

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: January 2, 2013
Electronic Signature for Marcus E. Browne: / Marcus E. Browne /

Docket No.: W0537-700620
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 11/768,729

Confirmation No.: 3536

Filed: June 26, 2007

Art Unit: 2435

For: UNIVERSAL SECURE REGISTRY

Examiner: Thomas A. Gyorfi

AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION UNDER 37 C.F.R. 1.111

Commissioner for Patents

Dear Madam:

INTRODUCTORY COMMENTS

In response to the Office Action dated October 2, 2013, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 11 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive, ~~from the first party,~~ a transaction request including at least the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed and an indication of the first party requesting the transaction, configured to map the time-varying multicharacter code to the identity of the entity in the database using the time-varying multicharacter code, to execute a restriction mechanism configured to determine compliance with any access restrictions for the first party to secure data for completing the transaction based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request, and to allow or not allow access to the secure data associated with the entity including information required to enable the transaction based on the determined compliance with any access restrictions for the first party, the information including account identifying information, wherein ~~where~~ the account identifying information is not provided to the first party and the account identifying information is provided to a third party to enable or deny the transaction with the first party ~~and~~ without providing the account identifying information to the first party.

2. (Canceled)

3. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is provided to the system via a secure electronic transmission device.

4. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is encrypted and transmitted to the system, and

wherein the system is configured to decrypt the time-varying multicharacter code with a public key of the entity.

5. (Previously Presented) The system as claimed in claim 1, wherein the transaction includes a service provided by the first party,

wherein said first party's service includes delivery,

wherein the information is an address to which an item is to be delivered to the entity,

wherein the system receives the time-varying multicharacter code, and

wherein the system uses the time-varying multicharacter code to obtain the appropriate address for delivery of the item by the third party.

6. – 8. (Canceled)

9. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes credit card account information regarding the entity, and wherein the processor is configured to provide the credit card account information based upon the multicharacter code of the entity to enable the transaction.

10. (Previously Presented) The system as claimed in claim 9, wherein the system is configured to receive an approval of the credit card transaction.

11. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes bank card account information regarding the entity, and wherein the processor

is configured to provide the bank card account information to enable the transaction based upon the multicharacter code of the entity.

12. (Previously Presented) The system as claimed in claim 11, wherein the system is configured to provide an approval of the bank card transaction.

13. (Previously Presented) The system as claimed in claim 1, wherein the information includes personal identification information regarding the entity.

14. (Previously Presented) The system as claimed in claim 13, wherein the personal identification information comprises a photograph of the entity, and wherein the photograph is provided to the first party.

15. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information identifies email address information regarding the entity.

16. (Currently Amended) A method for providing information to a first party to enable transactions between the first party and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code, the method comprising:

receiving a transaction request including at least the time-varying multicharacter code for an entity on whose behalf a transaction is to take place and an indication of the first party requesting the transaction;

mapping the time-varying multicharacter code to an identity of the entity in a database using the time-varying multicharacter code;

determining compliance with any access restrictions for the first party to secure data for completing the transaction based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request;

accessing information required to perform the transaction based on the determined compliance with any access restrictions for the first party, the information including account identifying information;

providing the account identifying information to a third party without providing the account identifying information to the first party to enable or deny the transaction; and

~~using the account identifying information to enable~~ enabling or denying the first party to perform the transaction without the first party's knowledge of the account identifying information.

17. – 18. (Canceled)

19. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving the time-varying multicharacter code transmitted via a secure electronic transmission device.

20. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving an encrypted multicharacter code, and wherein the method further comprises decrypting the encrypted multicharacter code.

21. (Previously Presented) The method as claimed in claim 16, wherein the transaction includes a service provided by the first party,
wherein the service includes delivery,
wherein the account identifying information is associated with an address to which an item is to be delivered for the entity, and
wherein the third party receives the address for delivery of an item provided by the first party.

22. – 23. (Canceled)

24. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information includes a credit card number, and wherein the act of using the account identifying information comprises using the credit card number to enable the transaction.

25. (Previously Presented) The method as claimed in claim 24, wherein the act of using the account identifying information comprises receiving a validation or denial of the transaction without providing the credit card number of the entity to the first party.

26. (Previously Presented) The method as claimed in claim 16, wherein the act of using the account identifying information comprises using bank card information about the entity to enable a transaction.

27. (Previously Presented) The method as claimed in claim 26, wherein the act of using the information comprises receiving a validation or denial of the bank card transaction without providing a bank card number of the entity to the first party.

28. (Previously Presented) The method as claimed in claim 16, wherein the act of mapping the time-varying multicharacter code to information required by the first party comprises mapping the time-varying multicharacter code to personal identification information about the entity.

29. (Previously Presented) The method as claimed in claim 28, wherein the personal identification information comprises a photograph of the entity, and
wherein the method further comprises an act of providing the photograph to the first party.

30. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information identifies email address information about the entity.

31. (Canceled)

32. (Previously Presented) The method as claimed in claim 24, further comprising an act of transmitting to the first party one of an approval or a denial of the credit card transaction.

33. (Previously Presented) The system of claim 1, wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry, respectively.

34. (Previously Presented) The system of claim 33, wherein the processor is further configured to map the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed and to provide the biometric information to the first party.

35. (Previously Presented) The system of claim 34, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed.

36. (Previously Presented) The system of claim 34, wherein the time-varying multicharacter code is generated by a device associated with the entity on whose behalf the transaction is to be performed.

37. (Previously Presented) The method as claimed in claim 16, further comprising an act of associating biometric information with each entity having secure data in the secure registry, respectively.

38. (Previously Presented) The method of claim 37, further comprising acts of:
mapping the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed; and
providing the biometric information to the first party.

39. (Previously Presented) The method of claim 38, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed.

40. (Canceled)

41. (Previously Presented) The system of claim 1, wherein the account identifying information includes an account number.

42. (Previously Presented) The system of claim 41, wherein the account identifying information includes credit card account information and the account number includes a credit card number.

43. (Previously Presented) The system of claim 41, wherein the third party includes a financial service provider and the account number includes at least one of a debit card number and a credit card number.

44. (Previously Presented) The system of claim 43, wherein the first party includes a merchant, and the service includes a sale of at least one of goods and services.

45. (Previously Presented) The system of claim 44, wherein the processor is further configured to receive, from the first party, a merchant ID, and a purchase amount.

46. (Previously Presented) The system of claim 1, wherein the identity of the entity is unknown until the time-varying code is mapped to the identity by the processor.

47. (Currently Amended) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system,

respectively, each time-varying multicharacter code representing an identity of one of the respective entities, wherein the database is configured to permit or deny access to information on the respective entity using the time-varying multicharacter code; and

a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity to identify the entity, configured to execute a restriction mechanism to determine compliance with any access restrictions for the first party to at least one portion of secure data for completing the transaction and to store an appropriate code with each such portion of secure data, configured to obtain from the database the secure data associated with the entity including information required to enable the transaction, the information including account identifying information, and configured to provide the account identifying information to a third party to enable or deny the transaction without providing the account identifying information to the first party.

48. (Previously Presented) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity without requiring further information to identify the entity, configured to access from the database secure data associated with the entity including information required to enable the transaction, the information including account identifying information, and configured to provide the account identifying information to a third party to enable or deny the transaction without providing the account identifying information to the first party, and wherein enabling or denying the transaction without providing account identifying information to the first

party includes limiting transaction information provided by the secure registry system to the first party to transaction approval information.

REMARKS

Claims 1, 3-5, 9-16, 19-21, 24-30, 32-39, and 41-48 were previously pending in this application. Claims 1, 16, 44, and 47 have been amended. As a result claims 1, 3-5, 9-16, 19-21, 24-30, 32-39, and 41-48 are pending for examination with claims 1, 16, 47 and 48 being independent claims. No new matter has been added.

Claim Objections

The Office Action object to claim 47 as allegedly being a substantial duplicate of claim 1. Without acceding to the correctness of this objection, Applicant has amended claims 1 and 47 to overcome this objection. Accordingly, withdrawal of the objection to claim 47 is respectfully requested.

Rejections Under 35 U.S.C. §103

The Office Action rejected claims 1, 3-5, 9-16, 19-21, 24-30, 32-39, and 41-48 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,571,139 to Giordano (hereinafter “Giordano”) in view of U.S. Patent No. 7,742,967 to Keresman (hereinafter “Keresman”). Without acceding to the substance of this rejection, Applicant has amended independent claims 1, 16, and 47 to further clarify the distinctions between the claims as pending and the asserted combination of references and submits the following remarks.

Claim 1, as amended, is directed to “a secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system.” The system comprises “a processor configured to receive a transaction request” that includes “the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed and an indication of the first party requesting the transaction” and “execute[s] a restriction mechanism configured to determine compliance with any access restrictions for the first party to secure data for completing the transaction *based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request*,” as recited in claim 1, as amended.

Giordano is directed to “a network for processing retail sales transactions” including “a customer transceiver with a unique customer number” (Abstract). Giordano teaches a “transaction processing system” that processes transactions with the “appropriate payment processing center” based on received authorization requests including “the customer ID, merchant ID and transaction data” (Col. 3 Lines 29-36). In summary, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center.

Claim 1, as amended, is patentable over Giordano because Giordano does not teach or suggest “a restriction mechanism configured to determine compliance with any access restrictions for the first party to secure data for completing the transaction *based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request.*” Rather, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center. Thus, Giordano does not teach or suggest “a restriction mechanism configured to determine compliance with any access restrictions for the first party to secure data for completing the transaction *based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request,*” as recited in claim 1, as amended. Accordingly, claim 1, as amended, distinguishes over the Giordano reference.

Keresman is directed to “a method of processing commercial transactions carried out over the Internet” where the commercial transactions are “between account holders” and “participating merchants” (Abstract). Keresman teaches that the “account holder record” may “contain information or data relating to account privileges” that may be “customize[d] or modif[ied]” (Col. 6 Lines 44-49). The account privileges may “restrict the account so that purchases thereon are not authorized for specific participating merchants or sellers,” restrict “automatically reoccurring transactions,” or restrict “single purchases over a certain price” (Col. 6 Lines 54-64). In summary, Keresman teaches the storage of account holder records that may limit specific types of transactions.

Applicant respectfully asserts that the addition of Keresman to Giordano does not cure the deficiencies discussed above with regard to Giordano. In particular, Keresman does not teach or suggest “a restriction mechanism configured to determine compliance with any access restrictions

for the first party to secure data for completing the transaction ***based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request,***” as recited in claim 1, as amended. Rather, Keresman simply discloses the storage of account holder records that may limit specific types of transactions. Therefore, Keresman does not teach or suggest a restriction mechanism that uses a “time-varying multicharacter code” in combination with an “indication of the first party” to “determine compliance with any access restrictions,” as recited in claim 1. Accordingly, claim 1, as amended, distinguishes over the Keresman reference.

As neither Giordano nor Keresman teach or suggest at least one element of claim 1, the combination, even if assumed proper, does not teach or suggest claim 1, as amended. Claims 3-5, 9-15, 33-36 and 41-46 depend from claim 1 and are allowable for at least the same reasons. Accordingly, withdrawal of the rejection of claims 1, 3-5, 9-15, 33-36 and 41-46 under 35 U.S.C. §103(a) is respectfully requested.

Independent Claim 16

Independent claim 16, as amended, is directed to “a method for providing information to a first party to enable transactions between the first party and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code.” The method includes, inter alia, “receiving a transaction request including at least the time-varying multicharacter code for an entity on whose behalf a transaction is to take place and an indication of the first party requesting the transaction” and “determining compliance with any access restrictions for the first party to secure data for completing the transaction ***based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request,***” as recited in claim 16, as amended. As discussed above with respect to claim 1, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center. Thus, Giordano does teach or suggest “determining compliance with any access restrictions for the first party to secure data for completing the transaction ***based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request,***” as recited in claim 16, as amended. Assuming without admitting that the combination is proper, the

addition of Keresman does not cure this deficiency. Claims 19-21, 24-30, 32 and 37-39 depend from claim 16 and are allowable for at least the same reasons. Accordingly, withdrawal of the rejection of claims 16, 19-21, 24-30, 32, and 37-39 under 35 U.S.C. §103(a) is respectfully requested.

Independent Claim 47

Independent claim 47 is directed to “a secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system.” The system comprises “a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed” and “execute a restriction mechanism to *determine compliance with any access restrictions for the first party to at least one portion of secure data for completing the transaction* and to *store an appropriate code with each such portion of secure data*,” as recited in claim 47. As discussed above with respect to claim 1, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center. Thus, Giordano does not teach or suggest “a restriction mechanism to *determine compliance with any access restrictions for the first party to at least one portion of secure data for completing the transaction* and to *store an appropriate code with each such portion of secure data*,” as recited in claim 47. Assuming without admitting that the combination is proper, the addition of Keresman does not cure this deficiency. Accordingly, withdrawal of the rejection of claim 47 under 35 U.S.C. §103(a) is respectfully requested.

Independent Claim 48

Independent claim 48 is directed to “a secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system.” The system comprises “a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed” and “provide the account identifying information to a third party to enable or deny the transaction without providing the account identifying information to the first party” wherein “enabling or denying the

transaction without providing account identifying information to the first party includes ***limiting transaction information provided by the secure registry system to the first party to transaction approval information,***” as recited in claim 48. In contrast, Giordano teaches the “transaction processing system” transmitting to the online merchant “identification information and other data unique to the associated customer in the absence of a retail transaction” (See Col. 4 Lines 17-21). Giordano explicitly teaches the transmission of information regarding the user (e.g., entity or purchaser), including loyalty program information (See e.g., Col. 4 Lines 54-58), to a merchant (e.g., first party) rather than limiting the information transmitted to the merchant to transaction approval information. The Office Action alleges on page 4 that Giordano discloses that “the buyer either succeeds in purchasing his desired products or is declined, with no other information being provided: col. 18, line 65 – col. 19, line 15.” However, the section cited in the Office Action (i.e., col. 18, line 65 – col. 19, line 15) of Giordano explicitly states that “authorization ***and the award data*** (if any) are transmitted to the merchant” (Col. 18 Lines 64-65). Further, Giordano states that even when “the transaction does not require authorization,” the “transaction processing system” still provides “transaction information ***and loyalty program information***” (Col. 19 Lines 19-24). Accordingly, Giordano does not teach or suggest claim 48, as amended. Assuming without admitting that the combination is proper, the addition of Keresman does not cure this deficiency. Accordingly, withdrawal of the rejection of claim 48 under 35 U.S.C. §103(a) is respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762 (Ref. No. W0537-700620).

Dated: January 2, 2013

Respectfully submitted,

Electronic signature: / Marcus E. Browne /
Marcus E. Browne

Registration No.: 71,891

Matthew H. Grady

Registration No.: 52,957

LANDO & ANASTASI LLP

Riverfront Office Park

One Main Street

Suite 1100

Cambridge, Massachusetts 02142

(617) 395-7000

Attorney for Applicant

Electronic Acknowledgement Receipt

EFS ID:	17799986
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	Marcus E. Browne
Filer Authorized By:	
Attorney Docket Number:	W0537-700620
Receipt Date:	02-JAN-2014
Filing Date:	26-JUN-2007
Time Stamp:	14:24:43
Application Type:	Utility under 35 USC 111(a)

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		-_Response_to_Non-Final_Office_Action_mailed_10-2-13_FINAL.pdf	64020 8ede93ea4d0ed5c571606a209120145577ced85	yes	16

Multipart Description/PDF files in .zip description			
Document Description		Start	End
Amendment/Req. Reconsideration-After Non-Final Reject		1	1
Claims		2	10
Applicant Arguments/Remarks Made in an Amendment		11	16

Warnings:

Information:

Total Files Size (in bytes):	64020
-------------------------------------	-------

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.