phone is created and/or is utilized on, or over, his or her cellular telephone account.

Typically, the cellular telephone owner first becomes aware of the unauthorized usage of his or her cellular telephone account when he or she receives their telephone account statement. Once again, in the time between the "cloning" of the cellular telephone and the discovery of same, hundreds, if not thousands, of dollars worth of cellular telephone calls may have been made before the unauthorized use is detected. At present, there is no apparatus or method for providing notification to the cellular telephone owner as to when his or her cellular telephone and/or cellular telephone number is, or has been, utilized in an unauthorized manner.

SUMMARY OF THE INVENTION

The present invention provides an apparatus and a method for providing financial transaction authorization, notification and/or security, and, in particular, provides an apparatus and a method for providing financial transaction authorization, notification and/or security in conjunction with credit card, charge card, debit card, and/or currency or "smart" card use, savings and/or checking account activity and use and/or cellular telephone use, which overcomes the shortcomings of the prior art.

The apparatus and method of the present invention, which is utilized in conjunction with a credit card, a charge card, a debit card and/or a currency or "smart" card authorization process comprises a point-of-sale authorization terminal which terminals are found in various establishments and which are utilized in conjunction with the sale of goods and/or services and/or in other types of financial transactions. The point-of-sale terminal may be utilized at the location of the seller and/or service provider, such as at a retail store or office, and/or the point-of-sale terminal may be located at the site of the goods or service provider or vendor, such as in cases when the sale is a telephone order, mail order and/or other type of transaction, including transactions made on, or over, the INTERNET and/or other on-line services or communication networks or mediums.

The apparatus also comprises a central processing computer for processing the credit, charge, debit and/or currency or "smart" card and/or other transaction requests, and data and/or information pertaining thereto, and/or the authorization pertaining thereto. The central processing computer may service any predefined group of card holders and/or any pre-defined group(s) and/or type(s) of cards. The central processing computer may also process accounts for any of the various banks and/or financial institutions which issue and/or manage credit cards, charge cards, debit cards and/or currency or "smart" cards and/or process or manage these accounts.

The point-of-sale terminal is linked and/or connected to the central processing computer via a communications system, link and/or medium, such as, for example, a telephone network or line. The communications system which is utilized may be any communications system and may include telecommunication systems, satellite communications systems, radio communication systems, digital satellite communications systems, personal communications services communication systems as well as any other appropriate communications system.

The point-of-sale terminal transmits signals and/or data to the central processing computer as well as receives signals and/or data from the central processing computer.

The apparatus also comprises a cardholder communication device which may receive signals and/or data from either or both of the point-of-sale terminal and/or the central processing computer. The communication device may also be equipped with a transmitter for transmitting signals and/or data to the central processing computer. In this regard, the central processing computer transmits signals and/or data to the communication device as well as receives signals and/or data from the communication device. The communication device may also transmit signals and/or data directly to the point-of-sale terminal and receive signals and/or data directly from the point-of-sale terminal.

The point-of-sale terminal may transmit signals and/or data to the central processing computer and to the communication device and may receive signals and/or data from the central processing computer and from the communication device.

The communication device may be a wireless device. In this regard, the communication device may be a telephone signal receiving device which may be a beeper or pager or other device which may be carried by the cardholder and/or be kept on and/or close to the cardholder's person so that the central processing computer may transmit signals and/or

data to the communication device so as to communication with the cardholder at any time and at any location.

The apparatus may also comprise a facsimile (fax) machine, a personal computer, a telephone, a telephone answering machine, an alternate telephone, an alternate telephone answering machine, a network computer and/or an alternate beeper or pager. The central processing computer may be linked with the above fax machine, personal computer, telephone, associated answering machine, alternate telephone and associated answering machine, network computer, and/or alternate beeper or pager via any suitable communication system. The telecommunications link or telephone line or link, which may or may not be a wireless link depending on the device and/or the circumstances, is utilized in order to link the central processing computer with each of the fax machine, the personal computer, the telephone, the associated answering machine, the alternate telephone, alternate telephone answering machine, the network computer and/or the alternate beeper or pager.

The apparatus and method of the present invention may be utilized in order to provide cardholder authorization, notification and/or security measures in financial transactions involving credit cards, charge cards, debit cards, and/or currency or "smart" cards and may be utilized in order to obtain cardholder authorization in a card-related transaction.

The apparatus and method of the present invention may commence operation when the card, which is to be utilized in a credit card, charge card, debit card, and/or currency or "smart" card, or number corresponding thereto, transaction, is offered at the point-of-sale or other appropriate location whereupon the attendant or point-of-sale terminal operator will activate the apparatus in any typical manner, such as by obtaining a phone line and entering card information into the point-of-sale terminal. Data entry may typically be performed by swiping the magnetic strip of the card through a card reader of the point-of-sale terminal. The information and/or data pertinent to the transaction and the card is then transmitted to the central processing computer.

The central processing computer will then process the information and/or data pertinent to the transaction and to the particular card account and may request, if needed, that the point-of-sale operator enter the transaction amount. The central processing computer will process the information and/or data pertinent to the transaction in conjunction with the card account information in order to determine if the card has been lost, stolen and/or cancelled and/or de-activated. Further, the central processing computer may perform a test in order to determine if the maximum credit, charge or debit account limit has been exceeded and/or if the card has been depleted of its currency value.

Once all of the information and/or data processing has been completed, the central processing computer will determine if the card has been lost, stolen, and/or cancelled and/or deactivated and/or if the credit, charge or debit account limit of the card has been reached and/or exceeded and/or if the currency value of the card has been depleted.

The central processing computer may also perform a test in order to determine if the predetermined maximum number of unauthorized transactions have occurred on the account. If any of the above listed conditions are found to exist (i.e. card is lost, stolen, cancelled and/or de-activated, or credit, charge or debit account limit has been reached or exceeded, currency value depleted, or unauthorized transaction limit reached or exceeded), the central processing computer may transmit a signal to the point-of-sale terminal indicating that the transaction is not approved and/or is not authorized. The point-of-sale terminal operator may then cancel the transaction. The point-of-sale terminal operator may then confiscate the card and/or alert the authorities.

If, however, the central processing computer should determine that the card is not lost, stolen, cancelled or de-activated, or that the credit, charge or debit account limit of the card has not been reached or exceeded, or that the of unauthorized transactions count has not reached a predefined limit, the central processing computer may transmit a signal and/or data to the communication device which is located with the cardholder. The central processing computer may then also transmit respective signals and/or data to any one or more of the cardholder's designated fax machine, personal computer, telephone, telephone answering machine, alternate telephone, alternate telephone answering machine, network computer, and/or alternate beeper or pager, either sequentially and/or simultaneously.

The information and/or data transmitted to the communication device includes information and/or data identifying the transaction and may include the name of the store or the service provider and the amount of the transaction. The information and/or data may also provide the time of the transaction, the location (i.e. city, town, village, state, country, etc.) of the transaction. The information and/or data may also include the phone number of the central processing office and/or computer servicing the account so that the cardholder may telephone same in order to authorize or cancel the transaction. The information and/or data may also be supplemented to include the type of goods and/or services involved in the transaction, if such information can be entered at the point-of-sale terminal.

The information and/or data which is transmitted from the central processing computer, and received at the communication device, may be displayed to the cardholder on a display device of the communication device. The information displayed on the display device may include the name of the store or the service provider, the amount of the transaction, the time of the transaction and the location of the transaction. The information and/or data may also be supplemented to include the type of goods and/or services involved in the transaction, if such information can be entered at the point-of-sale terminal.

The apparatus, or the central processing computer, may then wait for the cardholder to respond to the transmission. During this time, the cardholder may either utilize the reply or two-way pager feature on the communication device in order to either approve, or authorize, the transaction or to disapprove, or void the transaction. The apparatus may then determine if the cardholder has made a reply or response within a pre-defined time limit. The cardholder may also transmit a signal via an appropriate key or button suspending use of the card such as when he or she may first be apprised of the fact that the card has been lost or stolen. If the cardholder has replied or responded to the notice, the response may then be transmitted to, and received by, the central processing computer. The cardholder may also simply telephone the central processing office or processing center, servicing the card, so as to personally notify the office or center of his or her response to the central processing computer transmission regarding the transaction.

If the cardholder does not reply to the central processing computer within a pre-specified time, the central processing computer may transmit a signal and/or data to the point-of-sale terminal indicating that, with the exception of receiving the authorization of the cardholder, the transaction is otherwise approved. The central processing computer may also

simply transmit a signal indicating that the transaction is not authorized and, therefore, should be cancelled of voided. The point-of-sale terminal operator may then either proceed to complete the transaction, try to obtain additional information from the purchaser, or cancel the transaction.

The action taken by the point-of-sale terminal operator may be dictated by the specific agreement in effect between the sales or service establishment and the bank or financial institution administering the card accounts. Thereafter, the operation of the apparatus will cease. If the cardholder should reply or respond to the transaction notice at a later period, this information may then be utilized in order to approve, or to disapprove, and/or to dispute the transaction.

The central processing computer, after receiving the reply or response from the cardholder, may then identify the cardholder response. The apparatus, or the central processing computer, may then determine if the cardholder has replied or responded so as to authorize the transaction. If the cardholder's response is to cancel, to disapprove or not authorize, the transaction, the central processing computer may transmit a signal and/or data to the point-of-sale terminal which will notify and/or instruct the point-of-sale terminal operator that the transaction is not authorized and, therefore, should be cancelled or voided. The point-of-sale terminal operator may then cancel the transaction. The point-of-sale terminal operator may then confiscate the card and/or alert the authorities. Thereafter, the apparatus will cease operation.

If, however, the central processing computer identifies the cardholder reply or response as being one to authorize the transaction, the central processing computer may then transmit a signal and/or data to the point-of-sale terminal which may notify and/or instruct the point-of-sale terminal operator that the transaction is authorized and/or approved. The point-of-sale terminal operator may then complete the transaction. Thereafter, operation of the apparatus will cease.

In cases when the cardholder is the party to the transaction, he or she, having the communication device with, or on, his or her person, may authorize the transaction at the point-of-sale location or from his or her remote location. The cardholder may also program and/or set the communication device to automatically authorize or disapprove or disallow transactions.

In this regard, the communication device may be programmable so as to receive and/or to analyze the transaction information and/or data and reply or respond to same automatically and/or with preset or programmed replies and/or responses. The communication device may also be programmable so as to limit and/or restrict the amounts and/or types of transactions, and/or the goods and/or services which may be purchased with the card, the stores or service providers which may be authorized to accept the card, limits on the dollar amounts of transactions pertaining to each authorized vendor, seller and/or service provider, daily spending limits, and/or the geographical area or location to which authorized use may be limited, and/or authorized times for card usage (i.e. specific days, dates, time of day, time of month, year, etc.), and/or any other limitation and/or restriction regarding amount of the transaction, the parties involved, the geographical area limitations, and/or the times of allowed usage. In this regard, the cardholder may provide for temporary transaction and/or purchasing amounts.

The communication device may also be provided with a memory device for storing any number of transactions so that the cardholder may review his account activity and/or transactions which have occurred involving his or her card. In this manner, the cardholder may "scroll" through and/or in other ways review account activity at any time and for any time period and/or interval. The communication device may also be equipped to service more than one card. For example, a plurality of cards may be serviced with or by a single communication device.

The apparatus and method of the present invention provides for the real-time authorization, notification and/or security of financial transactions involving credit cards, charge cards, debit cards, and/or currency or "smart" cards, which enables a cardholder to monitor, in real-time, all activity involving his or her card(s) and the corresponding account numbers. The apparatus and method of the present invention also provides a means and a mechanism by which to inform a cardholder that his or her card(s) are lost, stolen and/or are or have been fraudulently used, and/or when his or her card number(s) are or have been fraudulently used, and provides an indication to the cardholder of where his or her card(s) are being or have been utilized in transactions. The cardholder may then report the card lost or stolen and/or cancel and/or de-activate the card.

The present invention also provides a means and a mechanism by which to monitor the number of transactions which are unauthorized by the cardholder and determine whether or not to authorize transactions and/or to cancel or to de-activate the card(s). In the above manner, the present invention provides an apparatus and a method to prevent and/or to drastically limit fraudulent and/or unauthorized use of credit cards, charge cards, debit cards, and/or currency or "smart" cards, and/or the account numbers corresponding thereto.

The present invention, in an alternate embodiment, may be utilized so as to provide authorization, notification and/or security in banking and related financial transactions involving checking accounts, savings accounts and/or automated teller machine (ATM) transactions and/or other transactions wherein an account holder can be notified of a transaction and/or attempted transaction. In such an alternate embodiment, the apparatus comprises a banking transaction terminal, which terminals are found in banks and financial institutions, and which may be a teller terminal, a processing computer terminal and/or an ATM terminal. The apparatus also comprises a central processing computer and a communication device. The banking transaction terminal transmits an authorization request which may include the data pertaining to the particular account which is accessed and/or involved in the transaction and the type and the amount of the transaction, over a communications medium, to the central processing computer for processing the transaction request and/or the authorization pertaining thereto.

The central processing computer may transmit signals and/or data pertaining to the transaction to the communication device. The apparatus may then operate and/or be utilized in a manner similar to, or analogous to, the apparatus utilized in conjunction with credit cards, charge cards, debit cards, and/or currency or "smart" cards, and/or the account numbers corresponding thereto, as described above.

In this manner, the apparatus and method of the present invention may provide for the real-time notification of banking and/or financial transactions involving various bank and/or financial accounts and enable an account owner to monitor, in real-time, all activity involving his or her bank and/or financial accounts. The apparatus and method of the present invention also provides a means and a mechanism by which to inform an account owner that his or her account is

overdrawn, has been charged against and/or that his or her ATM card(s) are lost, stolen, cancelled or de-activated and/or provides an indication to the account owner of when and/or where his or her accounts are being accessed in transactions and/or are being otherwise compromised. The account owner may then report the unauthorized activity, or the discovery of a lost or stolen ATM card, and/or cancel and/or de-activate the respective account(s) and/or ATM card(s).

In another alternate embodiment, the apparatus and method of the present invention may also be utilized so as to provide authorization, notification and/or security for, and in conjunction with, cellular and/or mobile telephones and/or communication systems wherein a cellular or mobile telephone owner and/or account holder can be notified of a transmission and/or an attempted transmission and/or telephone call made with his or her cellular or mobile telephone and/or with the telephone number and/or account information, which information may include, but not be limited to, transmission codes and/or associated signatures and/or data which corresponds to his or her cellular or mobile telephone.

The apparatus utilized in conjunction with a cellular telephone comprises a cellular telephone which serves as the transaction terminal, a central processing computer and a communication device. The cellular telephone transmits signals and/or data which are received by the central processing computer. The central processing computer may then transmit signals and/or data which are received by the communication device. The apparatus may then operate and/or be utilized in a manner similar to, or analogous to, the apparatus utilized in conjunction with credit cards, charge cards, debit cards, and/or currency or "smart" cards, savings accounts, checking accounts and/or automated teller machine accounts, and/or the account numbers corresponding thereto, as described above.

The apparatus and method of the present invention provides for the real-time notification of cellular or mobile telephone usage which enables a cellular telephone owner and/or account holder to monitor, in real-time, all activity involving his or her cellular telephone. The apparatus and method of the present invention also provides a means and a mechanism by which to inform a cellular telephone owner and/or account holder that his or her cellular telephone is lost, stolen and/or is being fraudulently used, and/or that the telephone number is being used in an unauthorized manner, and provides an indication to the cellular telephone owner and/or account holder of how, when and where his or her cellular telephone, or the account number which corresponds thereto, is being utilized in cellular communication transactions. The cellular telephone owner and/or account holder may then report the cellular telephone lost or stolen and/or cancel and/or de-activate the cellular telephone and/or the corresponding account and/or the account number.

The present invention also provides an apparatus and a method by which to monitor the number of cellular or mobile telephone transactions which are unauthorized by the cellular or mobile telephone owner and to determine whether or not a central processing computer should cancel or de-activate the cellular telephone and/or the account. In the above manner, the present invention provides an apparatus and a method for preventing and/or for drastically limiting fraudulent use and/or unauthorized use of cellular or mobile telephones and/or cellular or mobile telephone numbers. The present invention also provides an apparatus and a method for combating cellular telephone "cloning."

The apparatus and method of the present invention may also be utilized in connection with an on-line service and/or on, or over, the Internet and/or the World Wide Web, so as to provide for a means by which the authorized user or operator may utilize the apparatus in conjunction with a home and/or a personal computer and/or a commercial or industrial computer system (i.e., an internet server computer) and/or any other appropriate device, including a personal communication and/or computing device, in a network environment, and which may be utilized over any suitable and/or appropriate communications network or medium.

The communications system utilized in conjunction with the present invention may operate anywhere in the electromagnetic and/or the radio spectrum. Personal communication service (PCS) systems and devices, including stationary, portable and/or handheld devices, and digital signal communications devices and systems, may also be utilized. The communication system or medium should provide for the transmission and for the reception of a multitude of remote electrical, electronic, electromagnetic, and/or other suitable signals, over long distances and/or in a mobile and/or a wireless communications environment.

The apparatus and method of the present invention may be utilized in conjunction any appropriate communications device which may be utilized with any appropriate communications system and/or medium.

The present invention may also be equipped with, and be utilized with, hardware and software necessary for providing self-monitoring functions, automatic control and/or responses to occurrences, automatic notice of an occurrence and/or a situation, to an owner, user and/or authorized individual. In this regard, any and all of the embodiments described above may comprise a monitoring device, a triggering device and/or any other suitable device for detecting an occurrence and/or identifying a situation which may warrant providing notice to a card holder, account owner, cellular telephone owner and/or an authorized individual.

In this regard, the apparatus and method may provide a transmission of any appropriate signal from a transmitter and, if desired, from a voice synthesizer to the card holder, account owner and/or cellular telephone owner. The signal utilized could be in the form of a communication transmission, depending upon the communication medium utilized, a telephone call, a voice message, a beeper and/or a pager message, an electronic mail message, a fax transmission, and/or any other mode of communication which may be utilized with any of the apparatuses, devices and/or components described herein.

In this regard, the apparatus may be designed or programmed to telephone the cardholder, account owner and/or cellular telephone owner, and/or other authorized individual, at a primary phone number, at an alternate or forwarding phone number, and/or at a business phone number, send a beeper or pager message to the individual, and/or send a fax message, an electronic mail (e-mail) message, a voice mail message and/or an answering service message to, or for, the card holder, account owner and/or cellular telephone owner or authorized individual. In this manner, the apparatus may communicate with the desired individual by utilizing multiple notification and/or reporting avenues and/or devices so as to provide and to ensure that best efforts are to be made to communicate with the desired individual as soon as possible.

The apparatus and method of the present invention may also be programmable for programmed and/or automatic activation, self-activation, programmed and/or automatic operation and/or self-operation. The apparatus and method

of the present invention may provide for an immediate, as well as for a deferred, authorization, notification and/or security in any of the above-described financial transactions and/or wireless communication transactions.

The present invention may also be utilized in such a manner that a communication device may receive and/or transmit signals, data and/or information which pertains to multiple accounts and/or multiple types of accounts in order to provide authorization, notification and/or security for a plurality of any of the accounts described herein.

The present invention, in any of the embodiments described herein, may also be designed to be user-friendly. In this regard, the present invention may be menu-driven, and/or its operation may be menu-selected, from audio menus, visual menus, or both audio and visual menus.

Accordingly, it is an object of the present invention to provide an apparatus and a method for providing authorization, notification and/or security in financial transactions involving credit cards, charge cards, debit cards, and/or currency or "smart cards, savings accounts, checking accounts and/or automated teller machine accounts and for providing authorization, notification and/or security in wireless communications transactions involving cellular telephones and/or other cellular communications devices.

It is another object of the present invention to provide an apparatus and a method for providing authorization, notification and/or security in financial transactions involving credit cards, charge cards, debit cards, wherein the cardholder may authorize or disapprove of a transaction, in real time.

It is another object of the present invention to provide an apparatus and a method for providing authorization, notification and/or security in financial transactions involving savings account, checking accounts and/or automated teller machine accounts, wherein the account owner may authorize or disapprove of a transaction, in real time.

It is another object of the present invention to provide an apparatus and a method for providing authorization, notification and/or security in wireless communications transactions involving cellular telephones and/or other cellular communications devices, wherein the cellular telephone or cellular communication device owner may authorize or disapprove of a transaction, in real time.

It is another object of the present invention to provide an apparatus and a method for providing authorization, notification and/or security in financial transactions and/or in wireless communication transactions, which may be utilized on, over, or in conjunction with, an on-line service and/or the Internet, the World Wide Web, and/or any other suitable communication network or medium.

It is still another object of the present invention to provide an apparatus and a method for providing authorization, notification and/or security in financial transactions and/or in wireless communications transactions, which is programmable and/or which may provide for pre-programmed and/or pre-specified transaction authorization and/or transaction disapproval.

It is still another object of the present invention to provide an apparatus and a method for providing authorization, notification and/or security in financial transactions and/or in wireless communications transactions, which may be utilized over any suitable communications network or medium.

It is still another object of the present invention to provide an apparatus and a method for providing authorization, notification and/or security in financial transactions and/or in wireless communication transactions, wherein the respective cardholder, account owner or cellular telephone owner may increase or decrease the respective account credit limits, account activity, funds available, calling areas and/or usage limits at any time and/or from any location.

It is still another object of the present invention to provide an apparatus and a method for providing authorization, notification and/or security in financial transactions and/or in wireless communications transactions, which is programmable with respect to authorized times of usage (i.e. specific days, dates, time of day, time of month, year, etc.), and/or any other limitations regarding amount of transaction limitations, parties involved, and/or geographical area and/or location of allowed usage.

It is yet another object of the present invention to provide an apparatus and a method for providing authorization, notification and/or security in financial transactions, and/or in wireless communication transactions, for a plurality of accounts and types of accounts.

Other objects and advantages of the present invention will be apparent to those skilled in the art upon a review of the Description of the Preferred Embodiment taken in conjunction with the Drawings which follow.

BRIEF DESCRIPTION OF THE DRAWINGS

In the Drawings:

FIG. **1** illustrates a block diagram of the apparatus of the present invention which is utilized in conjunction with a credit card, a charge card, a debit card, and/or a currency or "smart" card authorization process;

FIG. **2** illustrates the various components of the apparatus of FIG. **1**;

FIG. **3** illustrates the operation of the apparatus of FIG. **1** in flow diagram form;

FIG. **4** illustrates a block diagram of an alternate embodiment of the apparatus of the present invention which is utilized in conjunction with a checking account, a savings account and/or an automated teller machine transaction;

FIG. **5** illustrates the various components of the apparatus of FIG. **4**;

FIG. **6** illustrates the operation of the apparatus of FIG. **4** in flow diagram form;

FIG. **7** illustrates a block diagram of an alternate embodiment of the apparatus of the present invention which is utilized in conjunction with a cellular and/or a mobile telephone;

FIG. **8** illustrates the various components of the apparatus of FIG. **7**;

FIG. **9** illustrates the operation of the apparatus of FIG. **7** in flow diagram form;

FIG. **10** illustrates yet another alternate embodiment of the present invention wherein the apparatus of the present invention is utilized on, or over, an on-line service, the INTERNET and/or the World Wide Web or other suitable communication network or medium; and

FIG. **11** illustrates yet another alternate embodiment of the present invention which is also utilized in conjunction with an on-line service and/or on, or over, the INTERNET and/or the World Wide Web or the suitable communication network or medium.

DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. **1** illustrates a block diagram of a preferred embodiment of the apparatus of the present invention, which is utilized in conjunction with a credit card, a charge card

and/or a debit card authorization process. The apparatus of FIG. **1** is denoted generally by the reference numeral **1**. With reference to FIG. **1**, the apparatus consists of a point-of-sale authorization terminal **2** which terminals are found in various establishments and utilized in conjunction with the sale of goods and/or services and in other financial transactions.

The point-of-sale authorization terminal **2** (hereinafter referred to as "point-of-sale terminal") may be any of the widely used and well known terminals or devices for providing point-of-sale authorization for transactions involving credit cards, charge cards, debit cards and/or other currency or "smart" cards. The point-of-sale terminal **2** may be utilized at the location of the goods and/or service provider, such as the retail store or office, and/or the point-of-sale terminal **2** may be located at the site of the goods or service provider or vendor, such as in cases when the sale is a telephone order, mail order and/or other type of transaction, including transactions made over the INTERNET and/or other on-line mediums.

Typically, the terminals and devices for providing point-of-sale authorization comprise and utilize a magnetic card reader and/or magnetic strip card reader, for reading data from the magnetic strip located on credit cards, charge cards, debit cards and/or the currency or "smart" cards. The point-of-sale terminal **2** transmits an authorization request which may include the data pertaining to the particular card utilized in the transaction and the amount of the transaction, over a communications medium, to a central processing computer for processing the credit, charge, debit and/or other transaction request and/or the authorization request pertaining thereto.

The point-of-sale terminal **2** also receives the authorization and/or authorization data and/or information from the central processing computer. A printed transaction receipt may also be provided at and/or obtained via the point-of-sale terminal **2**, or peripheral device associated therewith, for printing a transaction receipt which is usually or typically signed by the card holder in completing the transaction. The point-of-sale terminal **2** may be designed to read other data besides and/or in addition to magnetic card data. The point-of-sale terminal **2** may also comprise, or have associated therewith, a keypad for the manual entry of transaction information and/or data, such as the amount of the transaction. The point-of-sale terminal **2** may also be an integral component of a cash register or other transaction terminal or device which may provide for the automatic entry of transaction information and/or data.

The apparatus **1** also comprises a central processing computer **3** which services any predefined group of cardholders. For example, the central processing computer **3** may handle all MASTERCARD transactions for a given financial and/or credit institution. The central processing computer **3**, for example, may process credit cards, charge cards, debit cards, and/or currency or "smart" cards and/or combinations of same, such as, for example, VISA®, MASTERCARD®, and/or AMERICAN EXPRESS® cards and process and/or mange account information pertaining thereto. The central processing computer **3** may also process accounts for any of the various banks and/or financial institutions which issue and/or manage credit cards, charge cards, debit cards and/or currency or "smart" cards (hereinafter referred to as "card" or "cards") and/or process or manage these accounts.

The central processing computer **3** may be a mainframe computer, a mini-computer, a micro-computer, a server computer, such as those utilized in conjunction with on-line services and/or in a network environment, and/or any other suitable computer or computer system.

In the preferred embodiment, the point-of-sale terminal **2** is linked and/or connected to the central processing computer **3** via a telecommunications system, link and/or medium (hereinafter referred to as "communications system") such as, for example, a telephone network or line. It is important to note that the communications system which is utilized may be any communications system and may include telecommunication systems, satellite communications systems, radio communication systems, digital communications systems, digital satellite communications systems, personal communications services communication systems as well as any other appropriate communications system. The point-of-sale terminal **2** transmits signals and/or data to the central processing computer **3** as well as receives signals and/or data from the central processing computer **3**.

The apparatus **1** also comprises a cardholder communication device **4** which may receive signals and/or data from either or both of the point-of-sale terminal **2** and/or the central processing computer **3**. In the preferred embodiment of FIG. **1**, the communication device **4** receives signals and data from the central processing computer **3** with said signals being transmitted via a suitable communication system. In the preferred embodiment, the communications system utilized for transmitting signals and/or data to the communication device **4** is a wireless telephone line and the communication device **4** is a telephone signal receiving device such as a telephone beeper or pager. The communication device **4** or pager receives the wireless telephone signals and/or data from the central processing computer **3** during the authorization procedure as will be described in more detail below.

In the preferred embodiment, the communication device **4** is also equipped with a transmitter for transmitting signals and/or data to the central processing computer **3**. In this regard, the central processing computer **3** transmits signals and/or data to the communication device **4** as well as receives signals and/or data from the communication device **4**. The communication device **4** may also transmit signals and/or data directly to the point-of-sale terminal **2** and receive signals and/or data directly from the point-of-sale terminal **2**. In the preferred embodiment, the point-of-sale terminal **2** transmits signals and/or data to the central processing computer **3** and receives signals and/or data from the central processing computer **3**. Further, in the preferred embodiment, the communication device **4** receives signals and/or data from the central processing. computer **3** and transmits signals and/or data to the central processing computer **3**.

As noted above, the communication device **4** is a wireless device. In this regard, the communication device **4** or pager may be carried by the cardholder and/or be kept on and/or close to the cardholder's person so that the central processing computer **3** may transmit signals and/or data to the communication device **4** so as to communicate with the cardholder at any time. The communication device **4** may also comprise any one or more of a facsimile (fax) machine, a personal computer, a telephone, a telephone answering machine, an alternate telephone, an alternate telephone answering machine, a network computer, and/or an alternate beeper or pager. The central processing computer **3** may be linked with each of the above devices via any suitable communication system.

In the preferred embodiment, the apparatus **1** also comprises a facsimile (fax) machine **5**, a personal computer **6**, a

telephone **7**, a telephone answering machine **8**, an alternate telephone **9**, an alternate telephone answering machine **10**, a network computer **11**, an alternate beeper **12** and an alternate pager **13**. The central processing computer **3** may be linked with the above fax machine **5**, personal computer **6**, telephone **7**, associated answering machine **8**, alternate telephone **9**, alternate telephone answering machine **10**, network computer **11**, and/or alternate beeper **12** or pager **13**, via any suitable communication system. In the preferred embodiment, a telecommunications link or telephone network, line or link, which may or may not be a wireless link depending on the device and/or the circumstances, is utilized in order to link the central processing computer **3** with each of the fax machine **5**, the personal computer **6**, the telephone **7**, the associated answering machine **8**, the alternate telephone **9**, alternate telephone answering machine **10**, the network computer **11**, and/or the alternate beeper **12** and the alternate pager **13**.

FIG. **2** illustrates the various components of the apparatus **1** of FIG. **1**. In FIG. **2**, the point-of-sale terminal **2**, in the preferred embodiment, comprises a central processing unit or CPU **2**A, a magnetic card reader **2**e, which is connected to the CPU **2**A, associated random access memory **2**C (RAM) and read only memory **2**D (ROM) devices, which are also connected to the CPU **2**A, a user input device **2**E, which is typically a keypad or other suitable input device for inputting data into the terminal **2** and which is also connected to the CPU **2**A, and a display device **2**F for displaying information and/or data to a user.

The point-of-sale terminal **2** also comprises a transmitter **2**G for transmitting signals and/or data to the central processing computer **3**, and/or to the communication device **4** and/or to any other device associated with the cardholder and/or the apparatus, if desired. The transmitter **2**G is also connected to the CPU **2**A. The point-of-sale terminal **2** also comprises a receiver **2**H for receiving signals and/or data from the central processing computer **3**, and from the communication device **4** and/or any other associated device which may be utilized, if desired. The receiver **2**H is also connected to the CPU **2**A. The point-of-sale terminal **2** also comprises a printer **2**I or other appropriate output device for outputting data to the user. The printer **2**I is also connected to the CPU **2**A. In the preferred embodiment, the printer **2**I prints receipts corresponding to the transaction.

In FIG. **2**, the central processing computer **3**, in the preferred embodiment, comprises a central processing unit or CPU **3**A, associated random access memory **3**B (RAM) and read only memory **3**C (ROM) devices, which are connected to the CPU **3**A, a user input device **3**D, which is a keypad and/or any other suitable input device for inputting data into the central processing computer **3** and which is also connected to the CPU **3**A and a display device **3**E for displaying information and/or data to a user or operator.

The central processing computer **3** also comprises a transmitter(s) **3**F for transmitting signals and/or data to the point-of-sale terminal **2** and to the communication device **4** and/or to any one or more of the fax machine **5**, personal computer **6**, telephone **7**, telephone answering machine **8**, alternate telephone **9**, alternate telephone answering machine **10**, network computer **11** and/or alternate beeper **12** or alternate pager **13**. The transmitter(s) **3**F is also connected to the CPU **3**A. The central processing computer **3** also comprises a receiver(s) **3**G for receiving signals and/or data from the point-of-sale terminal **2** and from the communication device **4** and/or from any other suitable device which may be utilized in conjunction with the apparatus **1**. The receiver(s) **3**G is also connected to the CPU **3**A. The central processing computer **3**, in any and/or all of the embodiments described herein, may utilize a fax/modem and/or any other suitable computer communication device.

The central processing computer also comprises a database(s) **3**H which contains account information and data pertaining to the cardholders and/or to the cardholder accounts. The database **3**H contains information about the cardholder, the cardholders account number, credit and/or account limits, previous purchases, number of unauthorized purchases made to the account and other information and/or data necessary to manage and/or process an account transaction as described herein.

The database **3**H may also comprise data and/or information regarding specific limitations and/or restrictions which may be placed on a particular account, which may be pre-selected and/or programmed by the cardholder and which may include limitations and/or restrictions on the usage of the card. The limitations and/or restrictions may include the types of transactions which are allowed and/or authorized, the goods and/or services which may be purchased with the card, the vendors, stores and/or service provider which may be authorized to accept the card, limits on the dollar amounts of transactions pertaining to each authorized vendor, seller and/or service provider, daily spending limits, and/or the geographical area or location wherein authorized card use may be limited, and/or authorized times for card usage (i.e. specific days, dates, time of day, time of month, year, etc.), and/or any other limitation and/or restriction regarding amount of transaction, parties involved, geographical area, and/or times of allowed usage. The database **3**H is also connected to the CPU **3**A. The central processing computer **3** also comprises a printer **3**I or other appropriate output device for outputting information and/or data to a user or operator.

In FIG. **2**, the communication device **4**, in the preferred embodiment, comprises a central processing unit or CPU **4**A, associated random access memory **4**B (RAM) and read only memory **4**C (ROM) devices, which are connected to the CPU **4**A, a user input device **4**D, which is a keypad or a plurality of keys and/or switches for inputting data into the communication device **4** and which is also connected to the CPU **4**A, and a display device **4**E, for displaying information and/or data to the cardholder, and a database **4**F, which are also connected to the CPU **4**A. The communication device **4** also comprises a receiver **4**G for receiving signals and/or data from the central processing computer **3** and which is also connected to the CPU **4**A, a transmitter **4**H for transmitting signals and/or data to the central processing computer **3** and which is also connected to the CPU **4**A.

In the preferred embodiment, the communication device **4** which is utilized is a pager with a reply feature and/or device. A two-way pager and/or pager systems may also be utilized for implementing the respective component system (s) in the communication device **4**/central processing computer **3** combination and/or link.

The apparatus **1** of the present invention, in the preferred embodiment, may be utilized in order to facilitate cardholder authorization, notification and/or security measures in financial transactions involving credit cards, charge cards, debit cards, and/or currency or "smart" cards, in the manner described below and with reference to FIG. **3**. In this manner, the apparatus **1** of the present invention may be utilized to obtain cardholder authorization in a card-related transaction.

FIG. **3** illustrates the operation of the apparatus **1** in flow diagram form. With reference to FIG. **3**, the operation of the

apparatus **1** commences at step **30** when the card, which is to be utilized in a credit card, charge card, debit card, and/or currency or "smart" card transaction, is presented in the transaction. At step **31**, the sales or service attendant or point-of-sale terminal operator (hereinafter "point-of-sale terminal operator") will activate the apparatus **1** in any typical manner, such as by obtaining a phone line and entering card information into the point-of-sale terminal **2**. This data entry is typically performed by swiping the magnetic strip of the card through the card reader **2**B. The information and/or data pertinent to the transaction, and/or the card, is then transmitted, at step **32**, to the central processing computer **3**.

The central processing computer **3** will, at step **33**, process the information and/or data pertinent to the transaction and/or to the particular card account and may request, if needed, that the point-of-sale operator enter the transaction amount. The central processing computer **3** will then process the information and/or data pertinent to the transaction in conjunction with the card account information in order to determine if the card has been lost, stolen and/or cancelled and/or de-activated. Further, the central processing computer **3** will perform a test to determine if the card has reached and/or exceeded the maximum credit, charge or debit limit and/or if the card has been depleted of its currency value.

The central processing computer **3** may utilize any of the widely known data processing and/or software routines, which are known to those skilled in that art, in order to process transaction requests and/or authorizations involving the use of the respective card(s). Once the information and/or data processing has been completed at step **33**, the central processing computer **3**, at step **34**, will determine if the card has been lost, stolen, and/or cancelled and/or de-activated, or if the credit, charge or debit limit of the card has been reached and/or exceeded, or if the currency value of the card has been depleted.

The central processing computer **3** will, at step **34**, also perform a test in order to determine if the predetermined maximum number of unauthorized transactions have occurred on the account. The unauthorized transactions count refers to transactions which are not authorized by the cardholder as will be described herein. The authorized transaction count (UNAUTHCT) is a variable which is pre-set to zero (0) at the time the card account is issued. Each time an unauthorized transaction occurs, the unauthorized transaction count is incremented by one (1). Once the unauthorized transaction count reaches a pre-defined limit of, for example, three (3), the central processing computer **3** will cancel the transaction and de-activate the card. The central processing computer **3** will then notify the cardholder. In this manner, the apparatus **1** will enable the central processing computer **3** of an issuing and/or card servicing institution to cancel and/or de-activate the card, either permanently and/or temporarily, in cases when the cardholder may have failed to respond or to reply to transaction notices, which may be the case when the cardholder is not aware that the card has been lost or stolen, or when the card or account number has been duplicated, "cloned", or in other ways utilized without the cardholder's authorization, and/or when the cardholder is unable to respond or reply to the transaction notices for some other reason(s). This feature of the present invention serves to put a usage limit on the use of the card(s). The central processing computer **3**, at step **34**, will also perform a test(s) to determine if any additional limitations and/or restrictions have been met and/or satisfied.

If any of the above listed conditions exist (i.e. card is lost, stolen, cancelled and/or de-activated, or credit, charge or debit limit is reached and/or exceeded, currency value depleted, unauthorized transaction limit reached or exceeded limitations and/or restrictions violated, etc.), the central processing computer **3** will, at step **35**, transmit a signal to the point-of-sale terminal **2** indicating that the transaction is not approved and/or is not authorized. The point-of-sale terminal operator may then cancel the transaction, at step **36**. The point-of-sale terminal operator may then confiscate the card and/or alert the authorities. Upon the completion of step **36**, the apparatus will cease operation at step **55**.

If, at step **34**, the central processing computer **3** determines that the card is not lost, stolen, cancelled or de-activated, or that the credit, charge or debit limit of the card has not been reached or exceeded, or that the of unauthorized transactions count (UNAUTHCT) has not reached a pre-defined limit, or whether any other pre-defined, pre-selected and/or programmed limitation(s) and/or restriction(s) have been met, have been satisfied and/or have been reconciled, the central processing computer **3** will, at step **37**, transmit a signal and/or data to the communication device **4** which is located at the cardholder.

At step **37**, the central processing computer **3** will then also transmit respective signals and/or data to any one or more of the cardholder's designated fax machine **5**, personal computer **6**, telephone **7**, telephone answering machine **8**, alternate telephone **9**, alternate telephone answering machine **10**, network computer **11**, and/or alternate beeper **12** or alternate pager **13**.

The information and/or data which is transmitted to the communication device **4** includes information and/or data identifying the transaction and may include the name of the store or the service provider and the amount of the transaction. The information and/or data may also provide the time of the transaction, the location (i.e. city, town, village, state, country etc.) of the transaction. The information and/or data may also include the phone number of the central processing office and/or computer servicing the account so that the cardholder may telephone same in order to authorize or cancel the transaction. The information and/or data may also be supplemented to include the type of goods and/or services involved in the transaction, if such information can be entered at the point-of-sale terminal **2**.

At step **38**, the information and/or data which is transmitted from the central processing computer **3** and received at the communication device **4** is displayed to the cardholder on the display device **4**E of the communication device **4**. The information displayed on the display device **4**E includes the name of the store or the service provider, the amount of the transaction, the time of the transaction and the location of the transaction. The information and/or data may also be supplemented to include the type of goods and/or services involved in the transaction, if such information can be entered at the point-of-sale terminal **2**.

The apparatus **1** will then, at step **39**, wait for the cardholder to respond to the transmission. During this time, the cardholder may either utilize the reply or two-way pager feature on the communication device **4** in order to either approve or authorize the transaction or disapprove of or void the transaction. At step **39**, the central processing computer **3** will also receive the response if one is sent. At step **40**, the apparatus **1** will determine if the cardholder has made a reply or response within the pre-defined time limit which is chosen, in the preferred embodiment, to be one (1) minute. The cardholder may also transmit a signal via an appropriate key or button suspending use of the card such as when he or she may first be apprised of the fact that the card has been

lost or stolen. In instances when the communication device **4** does not have a reply or two-way pager feature, the cardholder may simply telephone the central processing office or a processing center for the card in order to personally appraise the center or office of his or her response to the central processing computer transmission regarding the transaction.

If the cardholder does not respond or reply to the central processing office within the pre-specified time, chosen, in the preferred embodiment, to be one (1) minute, the central office computer will, at step **41**, increment the unauthorized transaction count (UNAUTHCT) by one (1) and will, at step **42**, transmit a signal and/or data to the point-of-sale terminal **2** indicating that, with the exception of receiving the authorization of the cardholders the transaction is otherwise approved. The point-of-sale terminal operator may then, at step **43**, either proceed to consummate the transaction, try to obtain additional information from the purchaser, or cancel the transaction. The action taken by the point-of-sale terminal operator may be dictated by the specific agreement in effect between the sales and/or service provider establishment and the bank or financial institution administering the card account. Upon the completion of step **43**, the operation of the apparatus **1** will cease at step **44**. If the cardholder should reply or respond to the transaction notice at a later period, the response or reply information may then be utilized in order to approve of, or to disapprove and/or to dispute, the transaction.

If, at step **40**, the response or reply is determined to be timely, the central processing computer **3** will, at step **45**, process and identify the cardholder response. At step **46**, the central processing computer **3** will determine if the cardholder has replied or responded so as to authorize the transaction. If the cardholder's response is to cancel, disapprove or, or not to authorize, the transaction, the central processing computer **3** will, at step **47**, increment an unauthorized transaction count by **1**. At this juncture, it is important to note that the unauthorized count (UNAUTHCT) is set to zero at the time of the issuance of the card. After the unauthorized transaction count has been incremented, the central processing computer **3** will, at step **48**, transmit a signal and/or data to the point-of-sale terminal **2** which will notify and/or instruct the point-of-sale terminal operator that the transaction is not authorized and should, therefore, be cancelled or voided. The point-of-sale terminal operator may then cancel the transaction at step **49**. The point-of-sale terminal operator may then confiscate the card and/or alert the authorities. Upon the completion of step **49**, the apparatus will cease operation at step **50**.

If, at step **46**, the central processing computer **3** identifies the cardholder reply or response as being one to authorize the transaction, the central processing computer **3**, at step **51**, will reset the unauthorized transaction count (UNAUTHCT) to 0. An unauthorized transaction count (UNAUTHCT) of 0 will signify that any string of unauthorized transactions has now been broken by the cardholder, and further, that the present transaction is approved by the cardholder. The central processing computer **3** will then, at step **52**, transmit a signal and/or data to the point-of-sale terminal **2** which will notify and/or instruct the point-of-sale terminal operator that the transaction is authorized and/or approved.

The point-of-sale terminal operator may then complete the transaction, at step **53**. After the transaction has been completed at step **53**, the operation of the apparatus **1** will cease at step **54**.

In instances when the cardholder is a party to the transaction, he or she, having the communication device **4** on his or her person, may authorize the transaction at the point-of-sale location. If the transaction is a telephone and/or other remotely made transaction, the cardholder may authorize the transaction from his or her remote location. The cardholder may also program and/or set the communication device **4** to automatically authorize or disapprove or disallow transactions. In this regard, the communication device **4** may be programmable so as to receive and analyze the transaction information and/or data and reply and/or respond to same automatically and/or with preset and/or programmed relies and/or responses. The communication device **4** may also be programmable so as to limit the amounts of transactions. In this regard, the cardholder may provide for temporary transaction and/or purchasing amounts.

The communication device **4**, in the preferred embodiment, is provided with a memory device for storing any number of transactions so that the cardholder may review his or her card and/or account activity and/or transactions which have occurred involving his or her card. In this manner, the cardholder may "scroll" through and/or in other ways review card and/or account activity. The communication device **4** may also be equipped to service more than one card. For example, a cardholder's MASTERCARD®, VISA®, and/or AMERICAN EXPRESS® card or cards and the accounts corresponding thereto may all be serviced with or by a single communication device **4**.

The apparatus and method of the present invention provides for the real-time notification of financial transactions involving credit cards, charge cards, debit cards, and/or currency or "smart" cards, which enables a cardholder to monitor, in real-time, activity involving his or her card(s) and the corresponding accounts. The apparatus and method of the present invention also provides a means and a mechanism by which to inform a cardholder that his or her card(s) are lost or stolen, and/or that his or her card(s), and/or the account numbers corresponding thereto, are utilized without his or her authorization and also provides an indication to the cardholder of where his or her card(s) or corresponding account number(s) is being utilized in transactions. The cardholder may then report the card lost or stolen and/or cancel and/or de-activate the card and/or the account.

The present invention also provides a means and a mechanism by which to monitor the number of transactions which are unauthorized by the cardholder and to determine whether or not to authorize transactions and/or cancel or de-activate the card(s) and/or the account. In the above manner, the apparatus and method of the present invention provides an apparatus and a method for preventing and/or for drastically limiting fraudulent and/or unauthorized use of credit cards, charge cards, debit cards, and/or currency or "smart" cards and/or the account numbers corresponding thereto.

The present invention, in an alternate embodiment, may be utilized so as to provide authorization, notification and/or security in banking and related financial transactions involving checking accounts, savings accounts and/or automated teller machine (ATM) accounts and transactions and other transactions wherein an account owner may be notified of a transaction and/or an attempted transaction.

FIG. **4** illustrates a block diagram of an alternate embodiment of the apparatus of the present invention which is utilized in conjunction with a checking account, savings account and/or ATM account and/or transaction (hereinafter referred to as a "banking transaction") and/or the authori-

zation process involved therewith. The apparatus of FIG. **4** is denoted generally by the reference numeral **100**. In FIG. **4**, the apparatus **100** consists of a banking transaction terminal which terminals are found in banks and financial establishments. In the preferred embodiment, the banking transaction terminal **102** is a teller terminal, a processing computer terminal and/or an ATM terminal. Any other terminal or similar device may also be utilized as the banking transaction terminal **102** depending upon the application and/or the transaction.

The banking transaction terminal **102** (hereinafter referred to as "banking terminal") may be any of the widely used and well known terminals or devices for providing banking transactions over-the-counter, ATM transactions and/or in any other type of financial transactions, including clearing transactions, check clearing and/or account charging and/or charge-back transactions, which transactions banks and financial institutions perform and/or engage in.

Typically, the banking terminals and/or devices comprise a computer terminal having an input device such as a keyboard and/or various reader and/or scanning device for reading and/or scanning, respectively, information and/or data necessary in order to perform the transaction. The banking terminal transmits an authorization request which may include the data pertaining to the particular account which is accessed and/or involved in the transaction and the type and the amount of the transaction, over a communications medium, to a central processing computer for processing the transaction, the transaction request and/or the authorization request pertaining thereto. The banking terminal may transmit the transaction authorization request and/or notice to a central processing computer via a central bank computer (not shown) which may be a central computer at the particular bank or financial institution. The central processing computer may also be a central computer system which is not located at the bank or financial institution, but rather, services the particular bank or financial institution or a group of banks or financial institutions.

The banking terminal **102** also receives the transaction and/or authorization data and/or information from the central processing computer. If a central bank computer is utilized, the data transmitted from the central processing computer would be transmitted to the banking terminal **102** via the central bank computer. A printed transaction receipt may also be provided at and/or obtained via the banking terminal **102**, or peripheral device associated therewith, for printing a transaction receipt which is usually provided to the account holder at the time and/or location of the transaction.

The banking terminal **102** may also comprise, and/or have associated therewith, a keypad for the manual entry of transaction information and/or data, such as the amount of the transaction, account number, etc. The banking terminal **102** may also be an integral component of a teller and/or cashier work station and/or other transaction terminals and/or devices, including those which may provide for the automatic entry of transaction information and/or data.

The apparatus **100** also comprises a central processing computer **103** which services any bank and/or financial institution and/or any pre-defined group of banks and/or financial institutions and/or any number of accounts associated therewith. For example, the central processing computer **103** may handle all checking accounts, savings accounts and/or other accounts for a given bank or banks. The central processing computer **103**, for example, may process and maintain records of deposits, withdrawals, checks cashed, drafts, ATM deposits, ATM withdrawals, charges made against an account, credits made to an account, etc., and/or any combinations of same. The central processing computer **103** may process accounts for any of the various banks and/or financial institutions.

In the preferred embodiment, the banking terminal **102** is linked and/or connected to the central processing computer **103** via a telecommunications system, link and/or medium (hereinafter referred to as "communications system") such as, for example, a telephone network or line. As noted above, the banking terminal **102** may or may not be linked to the central processing computer **103** via a central bank computer. It is important to note that the communications system which is utilized may be any communications system and may include telecommunication systems, satellite communications systems, radio communication systems, digital communications systems, digital satellite communications systems, personal communications services communication systems as well as any other appropriate communications system. The banking terminal **102** transmits signals and/or data to the central processing computer **103** as well as receives signals and/or data from the central processing computer **103**.

The central processing computer **103** may be a mainframe computer, a mini-computer, a micro-computer, a server computer, such as those utilized in conjunction with on-line services and/or in a network environment, and/or any other suitable computer or computer system.

The apparatus **100** also comprises an account owner communication device **104** which may receive signals and/or data from either or both of the banking transaction terminal **102** and/or the central processing computer **103**. In the preferred embodiment of FIG. **4**, the communication device **104** receives signals and/or data from the central processing computer **103** with said signals being transmitted via a suitable communication system. In the preferred embodiment, the communications system utilized for transmitting signals and/or data to the communication device **104** is a wireless telephone line and the communication device **104** is a wireless telephone signal receiving device such as a telephone beeper or pager. The communication device **104**, which may be a pager, receives the wireless telephone signals and/or data from the central processing computer **103** during the authorization procedure as will be described in more detail below.

In the preferred embodiment, the communication device **104** is also equipped with a transmitter for transmitting signals and/or data to the central processing computer **103**. In this regard, the central processing computer **103** transmits signals and/or data to the communication device **104** as well as receives signals and/or data from the communication device **104**. The communication device **104** may also transmit signals and/or data directly to the banking terminal **102** and receive signals and/or data directly from the banking terminal **102**. In the preferred embodiment, the banking terminal **102** transmits signals and/or data to the central processing computer **103** and receives signals and/or data from the central processing computer **103**. Further, in the preferred embodiment, the communication device **104** receives signals and/or data from the central processing computer **3** and transmits signals and/or data to the central processing computer **103**.

As noted above, the communication device **104** is a wireless device. In this regard, the communication device **104** or pager may be carried by the account owner and/or be kept on and/or close to the account owner's person so that

the central processing computer **103** may transmit signals and/or data to the communication device **104** so as to communication with the account owner at any time.

In the preferred embodiment, the apparatus **100** also comprises a facsimile (fax) machine **105**, a personal computer **106**, a telephone **107**, a telephone answering machine **108**, an alternate telephone **109**, an alternate telephone answering machine **110**, a network computer **111**, and/or an alternate beeper **112** or alternate pager **113**. The central processing computer **103** may be linked with the above fax machine **105**, personal computer **106**, telephone **107**, associated answering machine **108**, alternate telephone **109**, alternate telephone answering machine **110**, network computer **111** alternate beeper **112** and alternate pager **113**, via any suitable communication system. In the preferred embodiment, a telecommunications link or telephone line or link, which may or may not be a wireless link, depending on the device and/or the circumstances, is utilized in order to link the central processing computer **103** with each of the fax machine **105**, the personal computer **106**, the telephone **107**, the associated answering machine **108**, the alternate telephone **109**, the alternate telephone answering machine **110**, the network computer **111**, the alternate beeper **112** and the alternate pager **113**.

FIG. **5** illustrates the various components of the apparatus **100** of FIG. **4** In FIG. **5**, the banking terminal **102**, in the preferred embodiment, comprises a central processing unit or CPU **102**A, a scanner or reader **102**B, which is connected to the CPU **102**A, associated random access memory **102**C (RAM) and read only memory **102**D (ROM) devices, which are also connected to the CPU **102**A, a user input device **102**E, which is typically a keypad or other suitable input device for inputting data into the banking terminal **102** and which is also connected to the CPU **102**A, and a display device **102**F for displaying information and/or data to a user or operator, which display device **102**F is also connected to the CPU **102**A.

The banking terminal **102** also comprises a transmitter **102**G for transmitting signals and/or data to the central processing computer **103**, and/or to the communication device **104** and/or to any other device associated with the account owner and/or the apparatus, if desired. The transmitter **102**G is also connected to the CPU **102**A. The banking terminal **102** also comprises a receiver **102**H for receiving signals and/or data from the central processing computer **103**, and from the communication device **104** and/or from any other associated device which may be utilized, if desired. The receiver **102**H is also connected to the CPU **102**A. The banking terminal **102** also comprises a printer **102**I or other appropriate output device for outputting data to the operator. The printer **102**I is also connected to the CPU **102**A. In the preferred embodiment, the printer **102**I prints receipts corresponding to the transaction.

In FIG. **5**, the central processing computer **103**, in the preferred embodiment, comprises a central processing unit or CPU **103**A, associated random access memory **103**B (RAM) and read only memory **103**C (ROM) devices, which are connected to the CPU **103**A, a user input device **103**D, which is a keypad or any other suitable input device, for inputting data into the central processing computer **103** and which is also connected to the CPU **103**A, and a display device **103**E for displaying information and/or data to a user or operator.

The central processing computer **103** also comprises a transmitter(s) **103**F for transmitting signals and/or data to the banking terminal **102** and to the communication device **104** and/or to any one or more of the fax machine **105**, the personal computer **106**, the telephone **107**, the telephone answering machine **108**, the alternate telephone **109**, the alternate telephone answering machine **110**, the network computer **111**, the alternate beeper **112**, and/or the alternate pager **113**. The transmitter(s) **103**F is also connected to the CPU **103**A. The central processing computer **103** also comprises a receiver(s) **103**G for receiving signals and/or data from the banking transaction terminal **102** and from the communication device **104** and/or from any other suitable device which may be utilized in conjunction with the apparatus **100**. The receiver(s) **103**G is also connected to the CPU **103**A.

The central processing computer **103** also comprises a database(s) **103**H which contains account information and data pertaining to the account owner's account(s). The database **103**H contains information about the account owner, the account number, etc., and any other information and/or data necessary to the manage and/or process an account and/or account transaction as described herein. The database **103**H is also connected to the CPU **103**A. The central processing computer **103** also comprises a printer **103**I or other appropriate output device for outputting information and/or data to a user or operator, which printer **103**I or other output device is also connected to the CPU **103**A.

In FIG. **5**, the communication device **104**, in the preferred embodiment, comprises a central processing unit or CPU **104**A, associated random access memory **104**B (RAM) and read only memory **104**C (ROM) devices, which are also connected to the CPU **104**A, a user input device **104**D, which is a keypad or a plurality of keys and/or switches for inputting data into the communication device **104** and which is also connected to the CPU **104**A, and a display device **104**E, for displaying information and/or data to the account owner, and a database **104**F. This display device **104**E and the database **104**F are also connected to the CPU **104**A. The communication device **104** also comprises a receiver **104**G for receiving signals and/or data from the central processing computer **103** and which is also connected to the CPU **104**A, and a transmitter **104**H for transmitting signals and/or data to the central processing computer **103** and which is also connected to the CPU **104**A.

In the preferred embodiment, the communication device **104**, which is utilized, is a pager with a reply feature and/or device. A two-way pager and/or pager system(s) may also be utilized for implementing the respective component systems in the communication device **104**/central processing computer **103** combination and/or link.

The apparatus **100** of the present invention, in the preferred embodiment, may be utilized in order to facilitate account owner authorization, notification and/or security, in financial transactions involving checking accounts, savings accounts and ATM accounts, and/or any transactions involving same in the manner described below and with reference to FIG. **6**. In this manner, the apparatus and method of the present invention may be utilized to obtain account owner authorization in a banking and/or financial transaction.

FIG. **6** illustrates the operation of the apparatus **100** in flow diagram form. With reference to FIG. **6**, the operation of the apparatus **100** commences at step **130** when the financial transaction and/or instrument or ATM card is presented to the bank or financial institution employee, representative and/or placed in a card reader, respectively. At step **131**, the employee or representative of the bank or financial institution will activate the apparatus, via the banking transaction terminal **102**, in any typical manner,

such as by entering account and/or card information, into the banking transaction terminal **102**. This data entry is typically performed by manual data entry and/or via a card reader, depending upon the transaction. For example, if a person offers a check for cashing and provides a savings account or a checking account number, as the means by which to endorse the check, the employee or representative will enter the savings account or checking account number into the banking terminal **102** for processing. Similarly, if one desires to withdraw money from an ATM account, the card reader will read and enter the account number and/or information for processing. The information and/or data pertinent to the transaction and the card is then transmitted, at step **132**, to the central processing computer **103**.

The central processing computer **103** will then, at step **133**, process the information and/or data pertinent to the transaction and to the particular account. The central processing computer **103** may utilize any of the widely known data processing and/or software routines, which are known to those skilled in that art, in order to process transaction requests and/or authorizations involving the use of the respective account(s) and/or related card(s).

The central processing computer **103** will process the information and/or data pertinent to the transaction in conjunction with the account information in order to determine the status of the account (i.e. whether any holds have been placed on the account, such as those prohibiting withdrawals). Further, the central processing computer **103** will then perform a test, at step **134**, in order to determine if the transaction amount has reached and/or exceeded the amount available in the account and/or if the ATM card has been reported lost, stolen, cancelled and/or de-activated, and/or determine whether any other pre-defined, pre-selected and/or programmed limitation(s) and/or restrictions) have been met, satisfied and/or reconciled. The central processing computer **103** will also perform a test in order to determine if the predetermined maximum number count of unauthorized transactions, pre-defined in the preferred embodiment to be one (1), has occurred on the account.

The unauthorized transaction count refers to a count of the transactions which are not authorized by the account owner as will be described herein. The authorized transaction count (UNAUTHCT) is a variable which is pre-set to zero (0) at the time the account is opened. Each time an unauthorized transaction occurs, the unauthorized transaction count is incremented by one. Once the unauthorized transaction count reaches a pre-defined limit of, for example, one (1), although it may be pre-defined to be zero (0), the central processing computer **103** will cancel the transaction and de-activate the account and/or the ATM card. The central processing computer **103** will then notify the account owner. In this manner, the apparatus **100** will enable the central processing computer **103** of a banking and/or financial institution to cancel and/or de-activate the account and/or the ATM card, either permanently or temporarily, in cases when the account owner may have failed to respond or to reply to transaction notices, which may be the case when the account owner is not aware that the account has been charged, overdrawn, and/or that the ATM card has been lost or stolen, cancelled or de-activated, duplicated, "cloned", or in other ways utilized without the account owner's knowledge or authorization, or when the account owner is unable to respond or reply to the transaction notices for some other reason(s). This feature of the present invention serves to place a transaction stop limit on the account and/or on the use of the ATM card.

If any of the above listed conditions exist (i.e. account overdrawn and/or ATM card is lost, stolen, cancelled and/or de-activated), the central processing computer **103** will, at step **135**, transmit a signal to the banking transaction terminal **102** indicating that the transaction is not approved and/or is not authorized. The banking terminal operator, or employee, or representative, may then cancel the transaction at step **136**. The employee or representative may then alert the authorities and/or confiscate the ATM card. In the case when an ATM machine is utilized as the banking terminal **102**, the ATM machine may confiscate the ATM card automatically. Upon the completion of step **136**, the apparatus will cease operation at step **137**.

If, at step **134**, the central processing computer **103** determines that the account is not overdrawn or that the ATM card is not lost, stolen, cancelled or de-activated, or that the of unauthorized transactions count (UNAUTHCT) has not reached a predefined limit, and/or that pre-defined or pre-specified limitations and/or restrictions have been met, the central processing computer **103** will, at step **138**, transmit a signal and/or data to the communication device **104** which is located at the account owner.

At step **138**, the central processing computer **103** will then also transmit respective signals and/or data to any one or more of the cardholder's designated fax machine **105**, personal computer **106**, telephone **107**, telephone answering machine **108**, alternate telephone **109**, alternate telephone answering machine **110**, network computer **111**, and/or alternate beeper **112** or alternate pager **113**.

The information and/or data transmitted to the communication device **104** includes information and data identifying the transaction and may include the name of the bank or financial institution where the transaction is taking place, the account number and/or description, the amount of the transaction, the time of the transaction and the location (i.e. city, town, village, state, country etc.) of the transaction. The information and/or data may also include the phone number of the central processing office and/or computer servicing, and/or the banking and/or financial institution handling, the account so that the account owner may telephone same in order to authorize or cancel the transaction. The information and/or data may also be supplemented to include a description of the person seeking to make the transaction and the type of transaction sought (i.e. cash withdrawal, cashing of check, etc.).

At step **139**, the information and/or data which is transmitted from the central processing computer **103**, and received at the communication device **104**, is displayed to the account owner on the display device **104**E of the communication device **104**. The information displayed on the display device **104** includes the name of the banking and/or financial institution, the amount of the transaction, the time of the transaction and the location of the transaction. The information and/or data may also include the type of transaction and a description of the person seeking to make the transaction, etc.

The apparatus **100**, at step **140**, will then wait for the account owner to respond to the transmission. During this time, the account owner may either utilize the reply or two-way pager feature on the communication device **104** in order to either approve or authorize the transaction or disapprove of, or void, the transaction. At step **140**, the apparatus **100** will receive the reply or response from the account owner. At step **141**, the central processing computer **103** will determine if the account owner has made a reply or response within the pre-defined time limit which is chosen,

in the preferred embodiment, to be one (1) minute. The account owner may also transmit a signal via an appropriate key or button suspending use of the account or ATM card, such as when he or she may first be apprised of the fact that the account is being unlawfully accessed, or the use thereof is unauthorized, or that the ATM card has been lost or stolen.

In instances when the communication device **104** does not have a reply or two-way pager feature, the account owner may simply telephone the central processing office or processing center and/or the banking or financial institution so as to personally reply or respond to the authorization request.

If, at step **141**, it is determined that the account owner's reply or response was not made within the pre-specified time, chosen in the preferred embodiment to be one (1) minute, the central processing computer **103** will, at step **142**, increment the unauthorized transaction count (UNAUTHCT) by one (1) and will, at step **143**, transmit a signal and/or data to the banking transaction terminal **102** indicating that the transaction is not authorized by the account owner. The banking terminal operator may then, at step **144**, either cancel the transaction, proceed to consummate the transaction, and/or attempt to obtain additional information or identification from the customer and/or obtain an alternate account number from which to draw against.

The action taken by the banking transaction terminal operator may be dictated by the specific agreement in effect between the account owner and the bank or financial institution administering the accounts. Upon the completion of step **144**, the operation of the apparatus will cease at step **145**. If the account owner should reply or respond to the transaction notice at a later period, this information may then be utilized to approve of or to disapprove and/or to dispute the transaction.

If, at step **141**, it is determined that the reply or response was timely, the central processing computer **103** will, at step **146**, process and identify the account owner response. At step **147**, the central processing computer **103** will determine if the account owner has authorized the transaction. If the account owner's response is to cancel, to disapprove, or to not authorize, the transaction, the central processing computer **103** will, at step **148**, increment the unauthorized transaction count (UNAUTHCT) by 1. At this juncture, it is important to note that the unauthorized count (UNAUTHCT) is set to zero at the time of the opening of the account.

After the unauthorized transaction count has been incremented, the central processing computer **103** will, at step **149**, transmit a signal and/or data to the banking terminal **102** which will notify and/or instruct the banking terminal operator that the transaction is not authorized and should, therefore, be cancelled or voided. The banking terminal operator may then cancel the transaction at step **150**. The banking transaction terminal operator or the ATM machine may then confiscate the ATM card and/or alert the authorities. Upon the completion of step **150**, the apparatus will cease operation at step **151**.

If, at step **147**, the central processing computer **103** identifies the account owner's reply or response as being one to authorize the transaction, the central processing computer **103** will, at step **151**, reset the unauthorized transaction count (UNAUTHCT) to zero (0). The central processing computer **103** will then, at step **153**, transmit a signal and/or data to the banking terminal **102** which will notify and/or instruct the banking terminal operator, and/or the ATM machine, that the transaction is authorized and/or approved. The banking terminal operator, and/or the ATM machine, may then complete the transaction, at step **154**. After the transaction has been completed at step **154**, the operation of the apparatus **100** will cease at step **155**.

In instances when the account owner is a party to the transaction, which should typically be the case in banking and/or financial transactions, the account owner, having the communication device **104** on his or her person, may authorize the transaction at the point of the transaction. If the transaction is an overnight or other remotely made transaction, such as in clearing and/or account settling transactions, the account owner may authorize the transaction from his or her remote location.

The account owner may also program and/or set the communication device **104** so as to automatically authorize or disapprove or disallow transactions. In this regard, the communication device **104** may be programmable so as to receive and analyze the transaction information and/or data and reply or respond to same automatically and/or with preset or programmed replies and/or responses. The communication device **104** may also be programmable so as to limit the amounts of transactions. In this regard, the account owner may provide for temporary transaction types and/or amounts.

The communication device **104**, in the preferred embodiment, is provided with a memory device for storing any number of transactions so that the account owner may review his or her account activity and/or transactions which have occurred involving his or her accounts and/or ATM card. In this manner, the account owner may "scroll" through and/or in other ways review account activity. The communication device **104** may also be equipped to service more than one bank and/or financial account and/or ATM card. For example, any number and/or types of accounts may be serviced with or by a single communication device **104**.

The apparatus and method of the present invention provides for the real-time notification of banking and/or financial transactions involving various bank and/or financial accounts and enables an account owner to monitor, in real-time, activity involving his or her bank and/or financial accounts and/or ATM card(s).

The apparatus and method of the present invention also provides a means and a mechanism by which to inform an account owner that his or her account is overdrawn, has been charged against and/or that his or her ATM card(s) are lost, stolen, cancelled or de-activated and/or provides an indication to the account owner of when and/or where his or her accounts are being accessed in transactions. The account owner may then report the unauthorized activity, and/or the discovery of a lost or stolen ATM card, and/or cancel and/or de-activate the respective account(s) and/or ATM card(s).

The present invention, in an alternate embodiment, may also be utilized so as to provide authorization, notification and/or security for, and in conjunction with, cellular and/or mobile telephone and/or communication systems wherein a cellular or mobile telephone owner and/or account owner may be notified of a transmission and/or an attempted transmission and/or telephone call made with his or her cellular or mobile telephone and/or with the telephone number and or transmission codes and/or associated signatures and/or data which corresponds to his or her cellular or mobile telephone.

FIG. **7** illustrates a block diagram of an alternate embodiment of the apparatus of the present invention which is

utilized in conjunction with a cellular or mobile telephone (hereinafter referred to as "cellular telephone") and/or corresponding cellular telephone account number and/or information related thereto. The apparatus of FIG. **7** is denoted generally by the reference numeral **200**. In FIG. **7**, the apparatus **200** consists of a cellular telephone **202** which may be any typical cellular and/or mobile telephone. Any other cellular and/or mobile communication device may also be utilized.

The cellular telephone **202** may be any of the widely used and well known cellular telephones and/or mobile communication device(s). In the embodiment of FIG. **7**, the cellular telephone **202** serves as the transaction terminal which is described above in conjunction with the previous embodiments. As is the case with cellular telephones, the cellular telephone may transmit the authorization request and/or notice to a central processing computer. The cellular telephone **202** may, but need not, receive authorization data and/or information from the central processing computer. The cellular telephone **202** may also comprise, or have associated therewith, a keypad for the manual entry of transaction information and/or data, such as the telephone number and various command codes utilized in making or placing a telephone call.

The apparatus **200** also comprises a central processing computer **203** which services any predefined group of cellular telephones or cellular communication devices. For example, the central processing computer **203** may handle all cellular telephone accounts for a given telecommunications company and/or area. The central processing computer **203**, for example, may process and maintain records of cellular telephone calls, including billing information, for any number of cellular telephones, cellular telephone accounts, and/or cellular telephone owners which or who are serviced by a particular communications company or central processing office or computer.

The central processing computer **203** may be a mainframe computer, a mini-computer, a micro-computer, a server computer, such as those utilized in conjunction with on-line services and/or in a network environment, and/or any other suitable computer or computer system.

The central processing computer **203** may also process accounts for any of the various cellular and/or mobile communications accounts and/or devices. In the preferred embodiment, the cellular telephone **202** is linked and/or connected to the central processing computer **203** via a telecommunications system, link and/or medium (hereinafter referred to as "communications system") such as, for example, a telephone network or line. It is important to note that the communications system which is utilized may be any communications system and may include telecommunication systems, satellite communications systems, radio communication systems, digital communications systems, digital satellite communications systems, personal communications services communication systems as well as any other appropriate communications system. The cellular telephone **202** transmits signals and/or data to the central processing computer **203** as well as receives signals and/or data from the central processing computer **203**.

The apparatus **200** also comprises a cellular telephone owner communication device **204** which may receive signals and/or data from either or both of the cellular telephone **202** and/or the central processing computer **203**. In the embodiment of FIG. **7**, the communication device **204** receives signals and data from the central processing computer **203** with said signals being transmitted via a suitable communication system. In the embodiment of FIG. **7**, the communications system utilized for transmitting signals and/or data to the communication device **204** is a wireless telephone network or line and the communication device **204** is a wireless telephone signal receiving device such as a telephone beeper or pager. The communication device **204** or pager receives the wireless telephone signals and/or data from the central processing computer **203** during the authorization procedure as will be described in more detail below.

In the preferred embodiment, the communication device **204** is also equipped with a transmitter for transmitting signals and/or data to the central processing computer **203**. In this regard, the central processing computer **203** transmits signals and/or data to the communication device **204** as well as receives signals and/or data from the communication device **204**. The communication device **204** may also transmit signals and/or data directly to the cellular telephone **202** and receive signals and/or data directly from the cellular telephone **202**.

In the preferred embodiment, signals and/or data which are transmitted by the cellular telephone **202** are received at the central processing computer **203**. The cellular telephone **202** also receives signals and/or data from the central processing computer **203**. Further, in the alternate embodiment of FIG. **7**, the communication device **204** receives signals and/or data from the central processing computer **203** and transmits signals and/or data to the central processing computer **203**.

As noted above, the communication device **204** is a wireless device. In this regard, the communication device **204** or pager may be carried by the cellular telephone owner and/or be kept on and/or close to the cellular telephone owner's person so that the central processing computer **203** may transmit signals and/or data to the communication device **204** so as to communicate with the cellular telephone owner at any time.

In the alternate embodiment of FIG. **7**, the apparatus **200** also comprises a facsimile (fax) machine **205**, a personal computer **201**, a telephone **202**, a telephone answering machine **208**, an alternate telephone **209**, an alternate telephone answering machine **210**, a network computer **211**, an alternate beeper **212**, and an alternate pager **213**.

The central processing computer **203** may be linked with the above fax machine **205**, personal computer **206**, telephone **207** and associated answering machine **208**, alternate telephone **209** and associated answering machine **210**, network computer **211**, alternate beeper **212** and/or alternate pager **213**, via any suitable communication system. In the preferred embodiment, a telecommunications link or telephone line or link, which may or may not be a wireless link depending on the device and/or the circumstances, is utilized in order to link the central processing computer **203** with each of the fax machine **205**, the personal computer **206**, the telephone **207** and associated answering machine **208**, the alternate telephone **209** and associated answering machine **210**, the network computer **211**, the alternate beeper **212**, and/or the alternate pager **213**.

FIG. **8** illustrates the various components of the apparatus **200** of FIG. **7**. In FIG. **8**, the cellular telephone **202**, in the preferred embodiment, comprises a central processing unit or CPU **202**A, associated random access memory **202**B (RAM) and read only memory **202**C (ROM) devices, which are also connected to the CPU **202**A, a user input device **202**D, which is a typically a keypad or other suitable input device for inputting data into the cellular telephone **202** and which is also connected to the CPU **202**A, and a display device **202**E for displaying information and/or data to a user or operator.

The cellular telephone **202** also comprises a transmitter **202**F for transmitting signals during normal telephone operation and/or for transmitting signals and/or data to the central processing computer **203**, and/or to the communication device **204** and/or to any other device associated with the account owner or apparatus **200** if desired. The transmitter **202**F is also connected to the CPU **202**A. The cellular telephone **202** also comprises a receiver **202**G for receiving signals during normal telephone operation and/or for receiving signals and/or data from the central processing computer **203**, and from the communication device **204** and/or from any other associated device which may be utilized, if desired.

The receiver **202**G is also connected to the CPU **202**A. The cellular telephone **202** may also comprise a printer **202**H or other appropriate output device for outputting data to the user. The printer **202**H, if utilized, is also connected to the CPU **202**A. In the preferred embodiment, the printer **202**H prints receipts corresponding to the transaction and/or information transmitted during the telephone call or transaction.

In FIG. **8**, the central processing computer **203**, in the preferred embodiment, comprises a central processing unit or CPU **203**A, associated random access memory **203**B (RAM) and read only memory **203**C (ROM) devices, which are connected to the CPU **203**A, a user input device **203**D, which is a keypad or any other suitable input device for inputting data into the central processing computer **203** and which is also connected to the CPU **203**A and a display device **203**E for displaying information and/or data to a user or operator.

The central processing computer **203** also comprises a transmitter(s) **203**F for transmitting signals and/or data to the cellular telephone **202** and to the communication device **204** and/or to any other device which may be utilized and/or to any one or more of the fax machine **205**, personal computer **206**, telephone **207** and associated answering machine **208**, alternate telephone **209** and associated answering machine **210**, network computer **211**, alternate beeper **212**, and/or alternate pager **213**. The transmitter(s) **203**F is also connected to the CPU **203**A. The central processing computer **203** also comprises a receiver(s) **203**G for receiving signals and/or data from the cellular telephone **202** and from the communication device **204** and/or from any other suitable device which may be utilized in conjunction with the apparatus **200**. The receiver(s) **203**G is also connected to the CPU **203**A.

The central processing computer **203** also comprises a database(s) **203**H which contains account information and data pertaining to the cellular telephone owner(s) and/or account(s). The database **203**H contains information about the cellular telephone owner, the telephone number, etc., and any other information and/or data necessary to the manage and/or process an account and/or account transaction as described herein. The database **203**H may also contain information regarding any limitations and/or restrictions placed on the cellular telephone and/or the use thereof. The database **203**H is also connected to the CPU **203**A. The central processing computer **203** also comprises a printer **203**I or other appropriate output device for outputting information and/or data to a user or operator.

In FIG. **8**, the communication device **204**, in the preferred embodiment, comprises a central processing unit or CPU **204**A, associated random access memory **204**B (RAM) and read only memory **204**C (ROM) devices, which also connected to the CPU **204**A, a user input device **204**D, which is a keypad or a plurality of keys and/or switches for inputting data into the communication device **204** and which is also connected to the CPU **204**A, and a display device **204**E, for displaying information and/or data to the cellular telephone owner, and a database **204**F, which are also connected to the CPU **204**A.

The communication device **204** also comprises a receiver **204**G for receiving signals and/or data from the central processing computer **203** and which is also connected to the CPU **204**A, a transmitter **204**H for transmitting signals and/or data to the central processing computer **203** and which is also connected to the CPU **204**A. In the preferred embodiment, the communication device **204** utilized is a pager with a reply feature and/or device. A two-way pager and/or pager systems may also be utilized for implementing the respective components, and/or systems in the communication device **204**/central processing computer **203** combination and/or link.

The apparatus **200** of the present invention, in the preferred embodiment, may be utilized in order provide cellular telephone owner and/or account owner authorization, notification and/or security measures in transactions involving cellular telephones and/or cellular telephone numbers, and any transactions involving same in the manner described below and with reference to FIG. **9**. In this manner, the apparatus and method of the present invention may be utilized to obtain cellular telephone owner and/or account owner authorization in a transaction involving cellular telephones and/or cellular telephone numbers.

FIG. **9** illustrates the operation of the apparatus **200** of FIG. **7** in flow diagram form. It is important to note, with regards to the apparatus **200** of FIG. **7**, that the cellular telephone replaces the transaction terminal of the previously described embodiments. With reference to FIG. **9**, the operation of the apparatus **200** commences at step **230** when the cellular telephone **202** is utilized to make a cellular telephone call and/or transaction.

The cellular telephone **202** will activate the apparatus **200**, at step **231**, with the initiation of the cellular telephone call, and/or in any other typical manner, such as when a cellular telephone is utilized to gain access to the telephone network so that the calling connection may be established via the cellular communications network and/or the cell site. Upon the making of the cellular telephone call, at step **231**, the cellular telephone **202** will transmit data and/or information, which identifies the calling telephone, to the central processing computer which services the particular cellular telephone or cellular telephone network, so that appropriate billing and/or accounting of telephone usage may be noted and/or processed. In the preferred embodiment, the central processing computer for the particular cellular telephone and/or cellular telephone network is the central processing computer **203**. At step **232**, the central processing computer will receive and store the data and/or information which is transmitted by the cellular telephone **202**. At step **233**, the central processing computer **203** will process the data and/or information which is received from the cellular telephone **202**.

The central processing computer **203** may utilize any of the widely known data processing and/or software routines, which are known to those skilled in that art, in order to process transaction requests and/or authorizations involving the use of the respective cellular telephone(s) and/or cellular communication device, and/or cellular telephone number. At step **234**, the central processing computer **203** will perform a test in order to determine if the cellular telephone is lost,

stolen, cancelled or de-activated. If the cellular telephone is determined to be lost, stolen, cancelled or de-activated, the central processing computer **203** will, at step **235**, block the telephone call or terminate the call if it has already been connected. The central processing computer **203** will then, at step **236**, cancel and/or de-activate the cellular telephone number or account. The central processing computer **203** will then, at step **237**, notify the cellular telephone owner that his or her cellular telephone has been cancelled and/or de-activated. The operation of the apparatus will then cease at step **238**.

If, at step **234**, the central processing computer **203** determines that the cellular telephone is not lost, stolen, cancelled or de-activated, the central processing computer **203** will, at step **239**, transmit a signal and/or data to the communication device **204** which is located at the cellular telephone owner. At step **240**, the communication device **204** will receive and display the data and/or information which is transmitted from the central processing computer **203**. The displayed information, in the preferred embodiment, will include the number called, the time of the call, and the duration of the call, in real-time. The information will remain displayed during the duration of the call so that the cellular telephone owner will be notified continuously throughout the duration of the call.

At step **241**, the central processing computer **203** will await the cellular telephone owner's reply or response. If the cellular telephone owner replies or responds, the reply or response data will also be transmitted to, and received by, the central processing computer **203** at step **241**. At step **242**, the central processing computer **203** will then determine if the cellular telephone owner's response was made within a pre-defined time period, which is chosen, in the preferred embodiment, to be one (1) minute. If at step **242**, it is determined that the cellular telephone owner did not reply or respond within the predefined time limit, the central processing computer will, at step **243**, increment the unauthorized transaction count (UNAUTHCT) by one (1).

The central processing computer **203** will then, depending upon pre-defined instructions of the cellular telephone owner, at step **244**, either allow the telephone call to continue, such as for a pre-defined duration of one (1) minute, so as to allow for cases wherein an emergency condition exists, or terminate the telephone call immediately. The decision to either allow the telephone call to continue or to terminate the telephone call can be made by the cellular telephone owner and/or by the cellular telephone service provider. Upon the completion of step **244**, the central processing computer **203** will then, at step **245**, cancel and/or de-activate the cellular telephone. Thereafter, the central processing computer **203** will, at step **246**, notify the cellular telephone owner that the cellular telephone number or account has been cancelled and/or de-activated. Upon completion of step **246**, the apparatus will cease operation at step **247**.

If, at step **242**, the cellular telephone owner did respond in time, the central processing computer **203** will process the reply or response data and/or information, at step **248**. The central processing computer **203** will then determine, at step **249**, if the cellular telephone call is authorized by the cellular telephone owner. If, at step **249**, the cellular telephone call is unauthorized, the central processing computer will, at step **250**, increment the unauthorized transaction count (UNAUTHCT) by one (1). The central processing computer **203** will then, at step **251**, terminate the telephone call immediately. Upon the completion of step **251**, the central processing computer **203** will then, at step **252**, cancel and/or de-activate the cellular telephone. Thereafter, the central processing computer **203** will, at step **253**, notify the cellular telephone owner that the cellular telephone has been cancelled and/or de-activated. Upon completion of step **253**, the apparatus will cease operation at step **254**.

If, at step **249**, the central processing computer **203** identifies the cardholder reply or response as being one to authorize the cellular telephone call, the central processing computer **203** will, at step **255**, reset the unauthorized transaction count (UNAUTHCT) to zero (0). An unauthorized transaction count (UNAUTHCT) of 0 will signify that any string of unauthorized transactions has now been broken by the cellular telephone owner. The central processing computer **203** will then, at step **256**, allow the cellular telephone call to continue uninterrupted. Upon the completion of the cellular telephone call, at step **256**, the apparatus **200** will cease operation at step **257**.

In instances when the cellular telephone owner is a party to the cellular telephone call and/or transaction, he or she, having the communication device **204** on his or her person, may authorize the call and/or transaction at his or her present location. If the cellular telephone owner has lent out the cellular telephone, he or she may authorize the cellular telephone call and/or transaction from his or her remote location. The cellular telephone owner may also program and/or set the communication device **204** to automatically authorize or disapprove or disallow cellular telephone calls and/or transactions with said selective authorizations being made as to time of day, calling areas, numbers called, and/or call and/or transaction duration. In this regard, the communication device **204** may be programmable so as to receive and analyze the cellular telephone call information and/or data and reply or respond to same automatically and/or with preset or programmed replies and/or responses. The communication device **204** may also be programmable so as to limit the number of cellular telephone calls made from the cellular telephone and/or with the cellular telephone number.

The communication device **204**, in the preferred embodiment, is provided with a memory device for storing any number of cellular telephone calls and/or transactions so that the cellular telephone owner may review his or her account activity and/or cellular calls and/or transactions made and/or which have occurred involving his or her cellular telephone. In this manner, the cellular telephone owner may "scroll" through and/or in other ways review account activity. The communication device **204** may also be equipped to service more than one cellular telephone and/or mobile communication device(s).

The apparatus and method of the present invention provides for the real-time notification of cellular and/or mobile telephone usage which enables a cellular telephone owner and/or account owner to monitor, in real-time, activity involving his or her cellular telephone and/or cellular telephone number. The apparatus and method of the present invention also provides a means and a mechanism by which to inform a cellular telephone owner that the cellular telephone is lost or stolen, and/or to provide notification to the cellular telephone owner that his or her cellular telephone number is being utilized in calls and/or transactions, such as when a cellular telephone has been illegally "cloned". The cellular telephone owner may then report the cellular telephone lost or stolen and/or cancel and/or de-activate the cellular telephone number and/or account.

The present invention also provides a means and a mechanism by which to monitor the number of cellular or mobile telephone calls and/or transactions which are unauthorized

by the cellular telephone owner and to determine whether or not to de-activate the cellular telephone and/or the cellular telephone number and/or account. In the above manner, the apparatus and method of the present invention provides an apparatus and a method to prevent and/or to drastically limit fraudulent and/or unauthorized use of, and/or the "cloning" of, cellular telephones and/or the unauthorized use of cellular telephone numbers.

The apparatus and method of the present invention may also be utilized in connection with an on-line service and/or on, or over, the Internet and/or the World Wide Web, so as to provide for a means by which the respective cardholder, account owner, and/or cellular telephone owner, may utilize the apparatus and method in conjunction with a home and/or a personal computer, a personal communications device, and/or a commercial or industrial computer system (i.e., an internet server computer), and/or any other appropriate device, in any appropriate network, system or medium.

FIG. **10** illustrates yet another alternate embodiment of the present invention wherein the apparatus and method of any of the embodiments described herein may be utilized on, or over, an on-line service, the Internet, and/or the World Wide Web, and/or any other suitable communication network or medium. In FIG. **10**, the apparatus, which is denoted generally by the reference numeral **300**, comprises a transaction terminal **302**, which may be a transaction terminal or a cellular telephone or communication device, depending upon the application, a server computer **350**, which is a central processing computer for processing data and/or information in an on-line, and/or Internet, and/or World Wide Web, communication environment, network, or medium.

The server computer **350** may be a mainframe computer, a mini-computer, a micro-computer, a server computer, such as those utilized in conjunction with on-line services and/or in a network environment, and/or any other suitable computer or computer system. The server computer **350**, in the preferred embodiment, should have associated therewith a suitable receiver(s) or transmitter(s) which may be a fax/modem and/or any other device(s) which are well known to those skilled in the art for providing communications and/or a link with a server computer in such a network environment.

The apparatus of FIG. **10** also comprises a communications device **304** which may comprise a home and/or a personal computer, a laptop or a notebook computer and any one or more of the herein-described personal communications devices so that the individual may access the apparatus **300**, and in particular, the server computer **350**, at any time and from any location. Basically, the embodiment of FIG. **10** serves to replace the central processing computer of the previously described embodiments with a server computer for utilization on, or over, an on-line service, the Internet, the World Wide Web, and/or any other suitable communications network or medium. The apparatus of FIG. **10** operates and is utilized in the same, in similar and/or an analogous, manner as described herein in conjunction with the previously described embodiments.

FIG. **11** illustrates yet another alternate embodiment of the present invention, wherein the present invention is also utilized in conjunction with an on-line service and/or on, or over, the Internet and/or the World Wide Web, and/or any other suitable communication network or medium. In FIG. **11**, the apparatus, which is denoted generally by the reference numeral **400**, comprises a transaction terminal **402**, which may be a transaction terminal and/or a cellular telephone and/or cellular communications device, depending upon the application.

The apparatus of FIG. **11** also comprises a central processing computer **403** which provides processing and/or control over the apparatus **400** in the manner described above in conjunction with the previously described embodiments. The central processing computer **403** and/or the server computer **450** may be a mainframe computer, a mini-computer, a micro-computer, a server computer, such as those utilized in conjunction with online services and/or in a network environment, and/or any other suitable computer or computer system.

The apparatus **400** of FIG. **11** also comprises a communications device(s) **404** such as those described herein and in conjunction with the apparatus **300** of FIG. **10**. The apparatus also comprises a server computer **450** which may either perform parallel operations and/or processing of the data and/or information which is performed and/or processed by the central processing computer **403** and/or may simply receive the data and/or information processed by the central processing computer **403**. In any event, the server computer **450** provides the means by which the data and/or information, which is provided by the apparatus, can be accessed and or utilized via an on-line service and/or on, or over, the Internet, and/or the World Wide Web, and/or any other communications network or medium.

The server computer **450** should have associated therewith a suitable receiver(s) or transmitter(s) which may be a fax/modem and/or any other device(s) which are well known to those skilled in the art for providing communications and/or a link with a server computer in such a network environment. The apparatus of FIG. **11** also comprises a communications device **404** which may comprise a home and/or a personal computer, a laptop or a notebook computer, and/or any one or more of the herein described personal communications devices so that the individual may access the apparatus, and in particular, the server computer **450**, at any time and from any location. The apparatus of FIG. **11** is utilized and/or operates in the same, a similar and/or an analogous, manner as any of the embodiments described herein.

Applicant hereby incorporates by reference herein all of the methods and/or techniques for providing information and/or data over on-line service and/or on, or over, the Internet, and/or the World Wide Web, and/or any other suitable communication network or medium, along with client/server and/or Web Site technology and methods and/or techniques utilized in conjunction therewith, which are known as of the filing date of this application.

In any and/or all of the embodiments described herein, each and every one the components of the apparatus, which include, but which are not limited to, the described transaction terminals, cellular telephones and/or other cellular communications devices, central processing computers, server computers, if utilized, and any of the various communications devices, may transmit and/or receive signals and/or data, and/or be capable or transmitting and/or receiving signals and/or data, to and from any and all of the other apparatus components which may be utilized in conjunction therewith, in and for a given embodiment. In this regard, it is important to note, with respect to the embodiments of FIGS. **10** and **11**, and any of the other embodiments described herein, that each and every component involved in the transmission and/or reception of signals, data and/or information may include an associated transmitter, receiver and/or suitable communication device.

The communication system or medium should provide for the transmission and/or for the reception of a multitude of remote electrical, electronic, electromagnetic, and/or other suitable signals, over long distances and/or in a mobile and/or a wireless communications environment. Telephone signals and telephone communication devices can be utilized in the present invention as well as personal computers and associated peripheral devices which may be utilized with telecommunications and/or other suitable communication systems and/or mediums.

The apparatus and method of the present invention may operate over any appropriate communications system, network and/or medium and/or other suitable communications systems, including radio signal, optical, satellite, digital, digital satellite, and/or other communications systems. The communications system utilized may operate anywhere in the electromagnetic and/or radio frequency spectrum. As noted above, the present invention may also be utilized in conjunction with a satellite communications system, in which case, the receivers and transmitters which are utilized in conjunction with the apparatus should be satellite communication receivers and transmitters, respectively. For example, the associated receiver(s) may be a satellite dish receiver(s).

In this regard, the cardholder, account owner or cellular telephone owner may utilize the apparatus and method of the present invention to its fullest capabilities over an on-line service and/or on, or over, the Internet, and/or the World Wide Web, and/or any other suitable communication network or medium. In this manner, the embodiment of FIGS. **10** and **11** may allow the cardholder, account owner or cellular telephone owner to utilize the apparatus and/or to monitor the operation of the apparatus over the on-line service and/or on, or over, the Internet, and/or the World Wide Web, and/or any other communication network or medium, from any suitable computer or device, and/or from any location.

The system receiver(s) may also be utilized in conjunction with a home and/or a personal computer and/or other personal communications device(s) and/or apparatuses which may be utilized with an associated receiver or equivalent peripheral device(s). The apparatus may also be utilized in conjunction with a computer network such as an on-line service and/or on, or over, the Internet, and/or the World Wide Web, by employing any appropriate server computer and/or an associated Web Site and/or Web Site technology in conjunction with an appropriate communication medium and communication equipment.

In any of the above described embodiments, the present invention may be utilized in conjunction with any suitable communication device(s) and/or communication system(s). In this manner, the present invention may be utilized in conjunction with a telephone, a line-connected and/or a permanent telephone, a touch-tone telephone, a cordless telephone and/or a cellular or mobile telephone, a home and/or a personal computer having associated telecommunication devices or other suitable peripheral device(s), such as a modem and/or a fax/modem, and/or other suitable personal communication devices which can operate over an appropriate communications system, and/or other suitable communications systems and/or mediums, including radio signal, optical, satellite, digital, and/or other communications systems and/or mediums.

Any suitable communication system and/or medium may be utilized. Personal communication service (PCS) systems and devices, including stationary, portable and/or hand-held devices, may also be utilized. Digital signal communications devices and systems may also be utilized. Televisions, interactive and/or digital televisions, personal communication devices, personal communication services (PCS) devices, personal digital assistants, cellular telephones, display telephones, video telephones, display cellular telephones and electronically equipped watches and/or other devices and/or effects and/or accessories, may also be utilized for performing user interactive control, monitoring, authorization, notification and/or security functions in conjunction with the present invention.

It should be noted that the telephone/telephone beeper or pager system, including two-way pager systems, may be replaced with any other type of transmitter/receiver combination, electronic or otherwise, which provides for the transmission and reception of a multitude of remote electrical, electronic, electromagnetic, and/or other suitable signals, over long distances and/or in a mobile and/or a wireless communications environment. As noted above, a personal computer system which may be adapted to such operation, or a personal communication device(s) or personal communication services (PCS) device(s) may also be utilized for, or in, any of the transmitter/receiver system combinations described herein. Two-way pagers and reply pagers may also be utilized for any, or in any, of the transmitter/receiver system combinations described herein.

The communication device(s) utilized in the present invention, as well as the associated transaction terminal and/or cellular communications device(s) and/or associated central processing computer may be personal communication services (PCS) devices and/or other suitable communications devices. A television, appropriately equipped to receive and/or to transmit signals may also be utilized. It is also envisioned that digital televisions, interactive televisions, personal communications devices, personal communications services (PCS) devices, personal digital assistants, display telephones, electronically equipped watches, cellular telephones and/or display cellular telephones may also be utilized in conjunction with the present invention.

It is also important to note that the communication device(s), in any of the embodiments described herein may be a home and/or a personal computer having associated therewith an appropriate receiver(s) and transmitter(s) such as, for example, a fax/modem.

It is important to note that the telephone/telephone beeper system, described above, may be replaced with any remote transmitter/receiver system, such as by a remote transmitter, i.e., a television-type remote control unit, which control unit would require a user interface feature and which has the capability to remotely transmit a multitude of signals over long distances to an associated receiver. A two-way pager, a reply pager, or any other appropriate two-way communication device may also be utilized. A home and/or a personal computer, with requisite peripheral devices, a personal communication device and/or a personal communication services (PCS) device may also be utilized. Digital communications devices, interactive televisions and/or digital televisions may also be utilized. It is also envisioned that digital televisions, interactive televisions, personal communications devices, personal communications services (PCS) devices, personal digital assistants, display telephones, video telephones, electronically equipped watches and/or other effects or accessories, cellular telephones, display cellular telephones, may also be utilized.

The apparatus of the present invention may be designed or programmed to telephone an owner, user, operator,

occupant, or other authorized central office individual or other authorized individual, at a primary phone number, at an alternate or forwarding phone number and/or at a business phone number, send a beeper or pager message to the individual or central office and/or send a facsimile message, an electronic mail message, a voice mail message and/or an answering service message to, or for, the individual or central office. In this manner, the apparatus may report a theft and/or a malfunction situation to the interested individual(s) by utilizing multiple notification and/or reporting avenues and/or schemes so as to provide and ensure that the interested individual(s) are in fact notified as soon as possible. The multiple notification transmissions may be sequentially and/or simultaneously performed.

The apparatus and method of the present invention may also be programmable for programmed and/or automatic activation, self-activation, programmed and/or automatic operation and/or self-operation. The apparatus and method of the present invention may provide for an immediate, as well as for a deferred, control, monitoring and/or security function, and/or response thereto, so as to provide for the immediate and/or the deferred control, activation, de-activation, programming, monitoring and/or security, etc., of any one or more the herein described credit cards, charge cards, debit cards, currency or "smart" cards, banking and/or financial accounts and associated transaction cards, and/or cellular telephones and/or cellular or mobile communications devices, and/or any other suitable application in and for which the present invention may be utilized.

In any of the herein-described embodiments, the communications devices and associated transaction terminals and/or cellular communications devices and associated central processing computers, may be devices for receiving, and transmitting, respectively, radio signals, satellite communication signals, telecommunications signals, optical communication signals and/or other signals and/or those signals, including digital signals, which are utilized in conjunction with personal communication devices and/or personal communication services (PCS) devices. The devices utilized should, however, be of the same type and/or operate compatibly with the corresponding transmitters and receivers of the apparatus of the present invention.

The present invention may also be equipped with, and be utilized in conjunction with, hardware and software necessary for providing self-monitoring functions, automatic control and/or responses to occurrences, providing automatic notice of an occurrence and/or a situation to an owner, user and/or authorized individual. In this regard, any and all of the embodiments described above may comprise a monitoring device, a triggering device and/or any other suitable device for detecting an occurrence and/or a transaction which may warrant providing notice to the respective cardholder, account owner and/or cellular telephone owner. In this regard, the apparatus may provide for an appropriate signal, data and/or information transmission to the central processing computer, and/or server computer, if utilized. The signal, data and/or information may be conveyed in the form of a communication transmission, depending upon the communication medium utilized, a telephone call, a voice message, a beeper and/or a pager message, an electronic mail message, a fax transmission, and/or any other mode of communication which may be utilized in conjunction with any of the embodiments described herein.

The present invention, in any of the embodiments described herein, may be designed to be user-friendly. In this regard, the present invention may be menu-driven, and/or its operation may be menu-selected, from audio menus, visual menus, or both audio and visual menus.

While the present invention has been illustrated and described as being utilized in conjunction with providing notice and for obtaining authorizations with regard to transactions involving credit cards, charge cards, debit cards, and/or currency or "smart" cards, banking and/or financial accounts, and/or in conjunction with cellular and/or mobile telephones, it is also envisioned that the present invention may be utilized in any similar type of transactional activity, such as purchasing and/or sale activity over an on-line service, the Internet, and/or the World Wide Web and/or in any other type of transaction wherein frequent notice and/or account holder authorization may be utilized to guard against theft and/or fraud and/or unauthorized transactions.

The apparatus of the present invention may be accessed at any time by the respective cardholder, account owner and/or cellular telephone owner and/or cellular communications device owner so as to obtain information regarding activity on his or her respective account. The respective cardholder, account owner and/or cellular telephone owner and/or cellular communications device owner may access the apparatus and, in particular, the central processing computer, and/or the server computer, if utilized, so as to obtain transaction records regarding any transaction, group or string of transactions, transactions by goods and/or service type, transactions by dollar amount, etc.

The respective cardholder, account owner, and/or cellular telephone owner and/or cellular communications device owner may also obtain, via the central processing computer, and/or the server computer, if utilized, periodic transaction records showing all transactions for a given week, which may by provided weekly, bi-weekly, monthly, yearly, and/or for any given and/or desired time period and/or interval. The apparatus and, in particular, the central processing computer, and/or the server computer, if utilized, may be designed and/or programmed so as to automatically and/or periodically provide and/or transmit any of the above-described account and/or transaction information to the respective cardholder, account owner and/or cellular telephone owner and/or cellular communications device owner, by transmitting same to the respective communications device, which may be any of the devices described herein which are utilized as the communications device.

The apparatus and, in particular, the central processing computer, and/or the server computer, if utilized, may also be designed and or programmed to transmit any of the above-described account information and/or transaction information to any one or all of the respective cardholder's, account owner's, and/or cellular telephone owner's and/or cellular communications device owner's facsimile (fax) machine, personal computer, telephone, telephone answering machine, alternate telephone, alternate telephone answering machine, network computer, and/or alternate beeper or pager. Such multiple notification transmissions, if utilized, may be performed sequentially and/or simultaneously.

The central processing computer may be linked with a fax machine, personal computer, telephone, associated answering machine, alternate telephone and associated answering machine, network computer, and/or alternate beeper or pager via any suitable communication system. The telecommunications link or telephone line or link, which may or may not be a wireless link, depending on the device and/or the circumstances, is utilized in order to link the central processing computer with each of the fax machine, the personal computer, the telephone, the associated answering machine, the alternate telephone, the alternate telephone answering machine, the network computer, and/or the alternate beeper or pager.

In any of the herein-described and/or envisioned embodiments, the respective central processing computer which is utilized may comprise a plurality of computers and/or computer systems. Further, the respective central processing computer may be the processing computer for processing account information, and/or for servicing, and/or monitoring, the respective account(s) activity, and/or the central processing computer may be a separate and/or distinct computer or computer system which is associated with and/or linked with the processing computer.

In any of the herein-described and/or envisioned embodiments, the respective communication device which may be utilized may operate independently of, and/or in conjunction with, a central service and/or a communications service. For example, a beeper or pager may be utilized in conjunction with a corresponding beeper or pager communications service, which communications service may serve to relay signals, data and/or information, to, and from, the beeper or pager, whichever the case may be. The communication device which may be utilized may also be capable of transmitting signals, data and/or information, directly to, and receiving signals, data and/or information, directly from, a component(s) of the apparatus, without the need for a central service and/or a communications service and/or a relay system.

It is also envisioned that the apparatus and method of the present invention may provide for transmitting signals, data and/or information to the cardholder, account owner and/or cellular telephone owner via transmissions made to, and received at a television, radio, car radio, computer and/or other communication device which receives signals transmitted via any suitable communication system. In this manner, for example, a cardholder, account owner and/or cellular telephone owner may be notified by having signals, data and/or information transmitted to their television, radio, car radio, computer, etc., in such a manner so as to interrupt the normal operation of same, so as to convey the information and/or message to the cardholder, account owner and/or cellular telephone owner, in real-time and/or upon the occurrence of the event triggering or giving rise to same.

In any and/or all of the above described embodiments, the apparatus may be programmed and/or be programmable by the respective cardholder, account owner and/or cellular telephone owner or cellular device owner, for his or her account. In conjunction with the use of credit cards, charge cards, debit cards, the cardholder may program the central processing computer, and/or the server computer, if utilized, so as to change the credit limits on his or her account, periodically and/or at any desired time. For example, a cardholder having a credit card with a $10,000.00 dollar credit limit, but who very seldom utilizes his or her card for much more than $500.00 dollars during a monthly billing period, may program the apparatus and, in particular, the central processing computer, or server computer, if utilized, so as to temporarily reduce his or her credit limit.

If the cardholder should then desire to make a major purchase with his or her credit card of, for example, a purchase in the amount of $8500.00, the cardholder may, prior to the transaction, reprogram the central processing computer and/or server computer, if utilized, so as to temporarily increase his or her temporary credit limit. The apparatus may then be programmed so that, after the major purchase has been made, the apparatus may revert operation back to the reduced credit limit.

The cardholder may program the central processing computer, and/or the server computer, if utilized, via the communication device, which may be any one or more of the devices described herein. The cardholder may also perform the above-described programming via a touch-tone telephone. In the same manner, the cardholder may program the apparatus so as to limit the types of transactions involving, and/or the goods and/or services which may be purchased with, his or her card, and/or the stores and/or service providers which may be authorized to accept the card, limits on the dollar amounts of transactions pertaining to each authorized vendor, seller and/or service provider, daily spending limits, the vendors, sellers, and/or service providers with which the card may be utilized, the geographical area or location within which the card may be utilized, and/or authorized times for card usage (i.e. specific days, dates, times of day, times of month, year, etc.), and/or any other limitations and/or restrictions regarding amount of transaction, parties involved, geographical area, and or times of allowed usage. In a similar manner, the cardholder may similarly program the apparatus as described above in conjunction with use of any of the herein-described cards.

In a similar manner, a cardholder of a currency and/or "smart" card may program the apparatus so as to limit the types of transactions involving, and/or the goods and/or services which may be purchased with, his or her card, and/or the stores or service providers which may be authorized to accept the card, limits on the dollar amounts of transactions pertaining to each authorized vendor, seller and/or service provider, daily spending limits, the vendors, sellers, and/or service providers with which the card may be utilized, the geographical area or location within which the card may be utilized, and/or authorized times for card usage (i.e. specific days, dates, times of day, times of month, year, etc.), and/or any other limitations and/or restrictions regarding amount of transaction, parties involved, geographical area, and or times of allowed usage.

In the case of savings accounts, checking accounts, and/or automated teller machine accounts, the account owner may program the apparatus and, in particular, the central processing computer, and/or the server computer, if utilized, so as to limit the amount of any one transaction or transactions, individuals who may make the transactions, proof of identity of which the types of proof may be specified, specific banks and/or financial institutions authorized to accept and/or perform transactions for the account, geographical areas and/or location within which banks and/or financial institutions may be authorized to accept and/or perform transactions with the account, specific times of day, specific days, dates and/or time of the month in, or on, which transactions may be authorized, limits of charge-backs, returned item amount withdrawals, maintenance and/or other fee charge withdrawals, etc. and/or authorized times for account usage (i.e. specific days, dates, times of day, times of month, year, etc.), and/or any other limitations and/or restrictions regarding amount of transaction, parties involved, geographical area, and or times of allowed usage.

With regards to automated teller machine accounts, it is also possible to specify and programmably change personal identification numbers and/or any other access code(s) and provide for various personal identification numbers and/or access codes for different locations, different automated teller machines, different days, different times and/or different transaction amounts.

In the cases of cellular telephones and/or cellular communications devices, the cellular telephone owner and/or cellular communication device owner may program the apparatus and, in particular, the central processing computer, and/or the server computer, if utilized, so as to limit the

phone numbers which may be called, and/or the numbers from which incoming calls may be accepted and/or received, the geographical areas and/or locations which may be called and/or accessed or from which calls may be received, the times of day, specific days, dates, times of month or year, during which the cellular telephone and/or cellular communication device may be utilized, specific phone numbers which may be called, specific time durations for a phone call and/or any authorized times for cellular telephone and/or cellular communication device usage (i.e. specific days, dates, times of day, times of month, year, etc.), and/or any other limitations and/or restrictions, regarding amount of transaction, parties involved, geographical area, and or times of allowed usage.

The present invention may also be utilized so as to provide financial transaction and/or wireless communication device authorization, notification and/or security for any number and/or types of accounts, including credit card accounts, charge card accounts, debit card accounts, currency or "smart" card accounts, and/or other transaction card accounts, savings accounts, checking accounts, automated teller machine accounts, cellular telephone accounts and/or cellular communication device accounts. In this manner, the apparatus may comprise a communication device or communications devices which may receive and/or transmit signals, data and/or information, for any number and/or types of the above accounts, and/or for each of the respective accounts utilized, from and to the respective central processing computer and/or central processing computers for the respective accounts. In this manner, an individual may utilize a single communication device so as to monitor all of his or her accounts and/or types of accounts.

The apparatus and method of the present invention provides for the real-time notification of financial transactions involving credit cards, charge cards, debit cards, and/or currency or "smart" cards, which enables a cardholder to monitor, in real-time, activity involving his or her card(s) and the corresponding accounts. The apparatus and method of the present invention also provides a means and a mechanism by which to inform a cardholder that his or her card(s) are lost, stolen, or is being utilized in an unauthorized manner and provides an indication to the cardholder of when and where his or her card(s) is being utilized in transactions. The cardholder may then report the card lost or stolen and/or cancel and/or de-activate the card. The apparatus and method of the present invention provides the same, and/or analogous, features and/or functions for banking and/or financial accounts and/or for cellular telephone accounts.

While the communications device(s) described above are described, in each of the respective embodiments, as being utilized for specific uses (i.e. credit and other cards transactions, banking and/or financial transactions, and/or cellular telephone transactions, the communication device (s) may also be adapted and/or programmed for use in all of these aforementioned transactions so that an individual may utilize a single communication device for all of the above described and/or envisioned transaction types.

It is envisioned that the apparatus and method of the present invention may be utilized in conjunction with other apparatuses and methods in the prior art, and that the present invention may be incorporated with these known apparatuses and methods so as to improve upon them and so as to find additional applications for the present invention.

Applicant hereby incorporates by reference herein the following United States Patents: U.S Pat. No. 5,173,594 which teaches a system for printing personalized charge-card service receipts at remote locations; U.S. Pat. No. 5,479,510 which teaches an automated data card payment verification method; U.S. Pat. No. 5,473,667 which teaches a paging system with third party authorization; U.S. Pat. No. 3,723,655 which teaches a credit authorization terminal; U.S. Pat. No. 5,485,510 which teaches a secure credit/debit card authorization; U.S. Pat. No. 5,406,619 which teaches a universal authentication device for use over telephone lines; U.S. Pat. No. 5,444,616 which teaches financial transaction systems and methods utilizing a multi-reader transaction terminal; U.S. Pat. No. 5,513,250 which teaches telephone based credit card protection; U.S. Pat. No. 4,485,300 which teaches a loss control system; U.S. Pat. No. 4,758,714 which teaches a point-of-sale mechanism; U.S. Pat. No. 4,947,027 which teaches a system for identifying authorized use of credit cards; U.S. Pat. No. 5,357,563 which teaches a data card terminal for receiving authorizations from remote locations; U.S. Pat. No. 5,444,763 which teaches a translation and connection device for radio frequency point of sale transaction system; U.S. Pat. No. 5,243,645 which teaches an automatic system for forwarding of calls; and U.S. Pat. No. 3,938,090 which teaches a terminal apparatus.

While the present invention has been described and illustrated in various preferred and alternate embodiments, such descriptions are merely illustrative of the present invention and are not to be construed to be limitations thereof. In this regard, the present invention encompasses any and all modifications, variations and/or alternate embodiments with the scope of the present invention being limited only by the claims which follow.

What is claimed is:

1. A transaction security apparatus, which comprises:

a receiver for receiving one of a limitation and a restriction on an account usage, wherein said one of a limitation and a restriction on an account usage are received in real-time from an individual account holder;

a memory device for storing said one of a limitation and a restriction on an account usage; and

a central processing device for processing an authorization request for a transaction on an account in conjunction with said one of a limitation and a restriction on an account usage,

wherein said central processing device generates a first signal, wherein said first signal contains information for one of authorizing and disallowing the transaction.

2. The apparatus of claim **1**, wherein said account is one of a credit card account, a charge card account, a debit card account, a currency card account, a "smart" card account, a bank account, a savings account, a checking account, an automated teller machine account, a cellular telephone account, and a cellular communication device account.

3. The apparatus of claim **1**, wherein said one of a limitation and a restriction on an account usage is one of a type of authorized transaction, one of a good and a service authorized, authorized one of vendor, store, and service provider, transaction amount limitation, daily spending limit, authorized geographical area of usage, authorized time of usage, authorized individual, transaction limit for one of a savings account, a checking account, a bank account, and an automated teller machine account, authorized individual for transacting on a savings account, a checking account, a bank account, and an automated teller machine account, proof of identity required for transaction, one of bank and financial institution authorized for the transaction, a limitation of a fee charge on an account, automated teller machine

account access code, authorized transaction location, authorized telephone number, authorized telephone calling time, authorized telephone calling area, authorized telephone calling destination, authorized number of telephone calls, authorized incoming telephone call, authorized telephone call duration, and authorized telephone call one of cost and transaction amount.

4. The apparatus of claim **1**, wherein said receiver receives a transaction authorization request signal.

5. The apparatus of claim **1**, wherein said apparatus further comprises:

a transmitter for transmitting a notification signal to an account holder in response to the authorization request.

6. The apparatus of claim **5**, wherein said notification signal is transmitted to an individual communication device.

7. The apparatus of claim **6**, wherein said individual communication device is one of a telephone, a beeper, a pager, a two-way pager, a reply pager, a home computer, a personal computer, a personal communication device, a personal communication services device, a digital communications device, a television, an interactive television, a digital television, a personal digital assistant, a display telephone, a radio, a car radio, a video telephone, a watch, a cellular telephone, a wireless telephone, a mobile telephone, a display cellular telephone, and a facsimile machine.

8. The apparatus of claim **1**, wherein said one of a limitation and a restriction on an account usage is transmitted to said receiver from one of a telephone, a touch-tone telephone, a two-way pager, a reply pager, a home computer, a personal computer, a personal communication device, a personal communication services device, a digital communications device, a television, an interactive television, a digital television, a personal digital assistant, a display telephone, a video telephone, a watch, a cellular telephone, a wireless telephone, a mobile telephone, a display cellular telephone, and a facsimile machine.

9. The apparatus of claim **1**, wherein said authorization request is transmitted from one of a point-of-sale device, a transaction device, a cellular telephone, and a cellular communication device.

10. The apparatus of claim **1**, wherein said one of a limitation and a restriction on an account usage is transmitted one of on-line and via a non-voice signal.

11. The apparatus of claim **1**, wherein said apparatus further comprises:

means for counting a number of unauthorized transactions which occur on an account.

12. The apparatus of claim **5**, wherein said notification signal contains one of transaction type, transaction amount, location of transaction, time of transaction, and one of good and service involved in the transaction.

13. The apparatus of claim **1**, wherein said apparatus operates one of on and over a telecommunication network, a satellite communication network, a radio communication network, a digital communications network, a cellular communication network, a personal communications services communication network, the Internet, and the World Wide Web.

14. A transaction security apparatus, which comprises:

means for receiving one of a limitation and a restriction on an account usage, wherein said one of a limitation and a restriction on an account usage are received in real-time from an individual account holder;

means for storing said one of a limitation and a restriction on an account usage; and

means for processing an authorization request for a transaction on an account in conjunction with said one of a limitation and a restriction on an account usage,

wherein said processing means generates a first signal, wherein said first signal contains information for one of authorizing and disallowing the transaction.

15. The apparatus of claim **14**, wherein said apparatus further comprises:

means for transmitting a notification signal to an account holder in response to the authorization request.

16. The apparatus of claim **14**, wherein said apparatus further comprises:

means for counting a number of unauthorized transactions which occur on an account.

17. A method for transaction security, which comprises:

receiving one of a limitation and a restriction on an account usage, wherein said one of a limitation and a restriction on an account usage are received in real-time from an individual account holder;

storing said one of a limitation and a restriction on an account usage;

processing an authorization request for a transaction on an account in conjunction with said one of a limitation and a restriction on an account usage; and

determining whether the transaction is one of authorized and unauthorized.

18. The method of claim **17**, further comprising:

notifying an account holder of the transaction.

19. The method of claim **17**, further comprising:

counting a number of unauthorized transactions which occur on an account.

20. The method of claim **17**, wherein said account is one of a credit card account, a charge card account, a debit card account, a currency card account, a "smart" card account, a bank account, a savings account, a checking account, an automated teller machine account, a cellular telephone account, and a cellular communication device account.

* * * * *

US 20010011249A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2001/0011249 A1**

YANAGIHARA et al. (43) **Pub. Date: Aug. 2, 2001**

(54) **ELECTRONIC MONEY CARD, ELECTRONIC MONEY RECEIVING/PAYING MACHINE, AND ELECTRONIC MONEY CARD EDITING DEVICE.**

(76) Inventors: **YASUSHI YANAGIHARA**, OWARIASAHI-SHI (JP); **CHIE HAYAMI**, OWARIASAHI-SHI (JP)

Correspondence Address:
50
104 EAST HUME AVENUE
ALEXANDRIA, VA 22301

(*) Notice: This is a publication of a continued prosecution application (CPA) filed under 37 CFR 1.53(d).

(21) Appl. No.: **09/072,455**

(22) Filed: **May 5, 1998**

(30) **Foreign Application Priority Data**

May 13, 1997 (JP) 09-122514

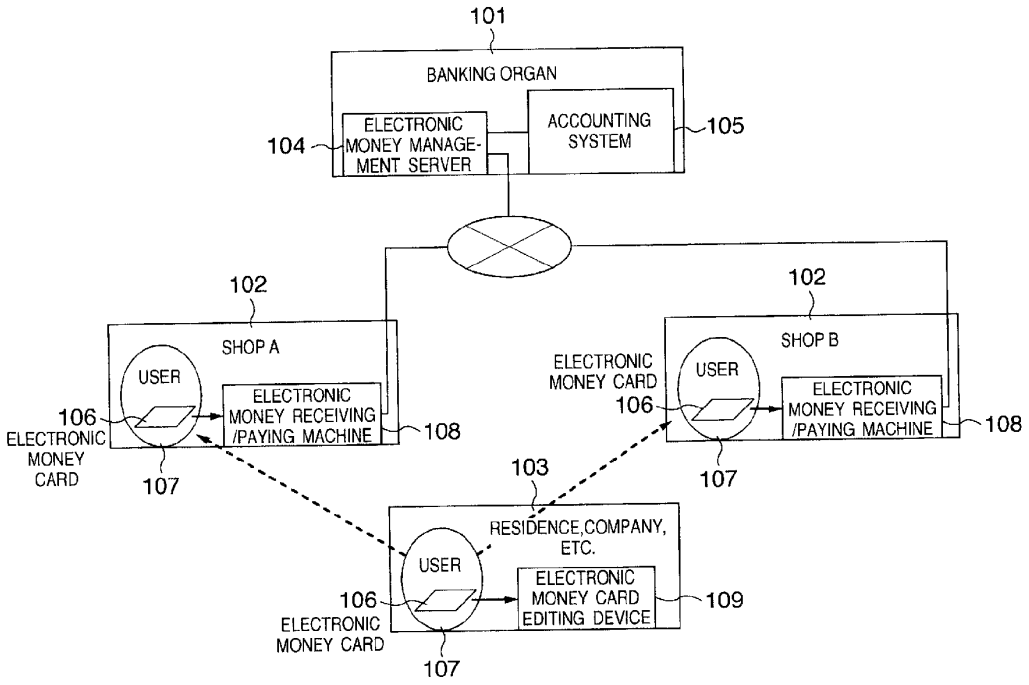
Publication Classification

(51) **Int. Cl.**[7] **G06F 17/60**

(52) **U.S. Cl.** **705/41**; 705/40; 705/42; 705/43; 235/379; 235/380

(57) **ABSTRACT**

An electronic money card includes a memory built in an IC chip of an IC card and reads and writes electronic money to and from the memory. The electronic money card allows conditions restricting an electronic money reading process to be written in a storage area excluding an electronic money storage area set for each user or usage of the electronic money.



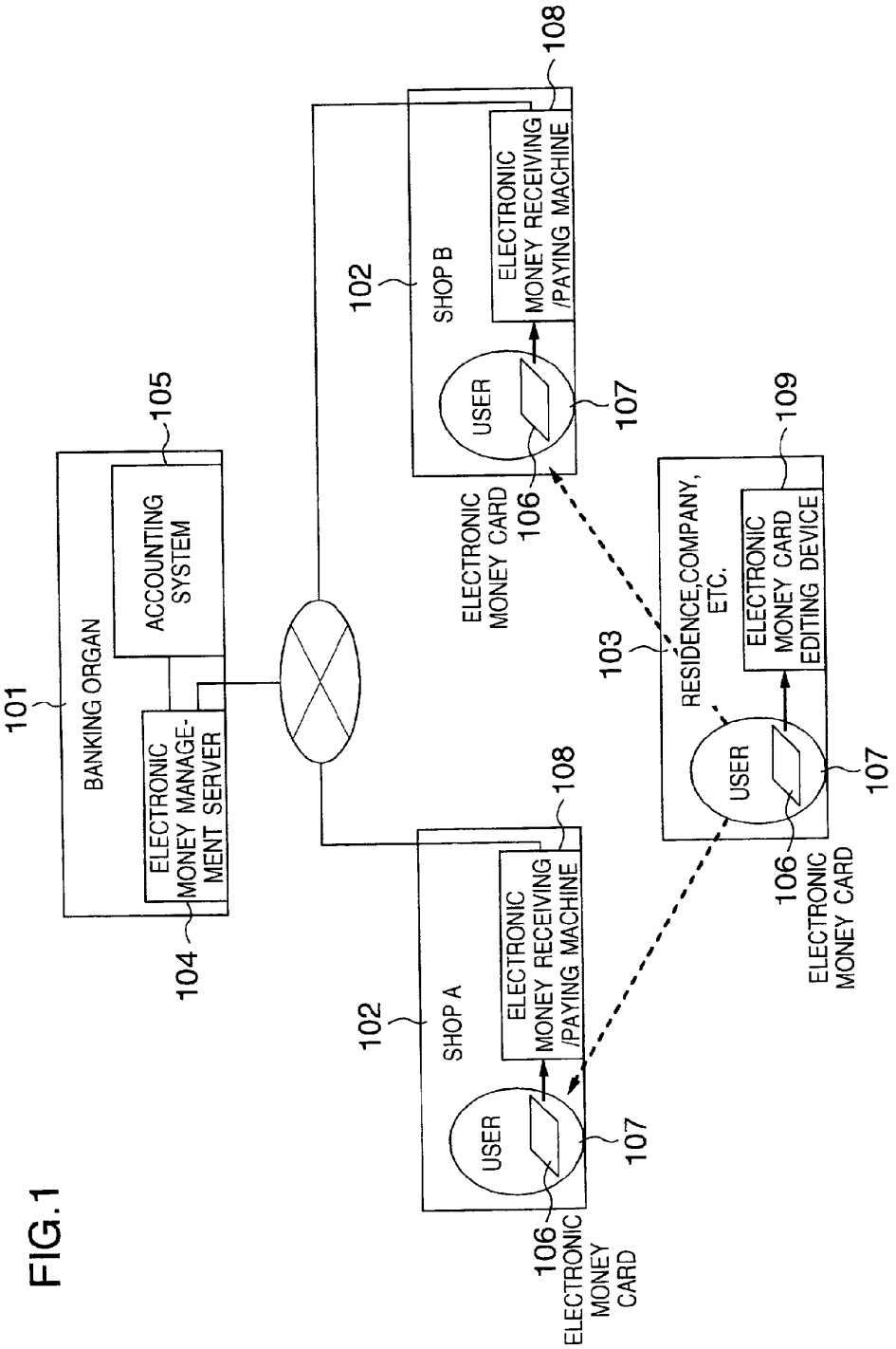

101
BANKING ORGAN
105
ACCOUNTING SYSTEM
ELECTRONIC MONEY MANAGE-MENT SERVER
104
102
SHOP B
108
ELECTRONIC MONEY RECEIVING /PAYING MACHINE
USER
107
ELECTRONIC MONEY CARD
106
103
RESIDENCE,COMPANY, ETC.
109
ELECTRONIC MONEY CARD EDITING DEVICE
USER
107
106
ELECTRONIC MONEY CARD
102
SHOP A
108
ELECTRONIC MONEY RECEIVING /PAYING MACHINE
USER
107
106
ELECTRONIC MONEY CARD

FIG.1

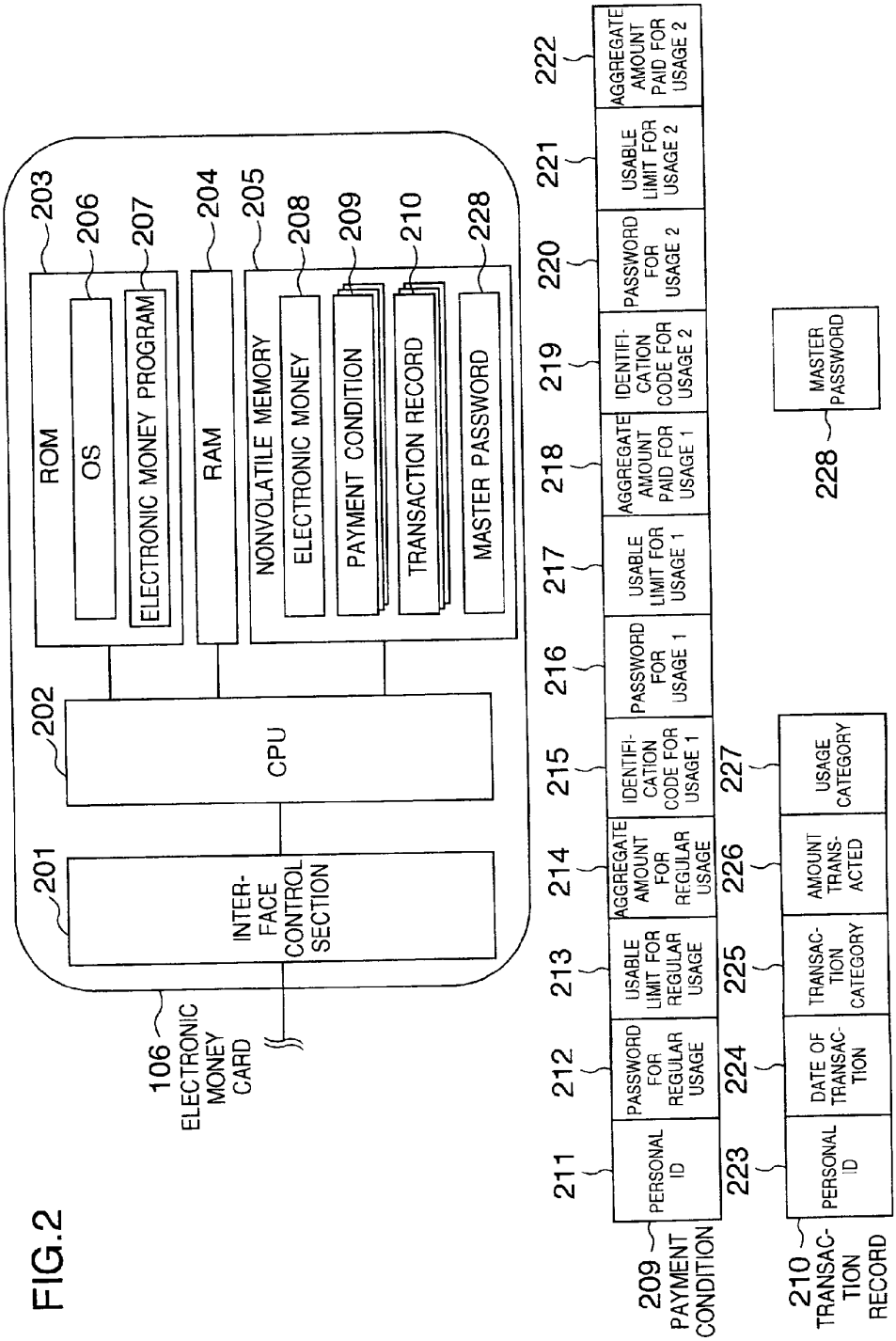

106
ELECTRONIC MONEY CARD
201
INTER-FACE CONTROL SECTION
202
CPU
203
ROM
206
OS
207
ELECTRONIC MONEY PROGRAM
204
RAM
205
NONVOLATILE MEMORY
208
ELECTRONIC MONEY
209
PAYMENT CONDITION
210
TRANSACTION RECORD
228
MASTER PASSWORD
209
PAYMENT CONDITION
211
PERSONAL ID
212
PASSWORD FOR REGULAR USAGE
213
USABLE LIMIT FOR REGULAR USAGE
214
AGGREGATE AMOUNT FOR REGULAR USAGE
215
IDENTIFI-CATION CODE FOR USAGE 1
216
PASSWORD FOR USAGE 1
217
USABLE LIMIT FOR USAGE 1
218
AGGREGATE AMOUNT PAID FOR USAGE 1
219
IDENTIFI-CATION CODE FOR USAGE 2
220
PASSWORD FOR USAGE 2
221
USABLE LIMIT FOR USAGE 2
222
AGGREGATE AMOUNT PAID FOR USAGE 2
210
TRANSAC-TION RECORD
223
PERSONAL ID
224
DATE OF TRANSAC-TION
225
TRANSAC-TION CATEGORY
226
AMOUNT TRANS-ACTED
227
USAGE CATEGORY
228
MASTER PASSWORD

FIG.2

FIG.3

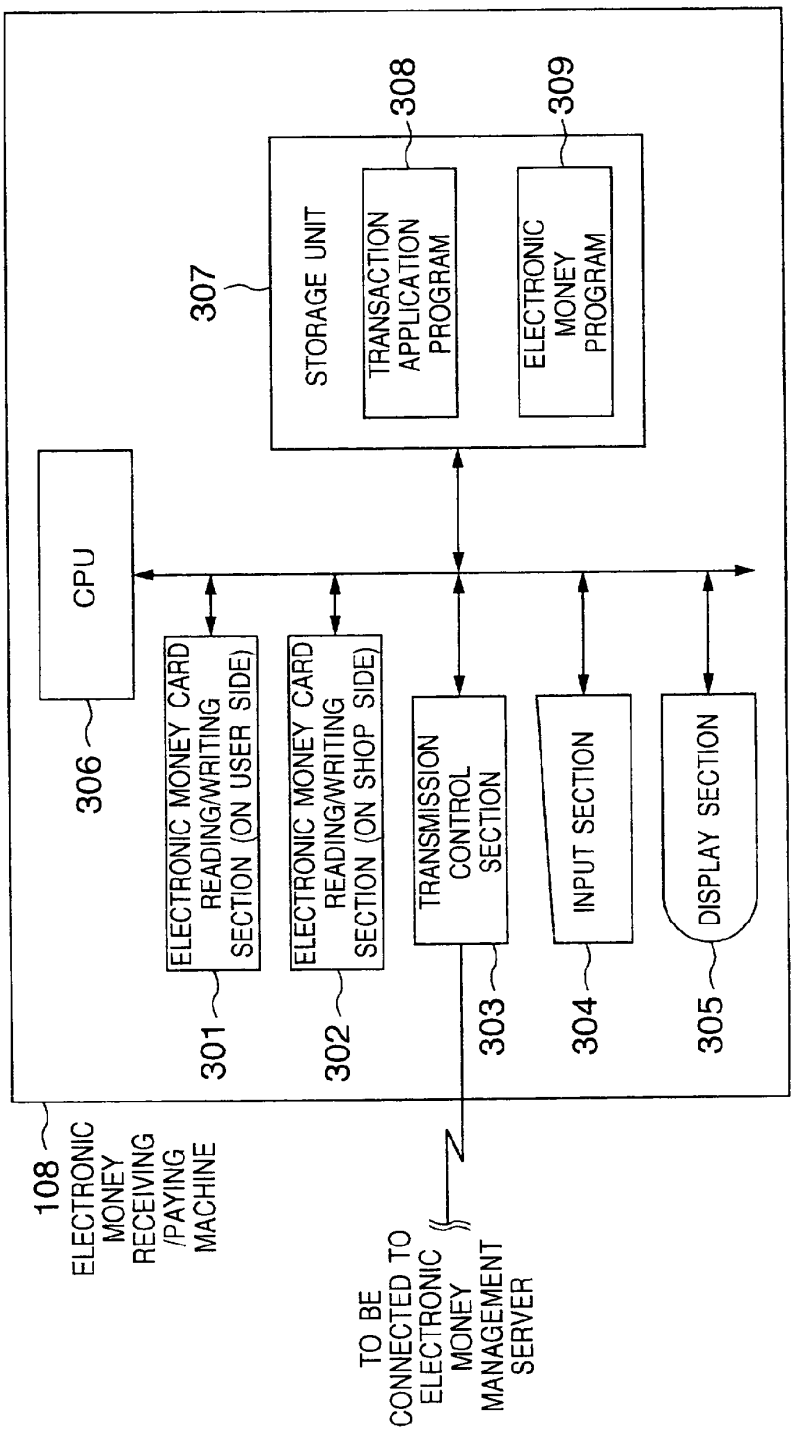

108
ELECTRONIC MONEY RECEIVING /PAYING MACHINE
TO BE CONNECTED TO ELECTRONIC MONEY MANAGEMENT SERVER
306
CPU
307
STORAGE UNIT
308
TRANSACTION APPLICATION PROGRAM
309
ELECTRONIC MONEY PROGRAM
301
ELECTRONIC MONEY CARD READING/WRITING SECTION (ON USER SIDE)
302
ELECTRONIC MONEY CARD READING/WRITING SECTION (ON SHOP SIDE)
303
TRANSMISSION CONTROL SECTION
304
INPUT SECTION
305
DISPLAY SECTION

FIG.4

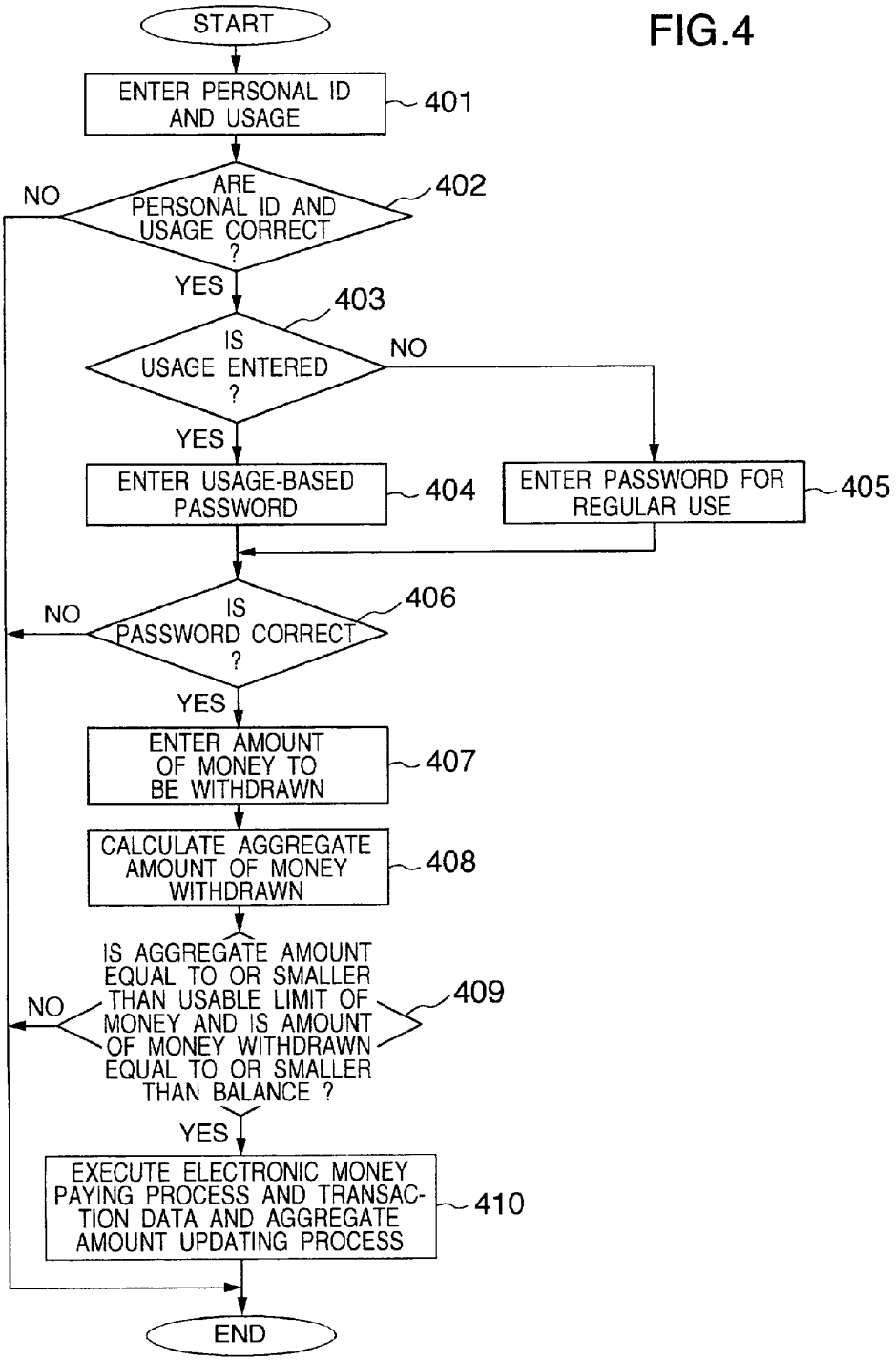

START
ENTER PERSONAL ID AND USAGE
401
ARE PERSONAL ID AND USAGE CORRECT ?
402
NO
YES
IS USAGE ENTERED ?
403
NO
YES
ENTER USAGE-BASED PASSWORD
404
ENTER PASSWORD FOR REGULAR USE
405
IS PASSWORD CORRECT ?
406
NO
YES
ENTER AMOUNT OF MONEY TO BE WITHDRAWN
407
CALCULATE AGGREGATE AMOUNT OF MONEY WITHDRAWN
408
IS AGGREGATE AMOUNT EQUAL TO OR SMALLER THAN USABLE LIMIT OF MONEY AND IS AMOUNT OF MONEY WITHDRAWN EQUAL TO OR SMALLER THAN BALANCE ?
409
NO
YES
EXECUTE ELECTRONIC MONEY PAYING PROCESS AND TRANSACTION DATA AND AGGREGATE AMOUNT UPDATING PROCESS
410
END

FIG.5

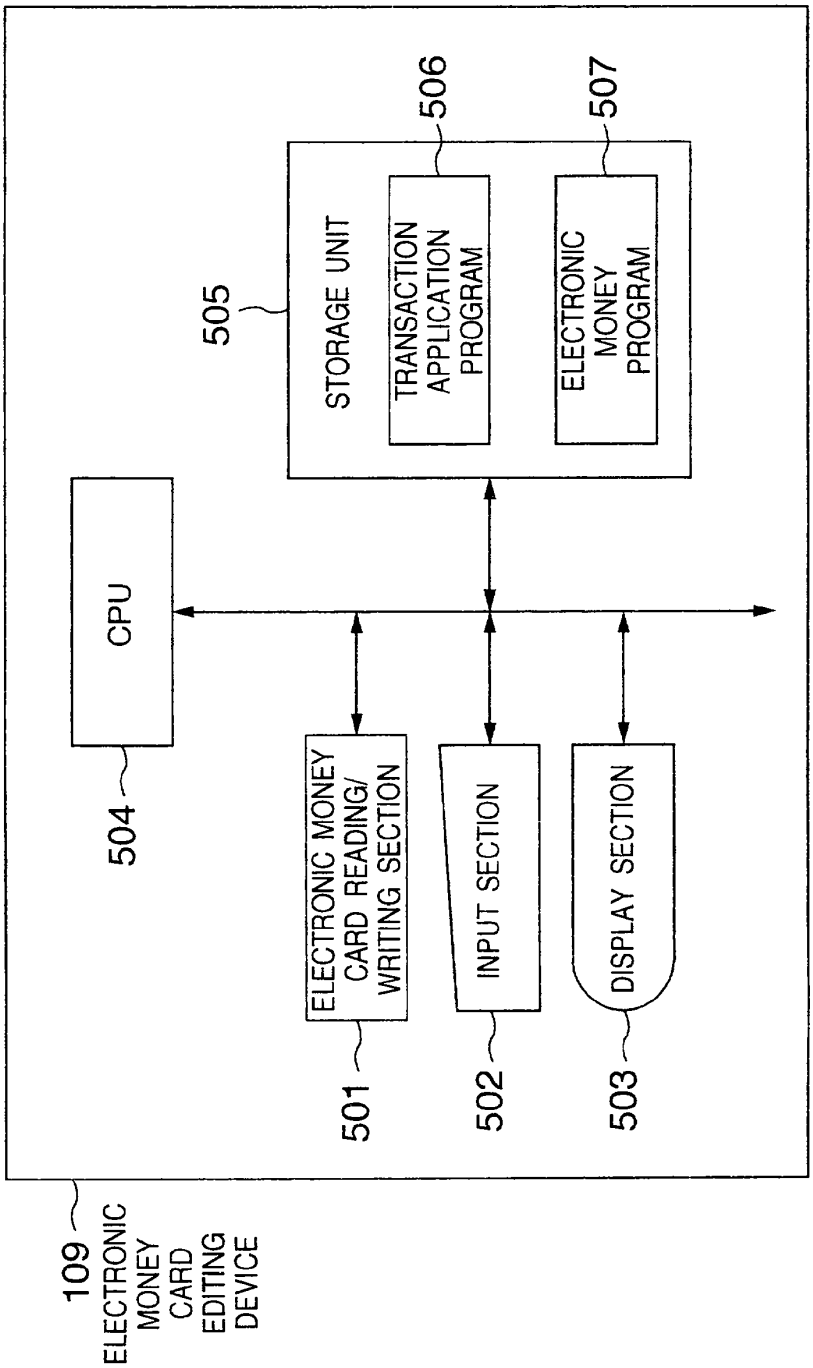
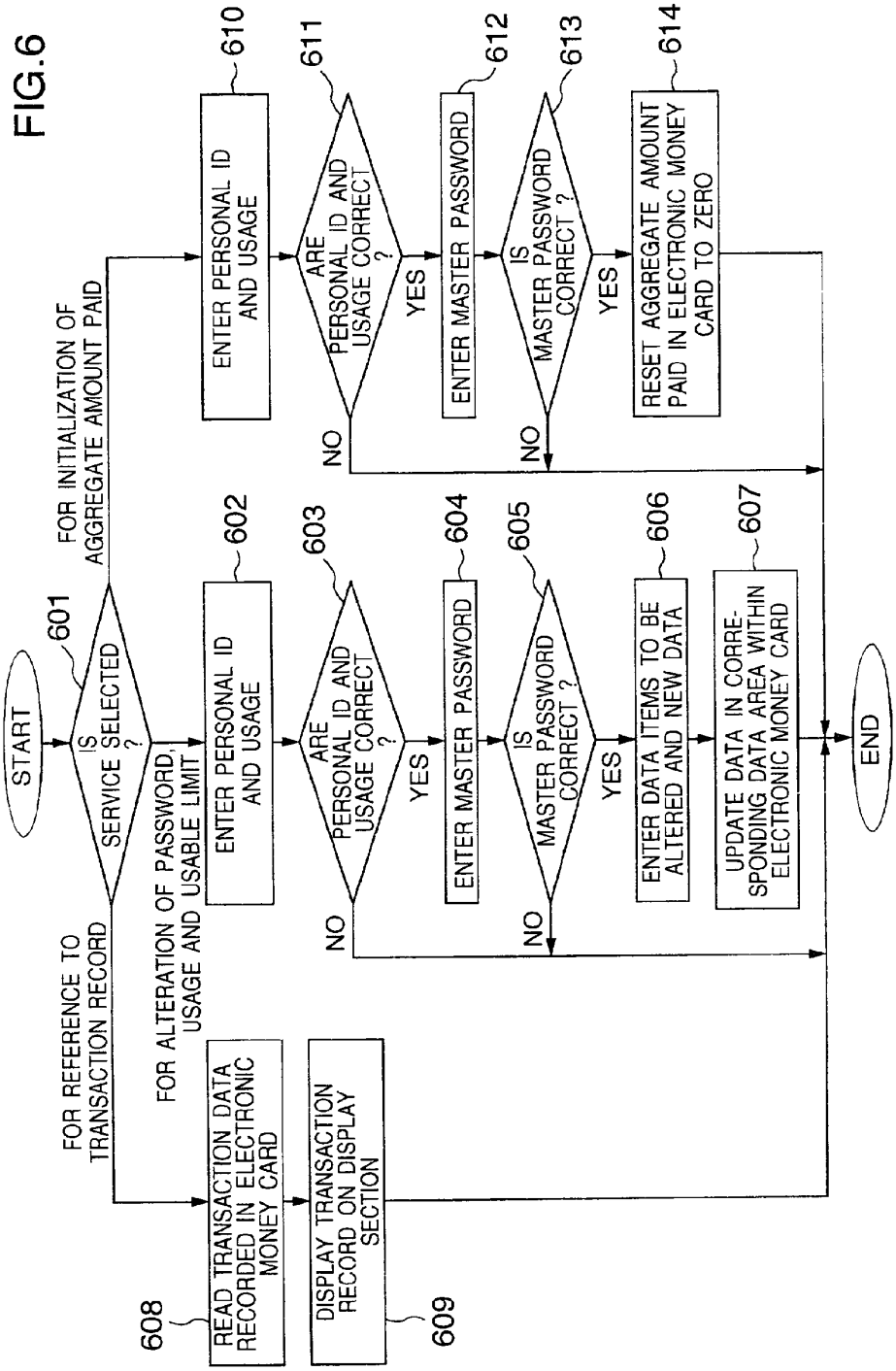

109
ELECTRONIC MONEY CARD EDITING DEVICE
504
CPU
505
STORAGE UNIT
506
TRANSACTION APPLICATION PROGRAM
507
ELECTRONIC MONEY PROGRAM
501
ELECTRONIC MONEY CARD READING/ WRITING SECTION
502
INPUT SECTION
503
DISPLAY SECTION

FIG.6


START
601
IS SERVICE SELECTED ?
FOR REFERENCE TO TRANSACTION RECORD
FOR ALTERATION OF PASSWORD, USAGE AND USABLE LIMIT
FOR INITIALIZATION OF AGGREGATE AMOUNT PAID
602
ENTER PERSONAL ID AND USAGE
603
ARE PERSONAL ID AND USAGE CORRECT ?
YES
NO
604
ENTER MASTER PASSWORD
605
IS MASTER PASSWORD CORRECT ?
YES
NO
606
ENTER DATA ITEMS TO BE ALTERED AND NEW DATA
607
UPDATE DATA IN CORRESPONDING DATA AREA WITHIN ELECTRONIC MONEY CARD
608
READ TRANSACTION DATA RECORDED IN ELECTRONIC MONEY CARD
609
DISPLAY TRANSACTION RECORD ON DISPLAY SECTION
610
ENTER PERSONAL ID AND USAGE
611
ARE PERSONAL ID AND USAGE CORRECT ?
YES
NO
612
ENTER MASTER PASSWORD
613
IS MASTER PASSWORD CORRECT ?
YES
NO
614
RESET AGGREGATE AMOUNT PAID IN ELECTRONIC MONEY CARD TO ZERO
END

ELECTRONIC MONEY CARD, ELECTRONIC MONEY RECEIVING/PAYING MACHINE, AND ELECTRONIC MONEY CARD EDITING DEVICE.

BACKGROUND OF THE INVENTION

[0001] The present invention relates to an electronic money card for dealing with money electronically, an electronic money receiving/paying machine for reading and writing electronic money from and to the electronic money card, and an electronic money card editing device for allowing a user, e.g, to refer to information stored in the electronic money card.

[0002] An electronic money card has a recording of money in the form of electronic cash in a memory built in an IC chip of an IC card. When a user stores electronic money in a recording area of a memory or withdraws the electronic money from the recording area, a certification number specific to the IC card or a password the user has for his account in a banking organ is used as a condition for payment with the card.

[0003] However, the aforementioned electronic money card certifies the user with a single password, and under this procedure, any user who knows the password can withdraw the total amount of electronic money stored in the electronic money card at once. Thus, when the user lends his electronic money card to or shares it with other people, the users must use the electronic money within the portions of a usable limit they mutually agreed upon, respectively. In addition, it is necessary to prepare a management ledger such as an account book to keep a record of used electronic money data.

SUMMARY OF THE INVENTION

[0004] The object of the present invention is to provide an electronic money card capable of storing usable limits of electronic money and passwords on a user or a usage basis and storing a transaction record including items indicating users and usages, an electronic money receiving/paying machine capable of receiving and paying electronic money to and from the electronic money card, and an electronic money card editing device allowing a user to refer to the transaction record stored in the electronic money card and to alter identifiers, usable limits of electronic money and passwords set on a usage basis.

[0005] To achieve the above object, the present invention provides an electronic money card, in which a storage section of the card has an area for storing a restricting condition for the withdrawal of electronic money and in which a logic is provided so that a user is allowed to read or write the electronic money stored in the electronic money card based on such condition.

[0006] The present invention further provides an electronic money receiving/paying machine that allows a user to receive or pay electronic money based on a restricting condition set in an electronic money card when the machine performs a receiving and paying process with the electronic money card in accordance with a message displayed on a display section of the machine.

[0007] The present invention still provides an electronic money card editing device that allows a user to refer to a transaction record in the electronic money card and to alter passwords, usages and usable limits in accordance with a message displayed on a display section of the device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] **FIG. 1** is a diagram showing an exemplary organization of an electronic money system using an electronic money card, an electronic money receiving/paying machine and an electronic money card editing device;

[0009] **FIG. 2** is a diagram showing an exemplary structure of an electronic money card for storing electronic money;

[0010] **FIG. 3** is a diagram showing an exemplary configuration of an electronic money receiving/paying machine installed in a shop for performing the receiving and paying operation with respect to the electronic money card;

[0011] **FIG. 4** is an exemplary flowchart showing an electronic money transaction provided by a transaction application program of the electronic money receiving/paying machine;

[0012] **FIG. 5** is a diagram showing an exemplary configuration of an electronic money card editing device which is possessed by a user and allows the user to refer to a transaction record stored in the electronic money card and by which the user can update a payment condition; and

[0013] **FIG. 6** is an exemplary flowchart showing a process provided by a transaction application program of the electronic money card editing device.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0014] Embodiments of the present invention will now be described with reference to the drawings.

[0015] **FIG. 1** is an exemplary organization of an electronic money system using an electronic money card, an electronic money receiving/paying machine using the electronic money card, and an electronic money card editing device for editing conditions and the like which are set for using the electronic money card.

[0016] When a user **107** uses an electronic money card **106** in order to pay the price for a service received at a shop **102** (among a plurality of shops A, B and so on), the user **107** inserts the electronic money card **106** into an electronic money receiving/paying machine **108** installed at the shop **102** to read electronic money stored in the card **106**. The electronic money receiving/paying machine **108** then writes the read electronic money into a shop's electronic money card (not shown) that has already been inserted into the machine **108**. A transaction is established between the user **107** and the shop **102** in this way.

[0017] Further, when the shop **102** deposits the electronic money accumulated in the shop's electronic money card to an account the shop **102** has with a banking organ **101**, the electronic money receiving/paying machine **108** reads the electronic money stored in the shop's electronic money card and transmits the read electronic money to an electronic money management server **104** installed at the banking organ **101**. The electronic money management server **104** requests an accounting system **105** installed at the banking organ **101** to follow a procedure for depositing an amount of

money equivalent to the received electronic money into the account of the shop **102**. When the accounting system **105** completes the depositing procedure, the electronic money receiving process is complete.

[**0018**] **FIG. 2** is a diagram showing a configuration of the electronic money card **106** shown in **FIG. 1**. When the electronic money card **106** is inserted into the electronic money receiving/paying machine **108** or an electronic money card editing device **109** (hereinafter referred to as the "control unit"), the electronic money card **106** is activated in response to an electronic signal supplied through an interface control section **201**. With the electronic money card **106** activated, an OS (operating system) **206** and an electronic money program **207** that are stored in a ROM **203** are loaded to a RAM **204**. As a result, a CPU **202** is allowed to read and write the data in the RAM **204** and a nonvolatile memory **205** in accordance with a command from the control unit received through the interface control section **201**. For example, when a command for withdrawing or storing electronic money **208** is received from the interface control section **201**, the CPU **202** rewrites data of the electronic money **208** recorded in the nonvolatile memory **205** in accordance with a logic described in the electronic money program **207**.

[**0019**] The nonvolatile memory **205** has a storage area **209** (hereinafter referred to as the "payment condition **209**") for recording a personal ID **211** set on a user basis, usage identification codes **215** and **219**, passwords **212**, **216** and **220** set on a usage basis, usable limits **213**, **217** and **221**, and aggregate amounts **214**, **218** and **222**. The usage identification code indicates what purpose a user uses the electronic money card **106** for. The usable limit indicates the maximum limit of electronic money the user can withdraw. The aggregate amount indicates a total sum of electronic money read from the electronic money card. Further, the electronic money program **207** has logics that allow the user to perform processes such as withdrawing electronic money and editing the electronic money card using the payment condition **209** and a master password **228** as permitting conditions. That is, one of the logics requires the payment condition **209** as permission to allow the user to read the electronic money, and the other logic requires the master password **228** as permission to allow the user to rewrite the payment condition **209**.

[**0020**] Further, the nonvolatile memory **205** additionally includes a storage area **210** (hereinafter referred to as the "transaction record **210**") for recording a user's personal ID **223**, a transaction date **224**, a transaction category **225**, an amount transacted **226**, and a usage category **227**. The transaction date **224** indicates the year, month and day in which the electronic money is read and written. The transaction category **225** indicates the reading or writing of electronic money. The amount transacted **226** indicates a volume of electronic money read or written. The usage category **227** indicates the purpose for which the electronic money is used. The nonvolatile memory **205** stores a record of electronic money and the like therein in accordance with a logic given to the electronic money program **207**. That is, the logic causes the program **207** to record transaction data in the transaction record **210** after the program **207** has read or written the electronic money.

[**0021**] As described above, the condition of usable limit is defined for each usage in the electronic money card. Therefore, even if there is a positive balance in the user's electronic money account, the user is prohibited from performing a payment process, such as in purchasing an article, using the electronic money **208** exceeding the usable limit. Hence, even if a third party happens to know a password corresponding to a usage, such third party, not knowing passwords corresponding to other usages, can use the electronic money for only one usage, and this means that the damage suffered by the user could be minimized with only a minimum amount of money illegally used by the third party. In other words, the electronic money card of the present invention provides the advantage of minimizing illegal use of electronic money.

[**0022**] **FIG. 3** shows an exemplary configuration of the electronic money receiving/paying machine **108** shown in **FIG. 1**.

[**0023**] A process for receiving or paying electronic money involves the step of transferring the electronic money from the electronic money card **106** possessed by the user **107** to the electronic money card possessed by the shop **102** or vice versa. First, a transaction application program **308** that controls electronic money receiving and paying transactions displays on a display section **305** an instruction prompting the user **107** to insert the user's electronic money card **106** into an electronic money card reading/writing section **301** on the user side and an instruction prompting the shop **102** to insert the shop's electronic money card into an electronic money card reading/writing section **302** on the shop side. After the user **107** and the shop **102** finish inserting their electronic money cards, the transaction application program **308** displays on the display section **305** an instruction prompting the user **107** to enter a group of data which includes an amount of money equivalent to a service the user received from the shop, a password certifying that the user **107** is a legitimate user of the electronic money card **106**, a personal ID identifying the user **107** and an identification code specifying a usage of the electronic money. As a result, the program **308** receives such group of data from the user **107** via an input section **304**. Then, the transaction application program **308** gives an electronic money program **309** a command and the group of data received from the input section **304**. The command causes the program **309** to transfer electronic money equivalent to the amount of money received from the input section **304** from the user's electronic money card **106** to the shop's electronic money card. Successively, in response to the command from the transaction application program **308**, the electronic money program **309** transfers the electronic money to the shop's electronic money card from the user's electronic money card **106**. The group of data transferred at this time is delivered to the electronic money program **207** stored in the user's electronic money card **106** and used as permission to perform the electronic money payment process described with reference to **FIG. 2**, i.e., as the condition set by the usage identification code **215**, the password **216** and the like.

[**0024**] In a process through which the shop deposits the electronic money stored in the shop's electronic money card in an account the shop **102** has with the banking organ **101**, the transaction application program **308** gives the electronic money program **309** a command for withdrawing the electronic money from the shop's electronic money card, and the electronic money program **309** transfers the withdrawn

electronic money to the electronic money management server **104** from a communication control section **303**.

[**0025**] **FIG. 4** is a flowchart showing an exemplary electronic money payment transaction provided by the transaction application program **308** of the electronic money receiving/paying machine **108**. A CPU **306** controls the transaction.

[**0026**] First, the user **107** enters a personal ID that identifies the user **107** and a usage of electronic money from the input section **304** (Step **401**). The transaction application program **308** checks the validity of the entered data (Step **402**). The checking process is performed when the electronic money program **309** of the electronic money receiving/paying machine **108** gives the electronic money program **207** of the electronic money card **106** an instruction for checking the entered data. On the other hand, the electronic money program **207** of the electronic money card **106** determines the validity of the received input data by comparing such received input data with the personal ID **211** and the usage-based identification codes **215** and **219** which are defined as the payment condition **209** in the nonvolatile memory **205**.

[**0027**] Next, the program **308** asks the input section **304** of the electronic money receiving/paying machine **108** if the user has entered the usage (Step **403**). If the answer is affirmative, the program **308** prompts the user to enter a usage-based password (Step **404**), whereas if the answer is negative, the program **308** prompts the user to enter a regular password (Step **405**). Then, the validity of the entered password is checked in accordance with the type of password, either usage-based or regular (Step **406**). The electronic money program **207** of the electronic money card **106** makes the validity check by comparing the entered password with the passwords **212**, **216** and **220** defined as the payment condition **209**.

[**0028**] If the entered password is found to be correct, an amount of electronic money **208** withdrawable from the electronic money card **106** within the usable limit **213**, **217** or **221** corresponding to the entered usage is obtained (Step **407**). Then, the amount of money withdrawn is added to the aggregate amount of electronic money so far paid **214**, **218** or **222** (Step **408**), and the obtained sum is compared with both the electronic money balance and the usable limit **213**, **217** or **221** in the electronic money card (Step **409**). If the sum is equal to or smaller than the balance and the usable limit **213**, **217** or **221**, the user is permitted to make payment in electronic money, so that the electronic money is withdrawn, and the payment transaction is terminated after a recording of transaction data is made (Step **410**). The transaction data includes the personal ID **223**, the date **224** in which the transaction is performed, the transaction category **225** that specifies the type of transaction, either receipt or payment, the amount of money transacted **226**, and the usage category **227** that indicates identification codes defined on a usage basis. When such transaction data is written into the transaction record **210** of the electronic money card **106**, a payment transaction is terminated.

[**0029**] The comparison process in Step **409** will be described more specifically. That is, the following describes in more detail the process of comparing the amount of money withdrawn to be added (or the amount of money to be paid which is to be added to the aggregate amount of electronic money paid shown in **FIG. 2**) with the electronic money balance in the electronic money card **106** and the usable limit **213**, **217** or **221** defined as the payment condition **209**. The usable limit means the maximum limit of electronic money set for each usage as described above. For example, if a user withdraws electronic money many times, the amount of money withdrawn is added up every time the withdrawing operation is performed. That is, under this procedure, the user is required to receive and pay the electronic money within a usable limit. Thus, not only the amounts of money withdrawn by the user is compared with the usable limit, but also the sum of the amount of money currently withdrawn and the aggregate amount of money so far paid is compared with the usable limit. On the other hand, in case the electronic money balance is insufficient, the amount of money to be added is compared with the current electronic money balance so that the user can perform transactions within the electronic money currently available as the balance. Thus, whether the user can withdraw the electronic money from his electronic money card or not is determined by making these comparisons.

[**0030**] Further, the steps described with reference to **FIG. 4** are not necessarily taken in the order they are mentioned. For example, the object of the present invention can be achieved by executing the usage-related steps (Steps **401** to **403**) after checking the balance in the electronic money card (Step **409**). The same applies to the flow of steps shown in **FIG. 6**.

[**0031**] **FIG. 5** is a diagram showing a configuration of the electronic money card editing device **109**.

[**0032**] A transaction application program **506** of the electronic money card editing device **109** provides a reference service and two types of rewriting services. The reference service allows a user to refer to the transaction record **210** stored in the electronic money card **106**. One of the rewriting services allows the user to rewrite the passwords **212**, **216** and **220** set on a usage basis, and the usage identification codes **215** and **219** and usable limits **213**, **217** and **221** recorded in the electronic money card **106**. The other rewriting service allows the user to reset to zero the aggregate amounts of electronic money paid **214**, **218** and **222** recorded in the electronic money card **106** on a user and a usage basis. An electronic money program **507** executes a process for reading and writing the payment condition **209** recorded in the electronic money card **106** and a process for reading the transaction record **210** stored in the card **106**. The user **107** inserts the electronic money card **106** to an electronic money card reading section **501** and enters data necessary for receiving desired services from an input section **502** in accordance with instructions displayed on a display section **503**.

[**0033**] **FIG. 6** is a flowchart showing how the services are provided by the transaction application program **506** of the electronic money card editing device **109**. A CPU **504** mainly controls the following processes.

[**0034**] First, the transaction application program **506** of the electronic money card editing device **109** displays on the display section **503** a message instructing the user **107** to select a service (Step **601**).

[**0035**] If the service for referring to the transaction record is selected from the input section **502**, the process for

reading the transaction record is executed (Step **608**). The transaction record is read when the electronic money program **507** applies to the electronic money program **207** stored in the electronic money card **106** a command for reading the transaction record **210** stored in the nonvolatile memory **205**. In response to the command, the electronic money program **207** of the electronic money card **106** reads a data table of the transaction record **210** and delivers the read data table to the transaction application program **506** through the electronic money program **507**. Then, the data table of the transaction record **210** is displayed on the display section **503** (Step **609**).

[**0036**] On the other hand, if the service for rewriting a password, a usage, and a usable limit of money is selected from the input section **502**, the user is requested to enter a personal ID and a usage (Step **602**). The entered data are delivered to the electronic money program **207** of the electronic money card **106** and used to select items to be rewritten from a data table of the payment condition **209**. Upon detection of the data that coincides with the entered data (Step **603**), the user **107** is requested to enter a master password given to a manager of the electronic money card **106** (the manager is one of the users **107** who is authorized to rewrite the payment condition **209**) (Step **604**). This step is effective in prohibiting a current possessor of the electronic money card **106** from altering any part of the payment condition **209** specified by others when the electronic money card **106** is lent to or shared among a plurality of people. The entered password is compared with the master password **228** of the electronic money card **106** (Step **605**). When both passwords coincide with each other, the user **107** is permitted to enter new data (updated data) (Step **606**). Then, the entered new data is delivered to the electronic money program **207** so that the data is rewritten (Step **607**). If the passwords do not coincide in Step **605**, the user cannot alter data (various conditions) in the electronic money card **106**.

[**0037**] On the other hand, when the user selects the service for resetting the aggregate amounts of money paid to zero, the user is requested to enter a usage, a password and the like as the user is so requested in the process described with respect to receiving the service for rewriting a password, a usage and a usable limit (Steps **610**, **611**, **612** and **613**). When the rewriting of the payment condition **209** recorded in the nonvolatile memory **205** of the electronic money card **106** is permitted, the aggregate amounts of money paid **214**, **218** and **222** are reset to zero (Step **614**). The reason why the aggregate amounts of money paid in the electronic money card are reset to zero is to avoid the inconvenience of prohibiting a legitimate user from legally using the electronic money card. That is, the legitimate user is no longer permitted to use the electronic money card if his electronic money payments exceed the usable limits as each payment is accumulated in the aggregate amounts in the electronic money card.

[**0038**] The present invention will be described more specifically. Let us take an example in which a plurality of people share a single card in common: e.g., family members such as the farther, the mother, an elder brother, a younger sister share a card, and company staff members such as a general manger, a manager, employees share a card. In these cases, the card can be used flexibly by setting on an individual member basis such usage-based conditions as passwords and identification codes defined in the payment condition **209** which is described with reference to **FIG. 2**. In addition, the card allows each member user to set conditions on a usage basis, such as the purchasing of books, foods or clothes.

[**0039**] While the processes (described especially with reference to **FIGS. 4 and 6**) of the electronic money card, the electronic money receiving/paying machine and the electronic money card editing device are performed chiefly under the control of the CPUs respectively equipped with the electronic money receiving/paying machine and the electronic money card editing device, it goes without saying that the CPU arranged in the electronic money card can control these processes. It may be noted that each of these CPUs is termed a "control section."

[**0040**] According to the present invention, an electronic money card allows a plurality of users to record their individual usable limits and passwords of electronic money on a usage basis, and the electronic money card prohibits the use of the electronic money in amounts exceeding the usable limits unless the manager of the electronic money card who has the master password is asked to reset the aggregate amounts of electronic money paid to zero. As a result of the present invention, a single electronic money card can be shared in common among a plurality of people, and thus the invention contributes to the promotion of a planned use of the electronic money card among family members or in corporate organizations.

[**0041**] Furthermore, the electronic money stored in the electronic money card is managed on the basis of a plurality of usable limits and passwords. Therefore, even if a certain password is leaked to a third party, the advantage of improving safety is provided in the sense that the third party cannot withdraw all the electronic money available in the card at once.

1. An electronic money card for transacting electronic money, comprising:

a control section and a storage section, wherein

the storage section stores data of the electronic money, a plurality of pieces of identification data for identifying usages to be specified when the electronic money card is used, and usable limit data for limiting an amount of electronic money to be used in correspondence with each piece of identification data, and wherein

the control section compares a piece of identification data received from outside the electronic money card with each of the pieces of identification data stored in the storage section upon request for payment and permits the payment in electronic money within the usable limit of the electronic money limited by the piece of identification data when the compared pieces of identification data coincide with each other.

2. An electronic money card according to claim 1, wherein

the storage section stores a password set to correspond to a piece of identification data, and

the control section permits payment in electronic money when a password received from outside the electronic money card coincides with the password stored in the storage section.

3. An electronic money card according to claim 1, wherein

the storage section stores an aggregate amount obtained by the control section adding up a total amount of electronic money paid every time the electronic money is paid.

4. An electronic money card according to claim 1, wherein

the storage section stores a transaction record in which transaction data are recorded when the control section performs an electronic money transaction.

5. An electronic money card according to claim 1, wherein

the control section updates the piece of identification data when instructed to update the piece of identification data stored in the storage section.

6. An electronic money card according to claim 5, wherein

the storage section stores a master password for giving permission to alter data stored in the storage section, and

the control section updates the piece of identification data when a password to be entered coincides with the master password.

7. An electronic money transaction apparatus for performing an electronic money transaction with an electronic money card for storing electronic money therein, comprising:

a CPU, an input section, and a display section, wherein

the CPU displays a message prompting a user to enter a usage of the electronic money card on the display section upon request for a transaction using the electronic money and performs an electronic money transaction with the electronic money card based on the usage entered from the input section.

8. An electronic money transaction apparatus according to claim 7, wherein

the CPU displays a message prompting a user to enter a password set in accordance with a usage on the display section and permits a transaction with the electronic money card when the password entered from the input section coincides with a password set in the electronic money card.

9. An electronic money transaction apparatus according to claim 7, wherein

the CPU stops a transaction with the electronic money card when an amount of electronic money for payment to be entered from the input section is greater than an electronic money balance in the electronic money card.

10. An electronic money transaction apparatus according to claim 7, wherein

the CPU stops a transaction with the electronic money card when an amount of electronic money for payment to be entered from the input section is greater than a usable limit set in the electronic money card.

11. An electronic money transaction apparatus according to claim 7, wherein

the CPU sums an amount of electronic money transacted in the electronic money card as an aggregate amount every time an electronic money transaction is performed with the electronic money card.

12. An electronic money transaction apparatus according to claim 11, wherein

the CPU stops a transaction with the electronic money card when a sum of an amount of electronic money for payment to be entered from the input section and the aggregate amount in the electronic money card is greater than an electronic money balance in the electronic money card.

13. An electronic money transaction apparatus according to claim 11, wherein

the CPU stops a transaction with the electronic money card when a sum of an amount of electronic money for payment to be entered from the input section and the aggregate amount in the electronic money card is greater than a usable limit set in the electronic money card.

14. An electronic money card editing device for editing an electronic money card, comprising:

a display section for displaying a message prompting a user to select a service from a plurality of services;

an input section for detecting selection of the service in accordance with the message displayed on the display section;

a reading/writing section for reading and writing data of the electronic money card; and

a CPU, wherein

the CPU detects selection of a service for editing data in the electronic money card made from the input section and, when the service is for altering a usage of the electronic money card, updates data indicating the usage stored in the electronic money card through the reading/writing section.

15. An electronic money card editing device according to claim 14, wherein

when the service is for altering a usable limit of the electronic money card, the CPU updates the usable limit set in the electronic money card through the reading/writing section.

16. An electronic money card editing device according to claim 14, wherein

the CPU displays a message prompting a user to select a service from a plurality of services on the display section, displays on the display section a password for permitting the user to edit data in the electronic money card when an instruction for editing the data in the electronic money card is received from the input section, and permits the user to edit the data in the electronic money card when a password entered from the input section coincides with a master password obtained through the reading/writing section.

17. An electronic money card editing device according to claim 14, wherein

when the service is for referring to a transaction record in the electronic money card, the CPU reads the transaction record in the electronic money card through the reading/writing section and displays data of the read transaction record on the display section.

18. An electronic money card editing device according to claim 14, wherein

when the service is for initializing the aggregate amounts of electronic money summed up in the electronic money card, the CPU resets the aggregate amounts stored in the electronic money card to zero through the reading/writing section.

19. A method of performing an electronic money transaction using an electronic money card, comprising the steps of:

storing electronic money data in the electronic money card, a plurality of pieces of identification data for identifying usages to be specified when the electronic money card is used, and usable limit data for limiting an amount of electronic money to be used in correspondence with each piece of identification data;

comparing a piece of identification data received from outside the electronic money card with each of the pieces of identification data stored in the storage section upon request for payment; and

permitting the payment in electronic money within the usable limit of electronic money limited in correspondence with the piece of identification data when the compared pieces of data coincide with each other.

* * * * *

US005826243A

United States Patent [19]

Musmanno et al.

[11] **Patent Number: 5,826,243**

[45] **Date of Patent: Oct. 20, 1998**

[54] **INTEGRATED SYSTEM FOR CONTROLLING MASTER ACCOUNT AND NESTED SUBACCOUNT(S)**

[75] Inventors: **Thomas Musmanno**, Warren; **Kelly Ur**, East Brunswick, both of N.J.

[73] Assignee: **Merrill Lynch & Co., Inc.**, New York, N.Y.

[21] Appl. No.: **176,207**

[22] Filed: **Jan. 3, 1994**

[51] **Int. Cl.**[6] **G06F 12/60**

[52] **U.S. Cl.** **705/35**; 705/39

[58] **Field of Search** 364/408; 235/379; 705/35, 39

[56] **References Cited**

PUBLICATIONS

Martin F. Stankard, "Profiting from the White Collar Service Boom," National Underwriter, v90, n31, pp. 13, 17, abstract, Aug. 2, 1986.

Mitchell S. Farkas, "The Account That Transformed a Brokerage into a Bank," Financial & Accounting Systems, v6, n4, pp. 8 –12, abstract, Wintr, 1991.

Bank on Windows with Money and Quicken Computer Shopper, Feb. 1992.

Financial Managers: Keeping Track of Your Personal Accounts PC Magazine, Dec. 27, 1988.

The King of Finance Software Gets a Brand–New Face, PC–Computing, Dec. 1990.

Checkfree: The Good, The Bad and The Zealots, Home Office Computing, Sep. 1992.

Technology Shatters "Bankers Hours", Arend, Mark, ABA Banking Journal, v85,n5 , p57(4), May 1993.

"Ways to Get the Most from Your Bank", Hedberg, Augustin, Money, Mar. 1988.

Field Communications Department, Merrill Lynch; *Introducing . . .* The CMA Master Financial Service; Dec. 8, 1992; pp. 1–6.

Primary Examiner—Gail O. Hayes

Assistant Examiner—William N. Hughet

Attorney, Agent, or Firm—Hopgood, Calimafde, Kalil & Judlowe

[57] **ABSTRACT**

Data processing for an improved securities brokerage/cash management system which supervises, implements and coordinates a composite account having a master account and one or more subaccount(s). The nested subaccounts incorporate a subset of features corresponding to the specific needs dictated by the purpose of the subaccount and thus streamline system operation for the recordkeeper.

8 Claims, 4 Drawing Sheets

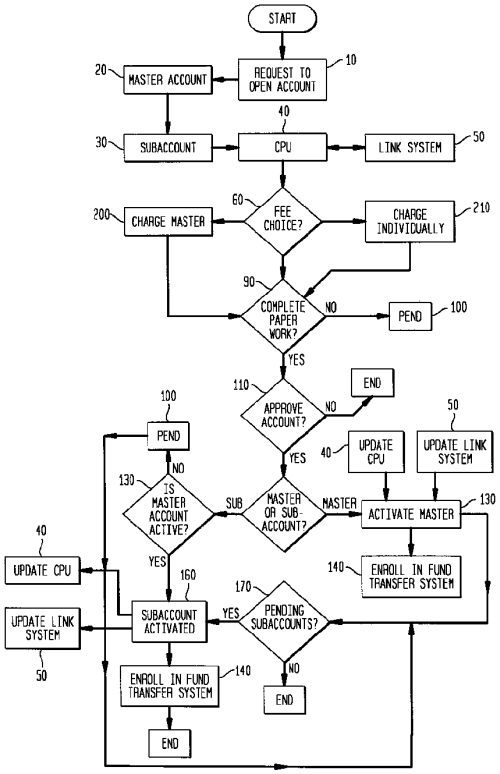


FIG. 1

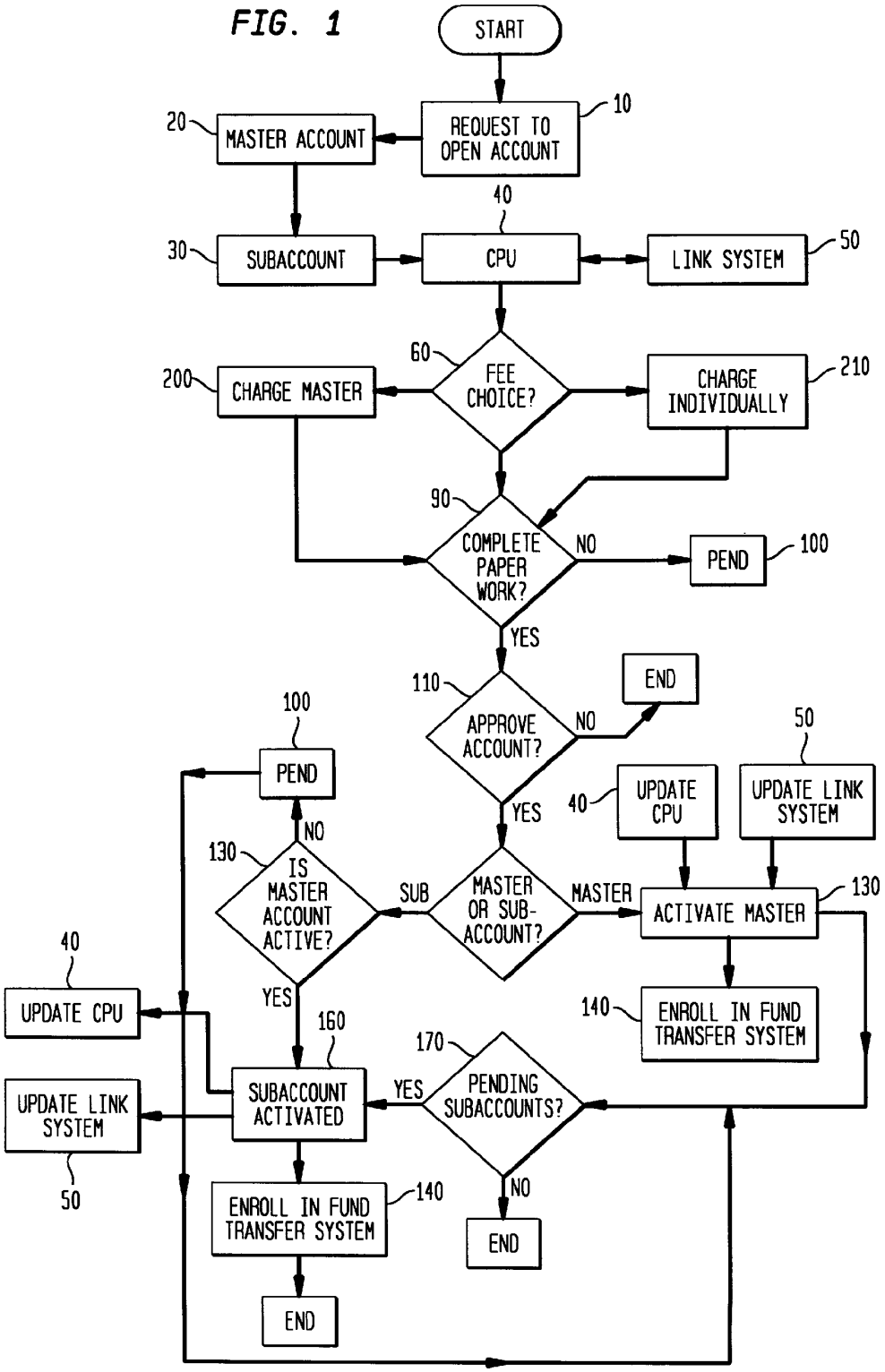

START
REQUEST TO OPEN ACCOUNT
10
MASTER ACCOUNT
20
SUBACCOUNT
30
CPU
40
LINK SYSTEM
50
FEE CHOICE?
60
CHARGE MASTER
200
CHARGE INDIVIDUALLY
210
COMPLETE PAPER WORK?
90
NO
PEND
100
YES
APPROVE ACCOUNT?
110
NO
END
YES
PEND
100
NO
IS MASTER ACCOUNT ACTIVE?
130
SUB
MASTER OR SUB-ACCOUNT?
MASTER
UPDATE CPU
40
UPDATE LINK SYSTEM
50
ACTIVATE MASTER
130
ENROLL IN FUND TRANSFER SYSTEM
140
YES
SUBACCOUNT ACTIVATED
160
PENDING SUBACCOUNTS?
170
YES
NO
END
ENROLL IN FUND TRANSFER SYSTEM
140
END
UPDATE CPU
40
UPDATE LINK SYSTEM
50

FIG. 2

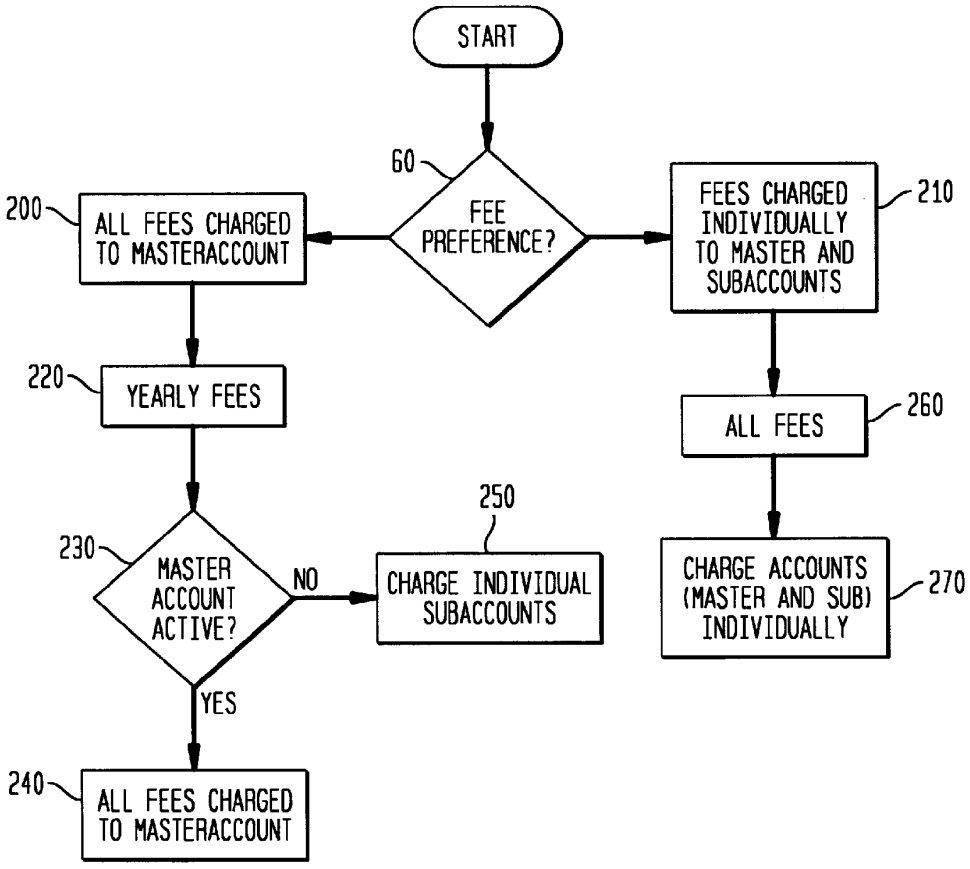

START
60
FEE PREFERENCE?
200
ALL FEES CHARGED TO MASTERACCOUNT
210
FEES CHARGED INDIVIDUALLY TO MASTER AND SUBACCOUNTS
220
YEARLY FEES
260
ALL FEES
250
230
MASTER ACCOUNT ACTIVE?
NO
CHARGE INDIVIDUAL SUBACCOUNTS
CHARGE ACCOUNTS (MASTER AND SUB) INDIVIDUALLY
270
YES
240
ALL FEES CHARGED TO MASTERACCOUNT

FIG. 3

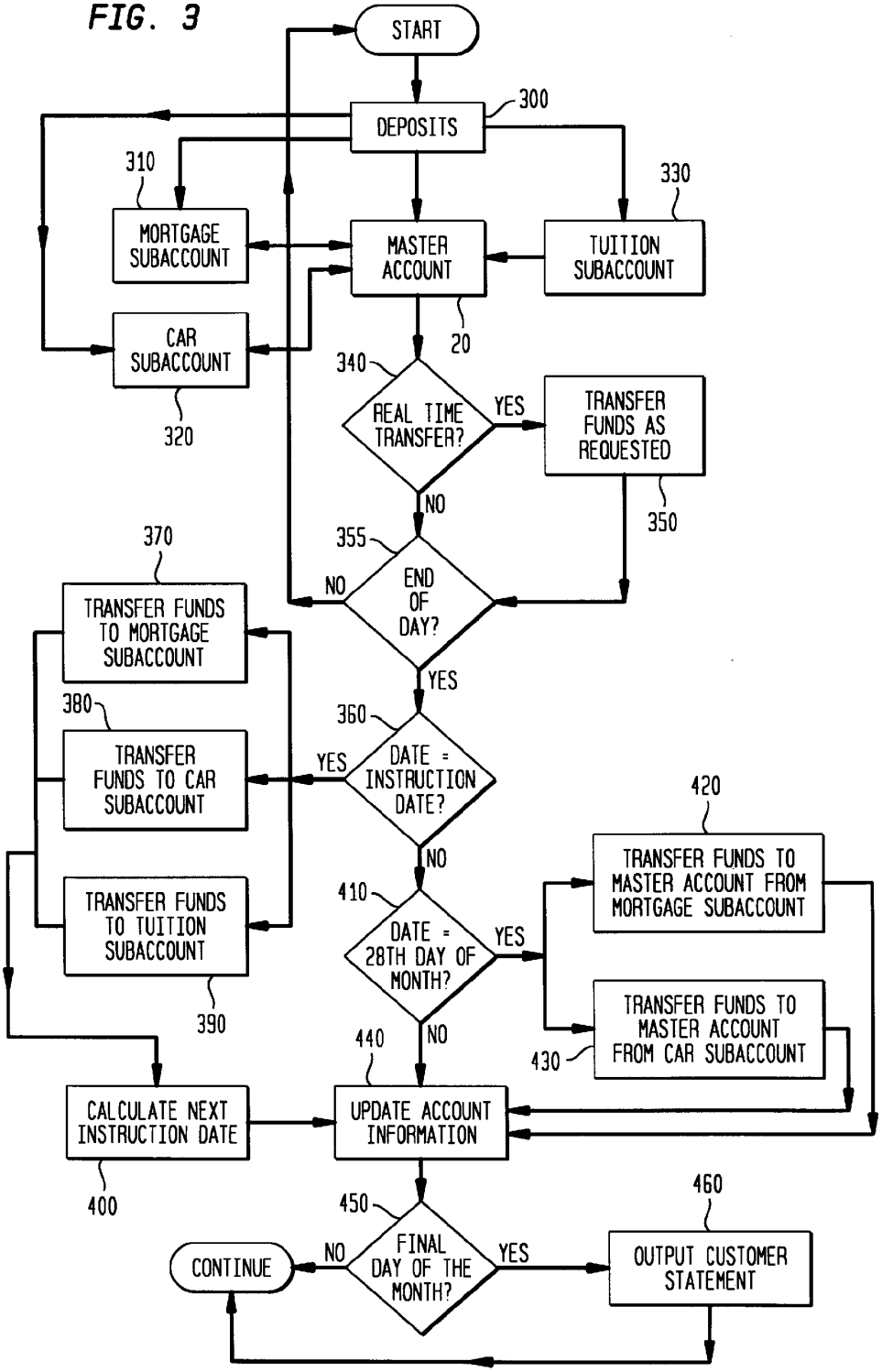
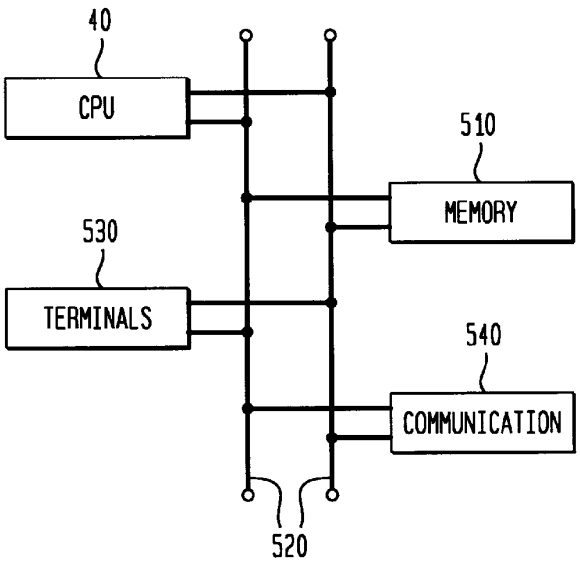

START
DEPOSITS
300
310
MORTGAGE SUBACCOUNT
330
MASTER ACCOUNT
TUITION SUBACCOUNT
20
CAR SUBACCOUNT
320
340
REAL TIME TRANSFER?
YES
TRANSFER FUNDS AS REQUESTED
350
NO
355
END OF DAY?
NO
370
TRANSFER FUNDS TO MORTGAGE SUBACCOUNT
YES
380
360
TRANSFER FUNDS TO CAR SUBACCOUNT
YES
DATE = INSTRUCTION DATE?
NO
420
TRANSFER FUNDS TO MASTER ACCOUNT FROM MORTGAGE SUBACCOUNT
410
TRANSFER FUNDS TO TUITION SUBACCOUNT
DATE = 28TH DAY OF MONTH?
YES
390
NO
TRANSFER FUNDS TO MASTER ACCOUNT FROM CAR SUBACCOUNT
430
440
CALCULATE NEXT INSTRUCTION DATE
UPDATE ACCOUNT INFORMATION
400
450
460
CONTINUE
NO
FINAL DAY OF THE MONTH?
YES
OUTPUT CUSTOMER STATEMENT

FIG. 4



INTEGRATED SYSTEM FOR CONTROLLING MASTER ACCOUNT AND NESTED SUBACCOUNT(S)

The present invention generally relates to computer managed financial business systems. More specifically the invention provides data processing methods and apparatus for directing an account management system which incorporates master accounts with a plurality of nested subaccounts having a specific subset of individual properties.

BACKGROUND OF THE INVENTION

The financial world has been enhanced by the ability to use computers to manage assets. Financial institutions extensively employ elaborate computer systems to direct and process the numerous accounts retained on behalf of the customers. These accounts routinely track individual assets for the account holder and permit timely updating thereof pursuant to transactions made by the account holders in accordance with the account restrictions. These systems are directed to accounts such as brokerage accounts wherein securities may be bought and sold with a minimal amount of paper work as the transactions and recordations thereof is fully automated within the computer.

More recently, systems have been developed that permit the integration of disparate types of accounts for a single account holder thus expanding substantially the account holders ability to control his/her assets. This is exemplified by the CMA® accounts which incorporate traditional check writing and credit/debit card features with brokerage and mutual fund accounts for a single user—integrated in a seamless fashion from the user's vantage.

The above-noted integrated account systems are best exemplified from a processing standpoint by the specific patents directed to their implementation. More particularly, U.S. Pat. Nos. 4,346,442, 4,376,978, 4,597,046 and 4,774,663 are directed to such integrated account processing by one or more digital computers and are herein incorporated by reference as if restated in full. Generally, the above-identified patents disclose a computer system for directing a plurality of securities brokerage/cash management accounts. That system, inter alia, supervises, implements and coordinates a margin securities brokerage account, and permits participation in one or more short term investments (e.g., money market or comparable funds).

In recent times, there has been an increasing desire by individual account holders to segment account functions into separately managed areas of financial interest. For example, account holders often desire the ability to provide separate account functions to other members of their families, or to separate specific expenses on an account basis, e.g., mortgage payments, etc. In the past, this has been accomplished by simply opening new accounts, fully featured, directed to the specific family member and/or specific expense. By pursuing this tack, the account holder develops multiple disparate accounts—often functionally equivalent, but without intercommunication therebetween. The fallout of this is excessive expenditures in maintaining multiple accounts that lack any coordination and thus become difficult to manage by the individual.

Moreover, a financial management institution such as a brokerage house handles accounts for thousands of people, usually with each person having two or more separate accounts (i.e., a checking account, a money market account for long-term goals and a savings account). The lack of integration between multiple accounts held by the same individual or individuals within the same household introduces, from the brokerage house perspective an additional level of recordkeeping requirements and thus a corresponding increase in fees to the account holder.

It was within the framework of the above understanding that the present invention was developed.

OBJECTS AND SUMMARY OF THE PRESENT INVENTION

It is an object of the present invention to provide an improved brokerage/cash management system.

It is another object of the present invention to enable individuals to easily and cost effectively manage their assets and have a concise, clear understanding of the value of their assets.

It is a further object of the present invention to enable an individual to delineate short and long term assets into a composite account with a single master account and a number of subaccounts which are linked within the composite account.

It is another feature of the present invention to allow individuals in the same household or family to create a single composite account for all their funds.

The above and other objects of the present invention are realized in a data processing system that directs and manages a plurality of brokerage/cash management accounts. The present system provides an account which includes at least one master account having one or more functional capabilities such as check writing, credit/debit card management, access to brokerage services, etc. The master accounts are linked to one or more nested subaccounts which are separately directed to a subset of features falling within the master account, said features corresponding to the specific needs associated with the purpose of that subaccount. Recordkeeping between the master and its associated subaccounts is done on an integrated basis as each subaccount is specifically linked and controlled by the parameters associated with its master.

In accordance with the varying aspects of the present invention, the foregoing subaccounts exclude specific credit/debit features to insure proper utilization for their intended functions, e.g., college savings, mortgage payment. By specifically tailoring the subaccount functional profile to the delineated needs of that account, the system operator can effectively streamline recordkeeping operations and thus reduce overall costs.

The foregoing and additional features and advantages of the instant invention will become more readily apparent from the following detailed description of a specific illustrative embodiment thereof, presented hereinbelow in conjunction with the accompanying drawings in which:

DESCRIPTION OF THE FIGURES

FIG. **1** is a flow chart for the establishment of the composite account with a master and subaccounts in the improved brokerage/cash management linked system;

FIG. **2** is a flow chart depicting the establishment of the fee charges for the linked accounts;

FIG. **3** is the flow chart for a representative account; and

FIG. **4** depicts the operative elements in block diagram form for the present invention.

DETAILED DESCRIPTION OF THE PRESENT INVENTION

First, briefly, the present invention is directed to a data processing system for managing a plurality of composite

accounts for financial cash management, wherein each composite account has a master account and at least one subaccount that allows an individual to establish and manage their (and their household's) complete portfolio of cash assets with one concise, cost effective account. For an individual, this system, described more fully below, has a single master account, with a variety of subaccounts directed to a specific goal such as monthly household expenses, long term investment strategies and other financial goals. The database management system has a central processing unit ("CPU") for information such as name, address and account information for each individual, with a data processing system, known as the Link System to recognize that an account (either a master account or a subaccount) is part of the composite account for the individual, a data processing means for receiving an individual's request on either a real time or periodic basis for the transfer of funds between the linked accounts and means for generating, displaying and outputting reports.

Referring now to FIG. **1** there is an operational flow chart showing the data processing system for establishment of a brokerage/cash management system in accordance with the invention.

Beginning at the top of the FIG. **1**, a request is inputted and received to open an account **10**. The Master Account **20** and one or more Subaccounts **30** are opened and a Central Processing Unit ("CPU") **40** containing the master database will receive the individual's identification such as the name and address of the individual, along with the information for that account such as the master account identification number, the subaccount identification number and the account asset information. This information will also be transmitted to the data processing unit which will link the accounts (the "Link System") **50**. The system will then request that a Fee Preference **60** be selected by the individual for the Master Account **20** and for each of the Subaccount(s) **30** opened. The Fee Preference **60** is illustrated in FIG. **2**, discussed below allows fees to be charged either completely to the Master Account **200** or individually to the Master Account and Subaccounts **210**.

At this point, the paperwork for the account is reviewed for completeness **90**. If the paperwork is not completed, the request will be Pended **100** for a set period of time (e.g. 90 days), after which time if the completed paperwork has not been received, the request will lapse. Once the paperwork is completed, then the request will be reviewed for Approval **110** for the Master Account **20** and the Subaccount(s) **30**. If it is not approved the request is denied (End). If the account is approved, then the Master Account **20** is Activated **130** and it is automatically Enrolled in the Fund Transfer System **140**. At this time, the CPU **40** containing the master database and the Link System **50** are automatically updated with the information that the Master Account **20** has been activated. The Fund Transfer System **140** will allow the Master Account **20** to transfer funds both internal and external to the system, including transfers to and from any linked subaccount(s).

At this point, the determination will be made, whether any Subaccount(s) **30** are Pending **170** with respect to the newly activated Master Account **20**. If the determination is made that Subaccount(s) **30** are Pending **170**, then the Subaccount (s) **30** are Activated **160** and Enrolled in the Fund Transfer System **140**. For the Subaccounts **30**, the Fund Transfer System **140** will allow funds to be transferred internally within the composite account to the linked Master Account **20** or another linked Subaccount **30**.

At a time after the Master Account **20** is activated, an individual may wish to open other subaccount(s). Each time a request is made to open a Subaccount **30**, the CPU **40** and the Link System **50** will receive all individual identification such as the name, address and all account information for the Master Account **20** and for all existing linked subaccounts **30** for the individual. The system will then request that a Fee Preference **60** be selected for the new Subaccount. See discussion of FIG. **2** below.

At this point, the paperwork for the Subaccount is reviewed for completeness **90**. If the paperwork is not completed, the request will be Pended **100** for a set period of time (e.g. 90 days), after which time if the completed paperwork has not been received, the request will lapse. Once the paperwork is completed, then the request will be reviewed for approval **110** for the Subaccount **30**. If it is not approved the request is denied (End). If the account is approved, then a determination will be made as to whether an Activated Master Account **130** has been linked to the new Subaccount **30**. If an Activated Master Account **130** is present then, the new Subaccount is activated **160** and Enrolled in the Fund Transfer System **140**. For the Subaccounts **30**, the Fund Transfer System **140** will allow funds to be transferred internally within the composite account to the linked Master Account **20** or another linked Subaccount **30**. At this time, the CPU **40** containing the master database and the Link System **50** are automatically updated with the information that the new Subaccount(s) **30** have been activated. If an activated Master Account **130** is not present, then the request will be Pended **100** for a set period of time (e.g. 90 days), after which time, the account will be upgraded to a Master Account **20**.

If the subaccount is for another household member, the CPU **40** containing the master database and the Link System **50** will be updated to reflect this information.

Now referring to FIG. **2**, once an account has been requested, the Fee Preference **60** for that account must be established. After the account has been requested, the individual will be asked to allot fee charges for the Master Account **20** and all Subaccount(s) **30** either entirely to the Master Account **200** or alternatively individually to the Master Account and each of the established Subaccount(s) **210**. Since the Subaccounts **30** have limited features with respect to a Master Account, fees applied to the Subaccount (s) will generally be noticeably less.

If the individual chooses to have All Fees charged to a Master Account **200**, then all initial fees for Master Account **20** and subsequently for all Subaccount(s) **30** will be charged against the Master Account **200**. Then when it is time for the Yearly Fees **220** for the Master Account and all Subaccounts, the system will check to see if the Master Account is Active **230**. If the Master Account is Active **230**, then all charges for the Master Account and all Subaccounts will be charged against the Master Account **240**. However, if the Master Account is not active, then the individual Subaccounts **250** will be charged on their respective anniversaries.

If the individual chooses to have All Fees charged against a Master Account and Subaccount(s) individually **210**, then All Fees **260** will be charged against each individual account on its respective anniversary **270**.

Cost savings will normally be shown if the individual chooses to have All Fees charged against a master account **200** since charges will not accrue on any subaccount until the next anniversary of the master account.

For example, if a master account with an annual fee of $100.00 is opened in April 1992 (with its yearly fees charged at that time), then a linked subaccount with an annual fee of $25.00 is opened in May 1992 and the individual chooses to

have all fees charged against the master account, no fees will be charged for the subaccount until April 1993, at which time the master account will be charged $125.00. However, if when the subaccount is opened, the individual chooses to have the subaccount fees charged against the subaccount, then in May 1992, $25.00 will be charged and another $25.00 will be charged in May 1993. By May 1993, if the individual chose to have all fees charged against the master account, the total fees incurred would have been a total of $225.00. If the individual chose to have fees charged individually, then by May 1993 the total fees incurred would have been a total of $250.00.

The above example also illustrates the cost effectiveness of the invention, generally. In the above example, if the composite account was not available, then the individual would have had to establish two separate primary accounts, each having an annual fee of $100.00. Therefore, in April 1992, the individual would have been charged $200.00 and then again in April 1993 the individual would have been charged $200.00 for a total of $400.00 as opposed to the $225.00 or $250.00 in fees incurred in the new system.

As discussed in FIGS. **1** and **2** above, the securities brokerage/cash management system which supervises, implements and coordinates a margin securities brokerage account is constructed of a Master Account and one or more subaccount(s) each having a fee preference option. Once the Master Account and the subaccount(s) are activated, linked and enrolled in the Fund Transfer System each can transfer funds between such linked accounts on a periodic basis, e.g., a weekly basis, and/or on a demand (as needed) basis by the individual. In addition to transferring funds, deposits can be directly made to the Master or any of the Subaccount(s).

FIG. **3** is an illustrative example of an improved securities brokerage/cash management system which supervises, implements and coordinates a margin securities brokerage account having a Master Account **20** and three subaccounts denoted respectively as Mortgage Subaccount **310**, Car Subaccount **320** and Tuition Subaccount **330**.

Starting with the Deposit **300**, deposits to the composite account can be made to the Master Account **20** or directly to the Mortgage Subaccount **310**, Tuition Subaccount **330** or Car Subaccount **320**. Next, on a continuing basis, the system will check to see if there are any real time transfers **340** (i.e. customers manual request for a transfer) pending and if there are, the transfer will be processed at the time of the request **350**. The system will transfer the requested funds from the specified account (e.g., the Tuition Subaccount **330**) to the destination account(s) (e.g., the Master Account **20**).

At the End of the Day **355**, the day's periodic transactions will be processed, including the transfers between the linked Master Account, Mortgage, Car and Tuition subaccounts.

In this example, the accounts have been set up to have an automatic transfer of funds from the Master Account **20** to the Mortgage Subaccount **310**, the Car Subaccount **320** and the Tuition Subaccount **330** every 14 days and an automatic transfer of funds to the Master Account **20** from the Mortgage Subaccount **310** and the Car Subaccount **320** on the 28th day of each month.

At the End of the Day **355**, the system will check to see if today's Date is the date of next periodic instruction **360**. If it is, then the system will transfer a predetermined amount of funds to each the Mortgage Subaccount **370**; the Car Subaccount **380**; and the Tuition Subaccount **390**. The system will then calculate and set the date of the next periodic instruction **400**. Next the system will determine whether the date is the 28th day of the month **410**. If the Date is the 28th day of the month **410**, then it will transfer a predetermined amount of funds to the Master Account from the Mortgage Subaccount **420** and from the Car Subaccount **430**. In this example, an individual does not have the subset ability to write checks directly from the subaccounts, therefore the individual can periodically transfer money to the Master Account for payments.

After the system has completed each transfer described above, it will appropriately update the Account Information **440** for the Composite Master Account **20** and Linked Subaccounts **30**. If it is the Final Day of the month **450**, the system will generate a concise customer statement **460** on the month's activities for the composite account including the Master Account **20** and each of the linked Subaccounts **30** for each individual.

Attention is now directed to FIG. **4** wherein hardware elements of the present invention are provided. In this context, the selected hardware platform is not particularly limitative and will be dictated by the number and activity of accounts under management. In particular, the Central Processing Unit ("CPU") **40** containing the system database and which implements the system commands is connected to memory unit **510** via address and data buses **520** for update and access to system records such as account assets. Additionally, support exists for terminal control **530** to allow multiple access and input to data and output to data, along with communication management **540** for communication exchange with the systems shown in FIG. **1**.

The above-described composite account arrangement has thus been shown to provide an improved securities brokerage/cash management system which supervises and integrates a brokerage account in which a Master Account with one or more linked subaccounts is used to manage an individual's funds which accounts (master and subaccounts) can transfer funds to and from, providing greater flexibility for the individual, while providing earned income for funds not invested or required to satisfy expenditures.

It should be noted that the above descriptions are presented to illustrate the invention and that modifications by those skilled in the art are possible without departing from the spirit and scope of the invention.

What is claimed is:

1. A data processing system for managing a plurality of accounts, wherein each account includes a master account, is held by a first individual, and is directed to particular profile of financial attributes and capabilities, comprising:

account input means for receiving account transactions from said individual corresponding to account activity inquiries and account asset transfers in a master account;

account processing means for creating and controlling one or more subaccounts associated with said master account, wherein said account processor permits a particular profile of account transactions to be associated with each said subaccount, said profile representing a subset of transaction functions or identifications associated with said master account; and

account reporting means for creating, displaying, or outputting reports corresponding to transactions undertaken for each account on a periodic basis.

2. The system of claim **1**, wherein said accounts processing means includes means for transferring assets between said master account and each of said subaccounts.

3. The data processing system of claim **2**, wherein said account processing means provides an identification that a particular subaccount is associated with a second individual

and with a master account held by said first individual, and further provides an identification that said first and second individuals are members of the same household.

4. The system of claim **1** wherein said master account includes asset transaction means for support of at least one credit card, one checking account and one security brokerage account.

5. The system of claim **4** wherein said subaccounts include transaction capabilities specifically limited to asset transfer between said subaccount and said master account.

6. The data processing system of claim **5**, wherein said account processing means provides an identification that a particular subaccount is associated with a second individual and with a master account held by said first individual, and further provides an identification that said first and second individuals are members of the same household.

7. The data processing system of claim **4**, wherein said account processing means provides an identification that a particular subaccount is associated with a second individual and with a master account held by said first individual, and further provides an identification that said first and second individuals are members of the same household.

8. The data processing system of claim **1**, wherein said account processing means provides an identification that a particular subaccount is associated with a second individual and with a master account held by said first individual, and further provides an identification that said first and second individuals are members of the same household.

* * * * *

Reexam
Attorney Docket No. 0076412-000029

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Reexamination Application of	**MAIL STOP:** ***Ex Parte Reexamination***
John D'Agostino	Group Art Unit: Unassigned
Patent No.: 8,036,988	Examiner: Unassigned
Issued: October 11, 2011	Confirmation No.: Unassigned
Reexam Control No.: _____	
For: SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES	

FIRST INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

To assist the Examiner, the accompanying documents are listed on the attached form PTO-1449. It is respectfully requested that an Examiner initialed copy of this form be returned to the undersigned.

The Director is hereby authorized to charge any appropriate fees under 37 CFR §§ 1.16, 1.17 and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: September 12, 2012

By: _____
Charles F. Wieland III
Registration No. 33096

Customer No. 21839
703 836 6620

Buchanan Ingersoll & Rooney PC
Attorneys & Government Relations Professionals

CERTIFICATE OF SERVICE

It is hereby certified by the undersigned that a true copy of the First Information Disclosure Statement and PTO-1449 filed on September 12, 2012 was transmitted via e-mail to:

Stephen Lewellyn, Esq.
Maxey Law Offices, PLLC
15500 Roosevelt Boulevard, Suite 305
Clearwater, Florida 33760

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: September 12, 2012 By: _____
Charles F. Wieland III
Registration No. 33096

Customer No. 21839
703 836 6620

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Bib Data Sheet

CONFIRMATION NO. 5785

SERIAL NUMBER	FILING OR 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
90/012,517	09/12/2012 RULE	705	3993	0076412-000029

APPLICANTS

8036988, Residence Not Provided;
JOHN D' AGOSTINO, SARASOTA, FL;
CHARLES F. WIELAND III, ESQ. (3RD PTY REQ.), ALEXANDRIA, VA;
BUCHANAN, INGERSOLL & ROONEY PC, ALEXANDRIA, VA

**** CONTINUING DATA ***************************

This application is a REX of 12/902,399 10/12/2010 PAT 8036988
which is a CON of 11/252,009 10/17/2005 PAT 7840486
which is a CON of 10/037,007 11/09/2001 ABN
which is a CIP of 09/231,745 01/15/1999 PAT 6324526

**** FOREIGN APPLICATIONS *********************

Foreign Priority claimed	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ yes ☐ no			38	5
35 USC 119 (a-d) conditions met ☐ yes ☐ no ☐ Met after Allowance				
Verified and Acknowledged _____ Examiner's Signature _____ Initials				

ADDRESS
34111

TITLE
SYSTEM AND METHOD FOR PERFORMING SECURE CREDIT CARD PURCHASES

FILING FEE RECEIVED	FEES: Authority has been given in Paper	
2520	No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit