US 20010029485A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2001/0029485 A1

Brody et al. (43) Pub. Date: Oct. 11, 2001

(54) SYSTEMS AND METHODS ENABLING ANONYMOUS CREDIT TRANSACTIONS

(75) Inventors: **Robert M. Brody**, Weston, CT (US); **Reuben S. Kennedy**, Duluth, GA (US)

Correspondence Address:
ALSTON & BIRD LLP
BANK OF AMERICA PLAZA
101 SOUTH TRYON STREET, SUITE 4000
CHARLOTTE, NC 28280-4000 (US)

(73) Assignee: **E-Scoring, Inc.**

(21) Appl. No.: **09/796,719**

(22) Filed: **Feb. 28, 2001**

Related U.S. Application Data

(63) Non-provisional of provisional application No. 60/186,166, filed on Feb. 29, 2000.

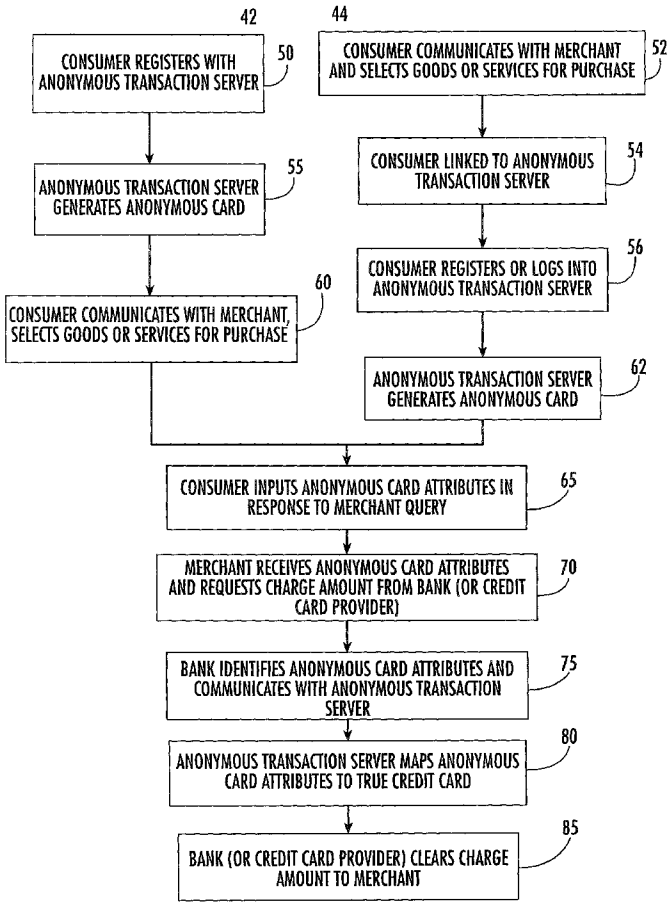
Publication Classification

(51) **Int. Cl.**[7] **G06F 17/60**; H04K 1/00

(52) **U.S. Cl.** **705/39**; 705/75

(57) **ABSTRACT**

The system and method of the present invention enables consumers to purchase goods and services from merchants, using credit cards, wherein the consumers can maintain the confidentiality of their credit card numbers and identity without disclosure to the merchants, so that an anonymous credit transaction can take place. The system and method takes blocks of consumer credit card numbers and creates dynamic mappings of the card numbers to account numbers or even other card numbers, such as pseudo-random credit card numbers. The system and method of the present invention generates pseudo-random credit card attributes, which are presented to merchants at the time of purchase for Internet, telephone, or mail order purchases. Because pseudo-random attributes are transmitted to the merchant, the transaction between the consumer and merchant will be anonymous. Pseudo-random attributes include the card number, name, billing zip code, expiration date, and purchase amount, each of which can be used singularly or in combination to authenticate a transaction according to consumer preferences, which are captured when the consumer establishes the agent relationship with system of the present invention.



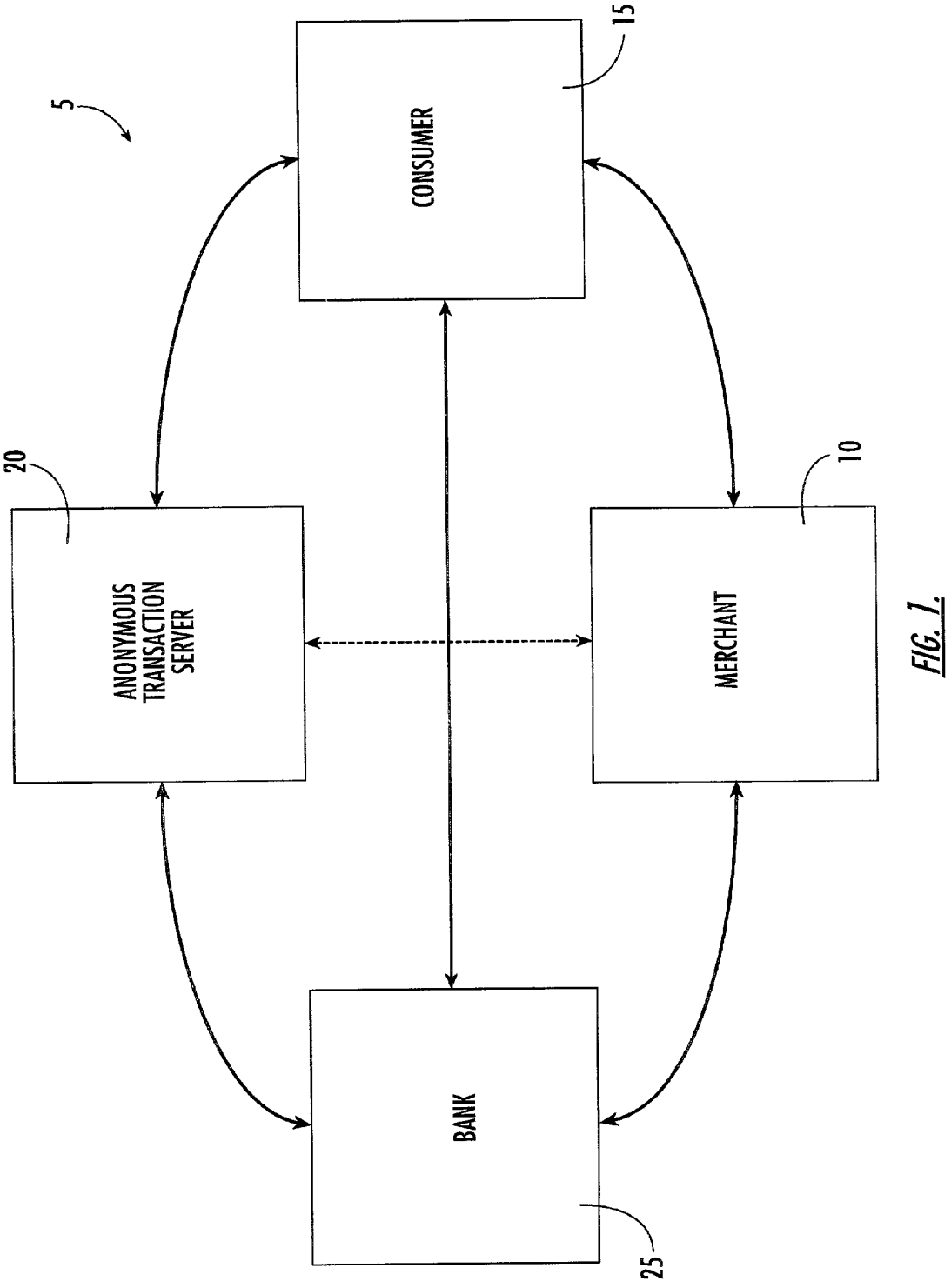


FIG. 1.

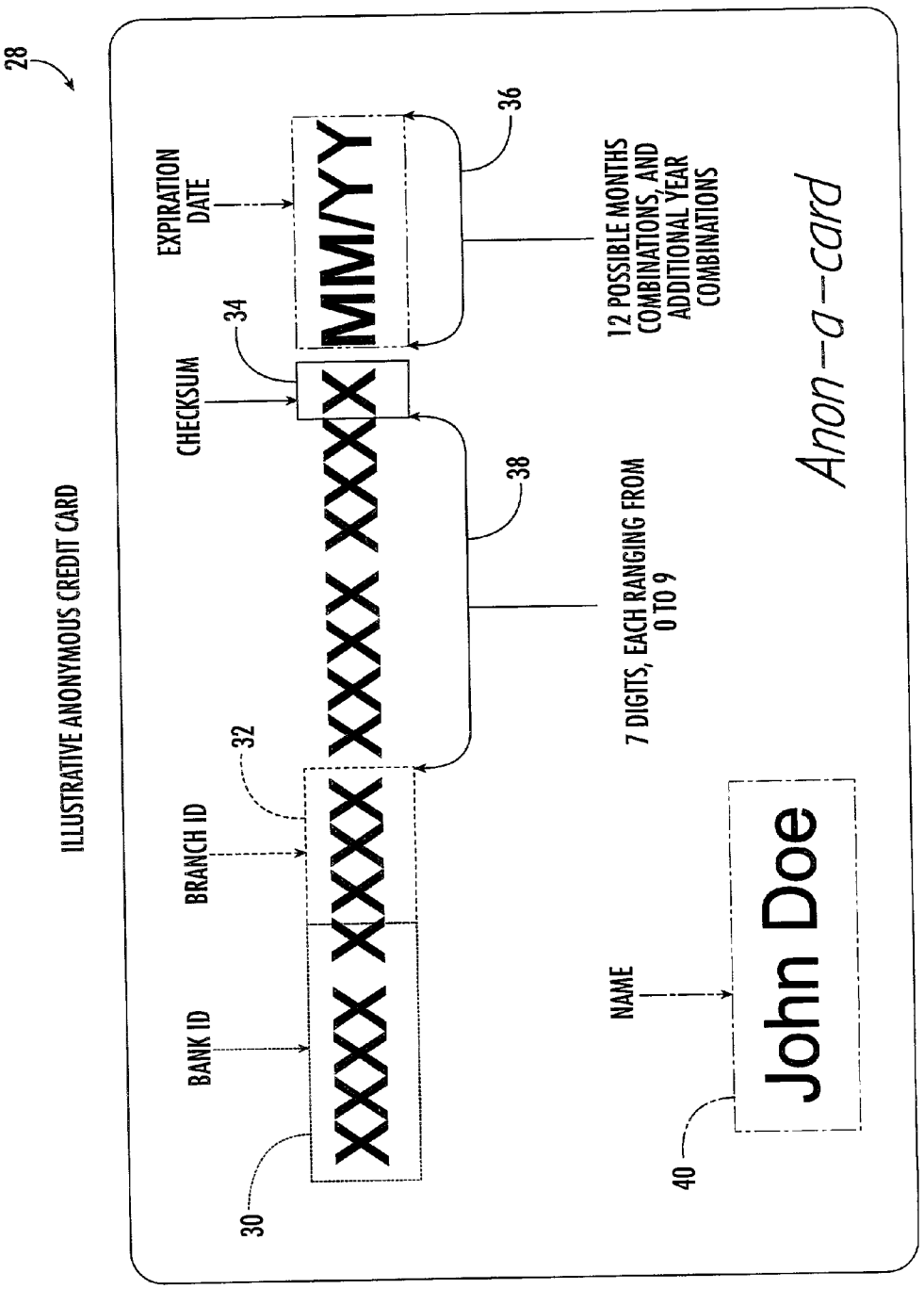


FIG. 2.

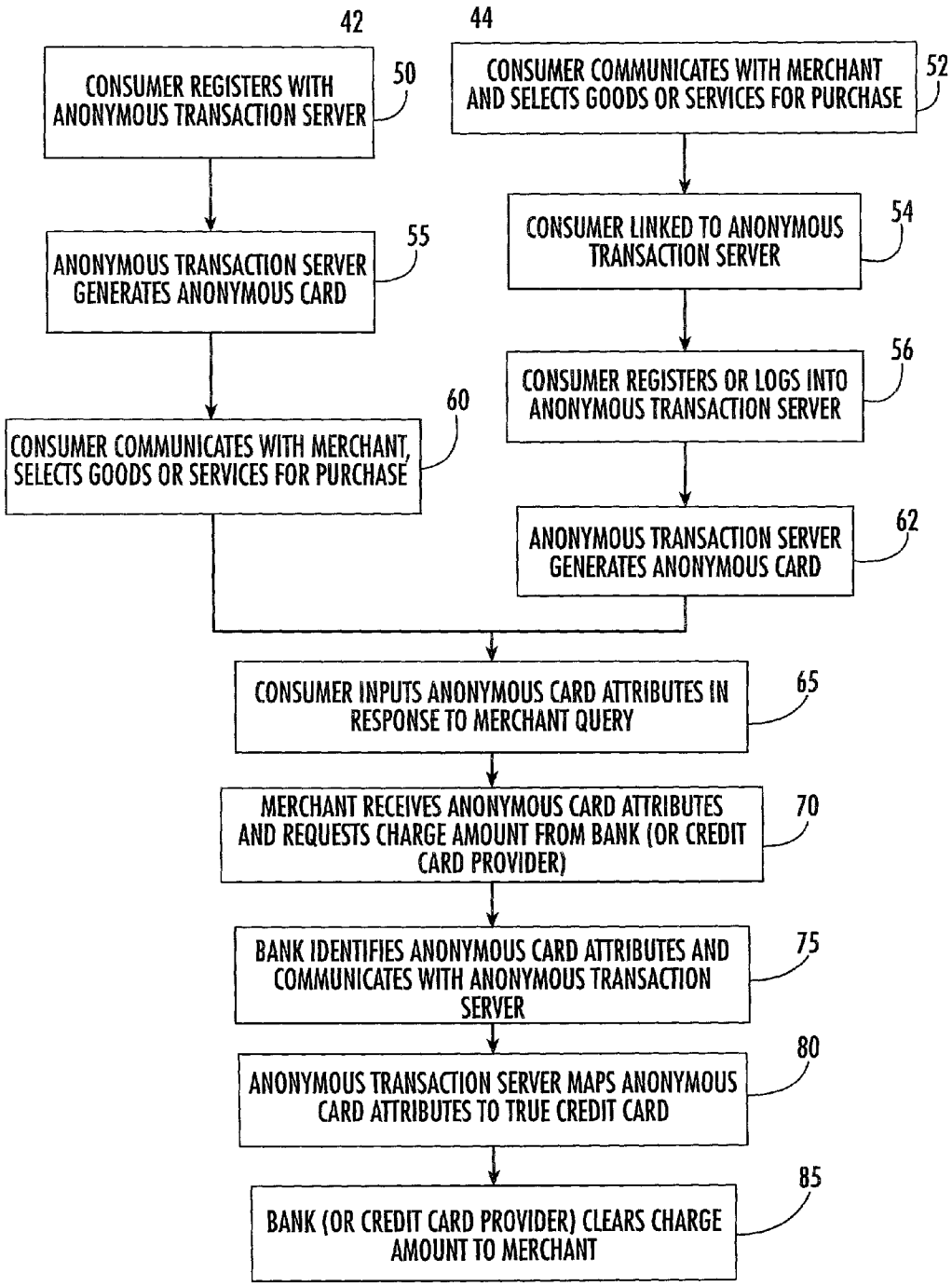


FIG. 3.

SYSTEMS AND METHODS ENABLING ANONYMOUS CREDIT TRANSACTIONS

RELATED APPLICATION DATA

[0001] The present application claims priority from U.S. Provisional Patent Application Serial No. **60/186,166**, filed Feb. 29, 2000, titled "Systems and Methods Enabling Anonymous Credit Transactions" and assigned to E-Scoring, Inc., the entire contents of which are herein incorporated by reference.

FIELD OF THE INVENTION

[0002] The present invention relates to electronic payments in exchange for goods and services, and more specifically, to systems and methods enabling consumers to purchase goods and services from merchants using credit cards.

BACKGROUND OF THE INVENTION

[0003] Shopping for goods and services using a personal computer to place an order on a network, such as the Internet, has exploded in volume over the past few years due to the ever increasing number of merchants selling goods and services via the Internet, as well as the increasing number of consumers online. Online shopping, which is a natural extension to the more traditional catalog shopping, enables consumers to quickly and efficiently browse through goods at their favorite online stores without leaving the comfort of their own home. The advantages of such shopping are countless- consumers can access stores that may be geographically remote, can order items not otherwise in stock or available at a local store, can quickly compare items from a number of stores, and can often pay less for the same items sold at conventional shopping stores.

[0004] Due to the remote and electronic nature of network transactions, just as in conventional catalog ordering most purchases over the Internet are made by credit cards. However, many consumers are concerned about their credit card numbers being transmitted over networks such as the Internet because of the lack of secure communications. Along with the increase of Internet traffic is an increase in opportunity for thieves to intercept credit card numbers for their own personal use. Because credit card transactions over the Internet are not face-to-face, a person having a stolen credit card can charge substantial amounts of goods to that card before the credit card company or consumer is even aware the theft is occurring, which may result in thousands of dollars of losses to the consumer, card issuer, or merchant. Furthermore, each time that credit card information is communicated to a merchant, another opportunity is presented for an unauthorized third party to gain access to the credit card data.

[0005] In addition to the possibility that credit card information may be stolen each time the information is submitted to a merchant over the network, the use of a credit card also enables merchants to store information such as the consumer's name, shipping address, and credit card information. After the information has been conveyed only once it can remain on file with the merchant within a customer database. Although this provides some advantages, such as the fact that for subsequent purchases the customer need not communicate their credit card number to the merchant, this also results in some undesired consequences. For instance, many merchants use this information for solicitation purposes, which is an inconvenience to many consumers. Additionally, merchants often also sell or provide this information to other entities who use the information to their own advantage, and without consumer consent. Further, the more purchases a consumer makes, the more physical locations where their credit and personal information is stored will be created. This increases the exposure the consumer has to fraudulent use of this data by, for example, a person that gains unlawful access to the data stored in the merchant's storage facilities.

[0006] A number of attempts have been made to alleviate the problem of data protection over networks such as the Internet. For instance, many prior art systems attempt to encrypt credit card numbers at the consumer's computer, prior to transmission over the network. Once the data has been encrypted it is transmitted over the network to the desired location, and decrypted and accessible to the receiving party. Credit card numbers can be encrypted using any of several techniques, such as public key encryption and SSL. However, applying encryption techniques when transmitting credit card numbers requires a merchant to have access to the proper decryption software. Furthermore, encryption may also be overcome by those persons with the ability to intercept credit card numbers transmitted over the network. Therefore, although encryption technology exists to protect consumer to merchant transactions, protecting information that is traded with transaction partners remains difficult.

[0007] In addition to problems faced by consumers in transactions over networks such as the Internet, merchants also face potential losses and liability due to fraud. For example, a person using a stolen credit card number may purchase items of value from a merchant, who then provides the items to the thief. When a credit card company refuses to pay the merchant because the merchant accepted credit card payment over the network without proof of identity, the merchant will be forced to incur loses for the value of the items.

[0008] What is therefore needed is a system and method that protects consumers and merchants alike from the potential theft of credit card information during transactions, particularly, Internet transactions.

SUMMARY OF THE INVENTION

[0009] The present invention can take blocks of consumer credit card numbers and create dynamic mappings of the card numbers to account numbers or other card numbers, such as pseudo-random credit card numbers. According to one aspect of the invention, the systems and methods of the present invention generate "pseudo-random" credit card attributes, which are presented to merchants at the time of purchase for Internet, telephone, or mail order purchases. The pseudo-random attributes are used by consumers in place of the consumer's credit card. Because pseudo-random attributes are transmitted to the merchant, the transaction between the consumer and merchant will be anonymous. Pseudo-random attributes include the card number, name, billing zip code, expiration date, and purchase amount, each of which can be used singularly or in combination by an authentication server to authenticate a transaction according to consumer preferences, which are captured when the

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.