(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 July 2008 (24.07.2008)

PCT

(10) International Publication Number
WO 2008/089091 A2

(51) International Patent Classification:
G06Q 40/00 (2006.01)

(21) International Application Number: PCT/US2008/050903

(22) International Filing Date: 11 January 2008 (11.01.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/623,968 17 January 2007 (17.01.2007) US

(71) Applicant *(for all designated States except US)*: **THE WESTERN UNION COMPANY** [US/US]; 12500 East Belford Avenue, Englewood, Colorado 80112 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KEANE, Tim** [IE/IE]; 2 Church Park Avenue, Mount Argus, Harolds Cross, Dublin, 6W (IE). **SEIFERT, Dean** [US/IE]; Roscahill Tresilian, Brighton Road, Foxrock, Dublin, 18 (IE). **GRAHMANN, Jonathan** [US/IE]; 82 Northumberland Road, Apt. 4, Ballsbridge, Dublin, 4 (IE).

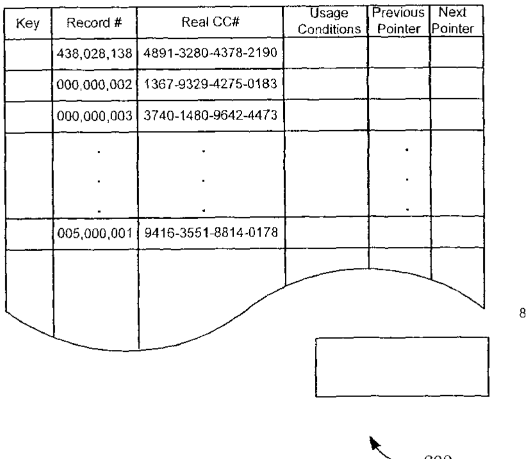
(74) Agents: GIBBY, Darin, J. et al.; TOWNSEND AND TOWNSEND AND CREW LLP, 1200 Seventeenth Street, Suite 2700, Denver, Colorado 80202 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

(54) Title: SECURE MONEY TRANSFER SYSTEMS AND METHODS USING BIOMETRIC KEYS ASSOCIATED THEREWITH



Key	Record #	Real CC#	Usage Conditions	Previous Pointer	Next Pointer
	438,028,138	4891-3280-4378-2190			
	000,000,002	1367-9329-4275-0183			
	000,000,003	3740-1480-9642-4473			
	⋮	⋮		⋮	
	005,000,001	9416-3551-8814-0178			

FIG. 8

(57) Abstract: A method for transferring funds from a sender to a recipient includes receiving a request to transfer the funds from a sender; creating a transaction record having a transaction identifier; providing the transaction identifier to the sender; receiving the transaction identifier from a recipient; obtaining a first biometric sample from the recipient; using the biometric sample to select a MTCN (Money Transfer Control Number) from a pool of predetermined MTCNs; associating the MTCN with the first biometric sample and the transaction record; providing the MTCN to the recipient; thereafter, receiving a request from the recipient to receive the funds; obtaining the MTCN from the recipient; obtaining a second biometric sample from the recipient; using the MTCN and/or the second biometric sample to locate the transaction record; comparing the second biometric sample to the first biometric sample; and determining whether to provide the funds based on the comparison.

SECURE MONEY TRANSFER SYSTEMS AND METHODS USING BIOMETRIC KEYS ASSOCIATED THEREWITH

FIELD OF THE INVENTION

[0001] Embodiments of the present invention relate generally to transaction settlement identifier generation systems and methods. More specifically, embodiments of the present invention relate to systems and methods for generating transaction settlement identifiers using biometric features.

CROSS-REFERENCES TO RELATED APPLICATIONS

[0002] The following U.S. patent application is being filed concurrently. The disclosure of this application is incorporated by reference in the present application in its entirety for all purposes: U.S. Patent Application No. 11/623,956 filed January 17, 2007, entitled "Generation Systems And Methods For Transaction Identifiers Having Biometric Keys Associated Therewith" (Attorney Docket No. 026595-009200US).

BACKGROUND OF THE INVENTION

[0003] Fraud in eCommerce transactions has become a significant problem. Credit card issuers have created the "surrogate card number" model in an attempt to address this problem. According to this model, a "one time" credit card number is generated by a credit card issuer and automatically mapped back (by the issuer system) to the original card number during any subsequent authorisation, capture or refund event. The original card number is, therefore, never exposed and in the event the "one time" number is compromised (e.g. a hacker successfully penetrates the merchant's system) the fraud risk is mitigated as the "one time" number is deactivated for further purchase activity once the first authorisation event is processed.

[0004] While this model represents a significant improvement in online fraud management and has helped to establish consumer confidence in online commerce, it remains vulnerable to the threat of identity theft (commonly referred to as "phishing"). A variety of sophisticated techniques, including social engineering, are employed by fraudsters to discover consumer information (e.g. User Ids, passwords etc.) to enable them to perform seemingly valid transactions for fraudulent purposes. For example, in the "one time" card model, the fraudster would attempt to discover the consumer's password to enable the fraudster to request a valid "one time" credit card number to purchase goods online and have them shipped to a different address. Customers subsequently repudiate the transaction leaving the issuer in the position of adjudicator with consequential financial loss or reduction in customer satisfaction levels.

[0005] In essence the point of attack is starting to shift away from merchant's systems back to the issuer's systems. While the "surrogate card number" model is principally designed to effectively address merchant vulnerabilities, further expansion of the concept is needed to consider issuer side threats and vulnerabilities.

[0006] Likewise, fraud is a significant problem in money transfer transactions. Under typical practice, a sender visits an "agent" (i.e., agent of a money transfer system operator, such as Western Union of Englewood, Colorado) location to specify payee details (name, destination country and test question, if applicable) and pay applicable fees and principal amount to be transferred. The agent receipts the transaction details into a money transmission system and receives a Money Transfer Control Number ("MTCN") that uniquely references the transaction. The agent provides the MTCN to the sender. The sender advises the recipient (Payee) through independent means (e.g. phone call or SMS) of the transfer's availability for collection and the MTCN. The payee visits an agent location, and supplies the MTCN, appropriate identification and correct response to the test question (if applicable). The agent pays out the principal amount on successful completion of verification checks. Some of the foregoing steps may be performed by Internet-based means.

[0007] This model is vulnerable to a number of attacks. For example, a paying agent may collude with a fraudster and pay out funds without complying with local verification procedures. An unrelated agent in the paying country may also retrieve the transaction details from the money transfer software using limited search criteria and enable an accomplice to proceed with collection at a separate location in the expected payout country. Or, a number of fraudulently inclined individuals may present themselves simultaneously at different agent locations in the destination country of a transfer and all receive payout before the money transfer system is able to detect the problem.

[0008] Hence, a more robust payee authentication method is required at point of payout to secure the process from these attacks.

BRIEF SUMMARY OF THE INVENTION

[0009] One embodiment of the invention provides for a method of transferring funds from a sender to a recipient. The method may include receiving a request to transfer funds from a sender; creating a transaction record having a transaction identifier; providing the transaction identifier to the sender; receiving the transaction identifier from a recipient; obtaining a first biometric sample from the recipient; using the biometric sample to select a MTCN (Money Transfer Control Number) from a pool of predetermined MTCNs; associating the MTCN with the first biometric sample and the transaction record; providing the MTCN to the recipient; receiving a request from the recipient to receive the funds; obtaining the MTCN from the recipient; obtaining a second biometric sample from the recipient; using the MTCN and/or the second biometric sample to locate the transaction record; comparing the second biometric sample to the first biometric sample; and determining whether to provide the funds based on the comparison.

[0010] The method may also include determining whether the funds have been paid out and/or determining whether an amount of the funds exceeds a threshold amount of funds transferred for which compliance is required. The biometric sample may be a voiceprint, a fingerprint, a retinal scan, and/or a DNA sample.

[0011] Another embodiment of the invention provides for a method of transferring funds from a sender to a recipient. The method may include receiving a request from the recipient to stage the transaction; obtaining a first biometric sample from the recipient; using the first biometric sample to select a transaction number from a pool of predetermined transaction numbers; creating a transaction record having the transaction number and the first biometric sample associated therewith; providing the transaction number to the recipient; receiving a request from the sender to deposit the funds; receiving the transaction number from the sender; modifying the transaction record to indicate that the funds have been deposited; thereafter, receiving a request from the recipient to receive the funds; and using a second biometric sample, at least in part, to determine whether to provide the funds to the recipient.

[0012] The method may further include receiving the transaction number from the recipient; obtaining the second biometric sample from the recipient; using the transaction number and/or the second biometric sample to locate the transaction record; comparing the first biometric sample to the second biometric sample; and based on the comparison, determining whether to issue a MTCN (Money Transfer Control Number). In another embodiment, the method may also include receiving the MTCN at a money transfer location; and providing the funds to the recipient. The method may further include determining whether the funds have been paid out and/or whether an amount of the funds exceeds a threshold amount of funds transferred for which compliance is required.

[0013] In another embodiment a second biometric sample may be used, at least in part, to determine whether to provide the funds to the recipient. This embodiment may include at a money transfer location, receiving a request to receive the funds from the recipient; receiving the transaction number from the recipient; using the transaction number to locate the transaction record; obtaining the second biometric sample from the recipient; and comparing the first biometric sample to the second biometric sample. The method may further include determining whether the funds have been paid out and/or whether an amount of the funds exceeds a threshold amount of funds transferred for which compliance is required. The biometric sample may include a voiceprint, a fingerprint, a retinal scan, and/or a DNA sample.

[0014] Another embodiment of the invention provides for a money transfer system that includes an input adapted to receive biometric samples; a storage arrangement configured to store the biometric samples or derivatives thereof; and a processor. The processor includes instructions to use a first biometric sample to select a MTCN (money transfer control number) from a pool of predetermined MTCNs; and link the first biometric sample to the MTCN. The biometric sample may include a voiceprint, a fingerprint, a retinal scan, and a DNA sample. The processor may also include instructions to respond to a request to settle a transaction using the MTCN by receiving a second biometric sample and comparing the second biometric sample to the first biometric sample. The processor may further include instructions to determine whether to provide funds to a recipient by determining whether the funds have been paid out and/or whether an amount of the funds exceeds a threshold amount of funds transferred for which compliance is required.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] A further understanding of the nature and advantages of the present invention may be realized by reference to the remaining portions of the specification and the drawings wherein like reference numerals are used throughout the several drawings to refer to similar components. Further, various components of the same type may be distinguished by following the reference label by a dash and a second label that distinguishes among the similar components. If only the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

[0016] Fig. 1A depicts a typical purchase transaction in which a consumer uses a one-time-use credit card to complete a transaction with an online merchant according to one embodiment of the invention.

[0017] Fig. 1B depicts a purchase transaction in which a fraudster acquires account details from the consumer leaving the issuer unable to collect the transaction funds from the consumer according to one embodiment of the invention.

[0018] Fig. 2 illustrates an exemplary system according to one embodiment of the invention.

[0019] Fig. 3A depicts an exemplary method according to one embodiment of the invention.

[0020] Fig. 3B depicts an exemplary repudiation process according to one embodiment of the invention.

[0021] Fig. 4A depicts an exemplary money transfer system according to one embodiment of the invention.

[0022] Fig. 4B depicts a money transfer method according to one embodiment of the invention.

[0023] Fig. 5A illustrates an exemplary master pool from which transaction settlement numbers may be selected according to one embodiment of the invention.

[0024] Fig. 5B depicts an exemplary method for populating a master pool according to one embodiment of the invention.

[0025] Fig. 6A depicts a method of generating an array of one-time-use credit card numbers according to one embodiment of the invention.

[0026] Fig. 6B depicts another method of generating a master pool of one-time-use credit card numbers according to one embodiment of the invention.

[0027] Fig. 7 depicts a method of generating an individual master pool of one-time-use credit card numbers for each credit card number according to one embodiment of the invention.

[0028] Fig. 8 depicts an assignment table according to embodiments of the present invention.

[0029] Fig. 9 depicts a method of assigning transaction settlement numbers from the master pool according to embodiments of the present invention.

[0030] Fig. 10 depicts a method of confirming the identity of user associated with a transaction settlement identifier according to one embodiment of the invention.

[0031] Fig. 11 depicts a method of confirming the identity of payee associated with a MTCN according to one embodiment of the invention.

[0032] Fig. 12 depicts a first exemplary method of a recipient-staged money transfer transaction.

[0033] Fig. 13 depicts a second exemplary method of a recipient-staged money transfer transaction.

DETAILED DESCRIPTION OF THE INVENTION

[0034] Embodiments of the present invention relate to systems and methods for assigning transaction settlement identifiers. In order to provide a context for describing embodiments of the present invention, embodiments of the invention will be described herein with reference to providing transaction settlement identifiers (aka "transaction settlement numbers") as one-time-use credit card numbers for purchase transactions and/or money transfer control number (MTCNs) for money transfer transactions. Those skilled in the art will appreciate, however, that other embodiments are possible. For example, embodiments of the invention may be used to provide brokerage account purchase and redemption transaction settlement numbers and the like.

[0035] The ensuing description provides preferred exemplary embodiment(s) only, and is not intended to limit the scope, applicability or configuration of the invention. Rather, the ensuing description of the preferred exemplary embodiment(s) will provide those skilled in the art with an enabling description for implementing a preferred exemplary embodiment of the invention. It is to be understood that various changes may be made in the function and arrangement of elements without departing from the spirit and scope of the invention as set forth in the appended claims.

[0036] Specific details are given in the following description to provide a thorough understanding of the embodiments. However, it will be understood by one of ordinary skill in the art that the embodiments may be practiced without these specific details. For example, systems may be shown in block diagrams in order not to obscure the embodiments in unnecessary detail. In other instances, well-known processes, structures and techniques may be shown without unnecessary detail in order to avoid obscuring the embodiments.

[0037] Also, it is noted that the embodiments may be described as a process which is depicted as a flowchart, a flow diagram, a data flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the operations may be re-arranged. A process is terminated when its operations are completed, but could have additional steps not included in the figure. A process may correspond to a method, a function, a procedure, a subroutine, a subprogram, etc. When a process corresponds to a function, its termination corresponds to a return of the function to the calling function or the main function.

[0038] Moreover, as disclosed herein, the term "storage medium" may represent one or more devices for storing data, including read only memory (ROM), random access memory (RAM), magnetic RAM, core memory, magnetic disk storage mediums, optical storage mediums, flash memory devices and/or other machine readable mediums for storing information. The term "computer-readable medium" includes, but is not limited to portable or fixed storage devices, optical storage devices, wireless channels and various other mediums capable of storing, containing or carrying instruction(s) and/or data.

[0039] Furthermore, embodiments may be implemented by hardware, software, firmware, middleware, microcode, hardware description languages, or any combination thereof. When implemented in software, firmware, middleware or microcode, the program code or code segments to perform the necessary tasks may be stored in a machine readable medium such as storage medium. A processor(s) may perform the necessary tasks. A code segment may represent a procedure, a function, a subprogram, a program, a routine, a subroutine, a module, a software package, a class, or any combination of instructions, data structures, or program statements. A code segment may be coupled to another code segment or a hardware circuit by passing and/or receiving information, data, arguments, parameters, or memory contents. Information, arguments, parameters, data, etc. may be passed, forwarded, or transmitted via any suitable means including memory sharing, message passing, token passing, network transmission, etc.

[0040] According to embodiments of the present invention, a biometric feature of an individual is used to generate a transaction identifier for subsequent use by the individual to complete a transaction. The transaction may be a purchase transaction, a money transfer transaction, or the like. The close association of the transaction identifier to the individual helps to minimize fraud associated with the transaction.

[0041] In the case of purchase transactions, a consumer provides a biometric sample to an issuer upon requesting the transaction identifier. The biometric sample may be a sample of any of a variety of biometric features of the consumer. For example, the consumer may provide a fingerprint, a voiceprint, DNA, retinal scan, or the like. Moreover, while embodiments of the present invention are described using a biometric feature of an individual to generate a transaction identifier, other physical identifiers may be used. For example, a PC signature or the keystroke dynamics of the user may be used. In such embodiments, the user may request a transaction identifier using a computer and use the PC signature or their keystroke dynamics to generate a transaction identifier. The PC signature or keystroke dynamics may be initiated locally by the user's computer or remotely through a network. Accordingly, while a biometric sample is used throughout the specification to describe embodiments of the invention, other physical identifiers uniquely identifying a user or user's system may be used to generate a transaction identifier.

[0042] The transaction identifier may be a one-time-use transaction identifier, such as a one-time-use credit card number, or the like. The issuer uses the biometric sample, or a function thereof (e.g., a hash), to select the transaction identifier from a large pool of transaction identifiers appropriate for the particular use. The consumer thereafter uses the transaction identifier to complete the transaction. In some cases, a second biometric sample is obtained from the consumer to authorize the transaction. In other cases, a second biometric sample is obtained only if the consumer attempts to repudiate the transaction.

[0043] In the case of money transfer transactions, a sender obtains a first transaction number upon depositing funds with a money transfer agent. The sender then provides the first transaction number to the desired recipient. The recipient then provides a biometric sample and the first transaction number to a money transfer system operator to receive a second transaction number (e.g., a MTCN, Money Transfer Control Number). The money transfer agent on the sender side, therefore, does not know the MTCN. The recipient then requests the funds deposited by the sender from a money transfer agent, which may be the same as the money transfer agent on the send side, but is most likely a different money transfer agent. At the time of request, the recipient provides the MTCN and a biometric sample. Only if the biometric sample matches the sample provided by the recipient to the money transfer system operator can the money transfer agent provide the funds. Hence, according to some embodiments, the transfer is protected from fraudulent collusion among money transfer agents since agents do not have access to transfer records using only an MTCN. Moreover, by providing a biometric sample at the time of receipt, a recipient is less able to claim not having received the funds. Further, embodiments of the present invention prevent multiple individuals from simultaneously requesting payment from different money transfer agents and receiving multiple payouts, since, presumably only one individual's biometric will result in transaction approval. Further still, collection of a biometric at the time of payment allows aggregation of transaction amounts for anti-money laundering compliance tracking.

[0044] Having described embodiments of the invention generally, attention is directed to Fig. 1A, which depicts a typical purchase transaction 100 in which a consumer uses a one-time-use credit card to complete a transaction with an online merchant. It will be appreciated, however, that, although embodiments of the present invention will be described herein with reference to online transactions using one-time-use credit cards, the present invention is not limited to such embodiments. This purchase transaction 100 begins at block 102 at which point a consumer requests and receives a one-time-use credit card number from an issuer. In doing so, the consumer provides, for example, an account number and password to the issuer. At block 104, the consumer uses the one-time-use credit card number to complete a purchase transaction with an online merchant. At block 106, the merchant obtains authorization for the transaction from the issuer, and the transaction is completed at block 108. Thereafter, the merchant obtains compensation for the transaction from the issuer at block 110, and the issuer obtains compensation from the consumer at block 112.

[0045] In the typical purchase transaction 100 of Fig. 1A, everything goes according to plan. Fig. 1B, however, depicts a purchase transaction 130 in which a fraudster acquires account details from the consumer leaving the issuer unable to collect the transaction funds from the consumer. The transaction 130 begins at block 132, at which point the fraudster obtains the consumer's account password. The fraudster then uses the password to obtain a one-time-use credit card number from the issuer (134) and complete a transaction with a merchant (136). Because the number appears to have been obtained by the consumer, the transaction is authorized (138) and completed (140). The merchant is able to obtain compensation from the issuer (142), but when the issuer attempts to obtain compensation from the consumer (144), the consumer is able to successfully repudiate the transaction (146). Hence, the issuer is penalized because of the consumer's failure to protect his password. Of course, the consumer may fraudulently repudiate the transaction, and the issuer has no ability to challenge him. Embodiments of the present invention provide a solution to this situation.

[0046] Attention is directed to Fig. 2, which illustrates an exemplary system 200 according to embodiments of the invention. Those skilled in the art will appreciate that the system 200 is merely exemplary of a number of possible system embodiments. The system includes a computer 202 associated with a consumer. The computer 202 may be any of a variety of well known computing devices such as, for example, a personal computer, a laptop computer, a personal digital assistant (PDA), a "Smart Phone,“ or the like. The consumer uses the computer 202 to communicate via a network 204 with a computer 206 associated with an issuer and/or an online merchant 208. The network 204 may be, for example, the Internet, but other embodiments are possible. The computer 206 associated with the issuer may be a host computer system that includes a mainframe computer, a collection of servers, and/or the like. The computer 206 has at least one associated data storage arrangement 210, which may be any of a variety of well know data storage arrangements. The computer 206 is programmed to perform the exemplary method embodiments disclosed herein.

[0047] The online merchant 208 may communicate with the issuer computer 204 via the network 204 or through a different network 212, which may be, for example, a credit card transaction processing network. The online merchant 208 communicates with the issuer to obtain authorization for credit card transactions.

[0048] According to some embodiments, the consumer obtains a one-time-use credit card by communicating with the issuer via the Internet. This assumes that the consumer is able to provide a biometric sample via the Internet. In other embodiments, the consumer may use a telephone 214 to contact the issuer via the PSTN (public switched telephone network) 216 or Internet using, for example VOIP (Voice Over Internet Protocol), to thereby provide a voice print. Those skilled in the art will appreciate, in light of the disclosure herein, a number of additional embodiments through which a consumer may provide a biometric sample to the issuer.

[0049] Having described an exemplary system 200, attention is directed to Fig. 3A, which depicts an exemplary method 300 according to embodiments of the invention. The method 300 may be implemented in the system 200 of Fig. 2 or other appropriate system. The method 300 begins at block 302 at which point a consumer requests a one-time-use credit card number from an issuer. The issuer obtains a biometric sample from the consumer at block 304 and uses the biometric sample to assign a one-time-use credit card to the consumer from a large pool of suitable one-time-use credit card numbers at block 306. Thereafter, the consumer provides the one-time-use credit card number to a merchant at block 308 in the process of completing a purchase transaction. The merchant obtains authorization for the transaction from the issuer at block 310, and the transaction is completed at block 312. The merchant thereafter obtains compensation from the issuer for the transaction at block 314, and the issuer obtains compensation from the consumer at block 316.

[0050] The method 300 depicts the typical case in which the consumer does not attempt to repudiate the transaction. Fig. 3B depicts what happens if the consumer attempts to repudiate the transaction.

[0051] Attention is directed to Fig. 3B, which depicts an exemplary repudiation process 320. At block 322, the consumer disputes the transaction. At block 324, the issuer obtains a biometric sample from the consumer. The issuer also retrieves the biometric sample used to assign the one-time-use credit card to the consumer at block 326. The issuer is then able to compare the two samples, and the consumer's ability to repudiate the transaction depends on the comparison. This is indicated by block 328.

[0052] Hence, according to embodiments of the invention, a consumer is less able to repudiate a transaction, due to the tight coupling between the consumer, using the biometric, and the issuance of the one-time-use number. Of course, the consumer could also claim that the one-time-use number was pilfered after issuance, but other controls may be used to limit such possibility. For example, a consumer may protect himself by requesting the number close in time to the planned usage. The issuer may protect itself by limiting the validity duration of the number to only a few minutes, a few hours, or a few days. The one-time-use nature of the number provides further protection for both the consumer and the issuer by preventing multiple uses of the number. Even further protection may be provided if the merchant takes a biometric sample from the consumer at the time of the purchase transaction. The merchant would then provide the sample to the issuer as part of the authorization process.

[0053] Those skilled in the art will appreciate a number of modifications and additional advantages to embodiments of the present invention in light of the disclosure herein. Moreover, in light of the disclosure herein, those skilled in the art will appreciate how the concepts disclosed herein by be applied to other types of transactions. For example, Figs. 4A and 4B depict an exemplary system 400 and exemplary method 430 for performing money transfer transactions according to embodiments of the present invention.

[0054] Attention is directed to Fig. 4A, which depicts an exemplary money transfer system 400 according to embodiments of the invention. The system 400 includes a sender agent location 402, at which a sender may deposit funds for receipt by a recipient. The sender location 402 may be a computer of the sender or may be a physical agent location (e.g., money transfer office, store, etc.) equipped to initiate money transfer transactions. The sender agent location communicates, via a network 404, with a money transfer system operator 406 to thereby receive a transaction identifier. Typically, a sender might receive a MTCN (Money Transfer Control Number) at this point, but that is not the case here. The sender receives a transaction identifier that cannot be used to obtain the funds like an MTCN could. The transaction identifier is stored at a storage arrangement 407 associated with the money transfer system operator.

[0055] The system 400 also includes a telephone 408 associated with a recipient and the PSTN (public switched telephone network) 410 though which the recipient may communicate with the money transfer system operator 406. The recipient, having received the transaction identifier from the sender, is able to provide the transaction identifier and a biometric sample to thereby obtain the MTCN. Those skilled in the art will appreciate many additional means through which the recipient may provide a biometric sample to and obtain a MTCN from the money transfer system operator.

[0056] The system also includes a recipient agent location 412 at which the sender may request payment. The sender agent location 412 is able to obtain a biometric sample from the recipient, communicate the biometric sample, along with the MTCN, to the money transfer system operator 406, and receive authorization to pay the recipient. The recipient is paid only if the biometric the recipient provides matches the biometric supplied to obtain the MTCN.

[0057] Having described the money transfer system 400, attention is directed to Fig. 4B, which depicts a money transfer method 430 according to embodiments of the invention. The method 430 may be implemented in the system 400 of Fig. 4A or other appropriate system. The method 430 begins at block 432, at which location a sender deposits funds with a money transfer agent and obtains a transaction number. The transaction number is provided by the money transfer system operator. The sender provides the transaction number to the designated recipient at block 434. The recipient contacts the money transfer system operator at block 436 and supplies the transaction identifier and a biometric sample to thereby receive the MTCN. The MTCN is generated by the money transfer system operator according to the embodiments of the invention.

[0058] At block 438, the recipient requests payment from a money transfer agent. The agent collects the MTCN and a biometric sample from the recipient at block 440 and supplies them to the operator at block 442 as part of an authorization request. The operator uses the MTCN to locate the biometric sample provided to obtain the MTCN and authorizes the agent to pay the recipient only if the samples match, which takes place at block 444.

[0059] Those skilled in the art will appreciate that the aforementioned embodiments are merely exemplary. Moreover, it will be appreciated that the any of a variety of methods may be employed to generate one-time-use credit card numbers, MTCNs, and the like from a biometric sample. In may embodiments, the one-time-use credit card number or MTCN is selected from a large pool of appropriately selected numbers using the biometric sample or a function of a biometric sample, but this is not required. The ensuing description, however, provides exemplary methods for generating a master pool, selecting numbers from the pool, and authorizing transactions using numbers selected from the pool.

[0060] Attention is directed to Fig. 5A, which illustrates an exemplary master pool 500 from which transaction settlement numbers may be selected. The transaction settlement numbers may be one-time-use credit card numbers, as in this example, or may be MTCNs, or the like in other embodiments. The master pool 500 includes a "record number" field, a "one-time CC#" field, and an "assignment table pointer" field. The record number field, in this exemplary embodiments, is numbered consecutively throughout the records in the pool, and the pool includes a sufficient number of records to satisfy expected demand for the transaction settlement numbers. The one-time CC# field includes a unique transaction settlement number in each record, and the field of each record is populated randomly as will be described with reference to Fig. 5B. The assignment table pointer field of each record maintains a pointer to a record in an assignment table. The assignment table will be described below with reference to Fig. 8. When a transaction settlement number is assigned, the assignment table pointer field is populated as will be described below with reference to Fig. 9.

[0061] Fig. 5B depicts an exemplary method 530 for populating a master pool. At block 532, an array of conforming numbers is generated. The numbers conform to appropriate specification for which the transaction settlement numbers will be used. For example, in this embodiment, the transaction settlement numbers are one-time-use credit card numbers, and the numbers which are sixteen digits long and include no letters. The numbers are in appropriate ranges (e.g., BIN ranges) to thereby prevent duplication with typical credit cards. In other examples, the transaction settlement numbers may be MTCNs, which would be appropriately formatted according to the desired specifications for MTCNs. Many such examples are possible.

[0062] At block 534, a first transaction settlement number is randomly selected from the from the array. At block 536 a determination is made whether the transaction settlement number has already been selected. If it has, another transaction settlement number is randomly selected at block 534. If the selected number has not been selected yet, the number is inserted into the master pool at block 538. The process continues, consecutively populating records of the master pool with transaction settlement numbers, until the master pool is fully populated with random selections of transaction settlement numbers from the array. Those skilled in the art will appreciate that this is but one exemplary method for populating an exemplary master pool.

[0063] Fig. 6A depicts another method 600 for generating an array of one-time-use credit card numbers. In this embodiment, an array of one-time-use credit card numbers is generated. This array is used to assign one-time-use credit card numbers to a user and/or a master pool.. At block 610 a one-time-use credit card number is created, which, according to specific embodiments, conforms to appropriate formats and/or standards for which the number will be used (e.g., credit care number, MTCN, etc.). The one-time-use credit card number is adjusted to comply with format and content specifications developed by the industry at block 615. The one-time-use credit card number is then stored in a one-time-use credit card number array at block 620 whereupon the system returns to block 610. Other means for storing the one-time-use credit card number may be used, such as a linked list, a generic file, a text file, etc.

[0064] Fig. 6B depicts a method 650 of generating a master pool of one-time-use credit card numbers according to one embodiment of the invention. At block 625 the record number is initiated and set to 1. A one-time-use credit card number is selected from a one-time-use credit card number array at block 630. The array may be the array generated at block 620 of Fig. 6A. This number may be selected randomly, incrementally or systematically. Furthermore, the system may also select the one-time-use credit card number from any other storage location. Once the number is selected, the system, at block 635, determines if it is currently in use or not. If it is currently in use, then the system returns to block 630 and another one-time-use credit card number is selected. The one-time-use credit card number may also be deleted from the one-time-use credit card number array. If the one-time-use credit card number is not in use, the one-time-use credit card number is inserted into the master pool 650 at block 640 at the location associated with the record number. The record number is incremented at block 645 and the system selects another number from the one-time-use credit card number array at block 630 whereupon the system is repeated.

[0065] Fig. 7 depicts a method 700 of generating an individual master pool of one-time-use credit card numbers for each credit card according to one embodiment of the present invention. While this embodiment generates and stores one-time-use credit card numbers in a pool, the method may be used for any type of transaction settlement number. According to this embodiment, each credit card number has an associated pool of one-time-use credit card numbers 730. Each one-time-use credit card number pool 730 may be a fixed size or the size may be adjusted dynamically according to the number of one-time-use credit card numbers used or required by the user.

[0066] A credit card number is selected at block 710 for populating the one-time-use credit card number pool 730 associated with the credit card number. A one-time-use credit card number is randomly generated at block 715. Generation of the one-time-use credit card number may also include steps to ensure the one-time-use credit card number complies with industry specifications. At block 720, the method determines if the one-time-use credit card number generated at block 715 is unique, if it is not unique, the method returns to block 715.

The system may determine if the one-time-use credit card number is unique by refereeing to a list or array of issued credit card numbers, unissued credit card numbers or the like. If the one-time-use credit card number is unique, the method moves to block 725. At block 725, the one-time-use credit card number pool record number is incremented. At block 735, the system determines if the one-time-use credit card number pool is full. If the pool is full, the system returns to block 710, where another credit card number is selected. In alternative embodiments, the size of the one-time-use credit card number pool 730 may be increased and the system moves along to block 740. In other embodiments, more than one-time-use credit card number pool may be associated with the credit card number. At block 740, the randomly produced one-time-use credit card number is entered into the one-time-use credit card number pool and the system returns to block 715.

[0067] Attention is directed to Fig. 8, which depicts an assignment table 800 according to embodiments of the present invention. The assignment table 800 maps starting numbers to transaction settlement numbers in the master pool 500. The starting numbers maybe, for example, a consumer's credit card account number, as in this example, a transaction identifier provided to a sender in a money transfer transaction, or the like. The assignment table 800 includes a "key" filed, a "record number" field, a "real CC#" field, a "usage conditions" field, a "previous pointer" field, and a "next pointer" field.

[0068] The key field provides an index to the assignment table. According to embodiments of the invention, the key field is based on a biometric sample as will be described in greater detail with respect to Fig. 9. The record number field identifies a record in the master pool. The "real CC#" field stores the starting number from which the transaction settlement number is generated. In other exemplary embodiments, the real CC# field may be, for example, the transaction identifier provided to the sender in a money transfer transaction. The usage conditions field may include any of a variety of usage conditions associated with the transaction settlement number. For example, the usage conditions field may identify a limited number of merchants at which the transaction settlement number may be used. It may include an expiration time and/or date for the number, and/or the like. Those skilled in the art will appreciate a number of additional conditions that may be included in the usage number field. The previous and next pointers identify previous and next assignment table records in a daisy chain of records assigned to a common consumer, customer, recipient, or the like, as will be described in greater detail with respect to Fig. 9.

[0069] The assignment table 800, unlike the master pool 500, is not fully populated initially. Additional records are added as transaction settlement numbers are requested and assigned by the issuer. A "last record assigned" pointer is used in the process of assigning transaction settlement numbers as will be described with respect to Fig. 9.

[0070] Attention is directed to Fig. 9, which depicts a method 900 of assigning transaction settlement numbers from the master pool according to embodiments of the present invention. At block 902, a request for a transaction settlement number is received from a customer. In this embodiments, the request is for a one-time-use credit card number and the request is received by an issuer. In other embodiments, the request may be for a MTCN and be received by a money transfer system operator. The request includes a biometric sample (e.g., a voiceprint) from the customer. The request also identifies the customer's credit card account. For example, the customer may have used a USER ID and password to access an account electronically, and the account includes a feature that allows the customer to request a one-time-use credit card number.

[0071] At block 904, the issuer creates a hash of the biometric sample, thereby producing #V. In this embodiment, the hashing algorithm produces a #V that is repeatable for different biometric samples of the same individual. In other embodiments, a function other than hashing may be used to produce #V. In other embodiments, the function may not produce a #V that is repeatable for different biometric samples of the same individual.

[0072] At block 906, #V is used to search the assignment table. At block 908, a determination is made whether #V has been used previously as an assignment table key. If not, the process continues at block 910. If so, the process continues at block 918 as will be described below.

[0073] At block 910, #V is populated into the key field of a new assignment table record. At block 912, the "last record assigned" pointer is incremented to point to the next, unassigned, record in the master pool. At block 914, the record # of the indicated record of the master pool is populated into the record # field of the new record of the assignment table. The customer's real credit card account number is populated into the real CC# field of the new assignment record, the key of the new assignment record is populated into the assignment pointer field of the current master pool record, and any usage conditions are populated into the usage conditions field of the assignment record. The next and previous pointers of the new assignment record are populated appropriately as will be described in greater detail hereinafter.

[0074] At block 916, the transaction settlement number is returned to the customer. The customer may thereafter use the transaction settlement number in an appropriate transaction.

[0075] Returning to block 910, if #V has been used previously (i.e., a record in the assignment table has the value #V as a key), blocks 912 and 914 are traversed repeatedly until the last assignment table record in the chain is located. Locating the last record in the chain, however, requires knowing how subsequent keys are assigned.

[0076] Each time a customer requests a transaction settlement number (e.g., a one-time-use credit card number), a new key is created. The first key is #V. The second key is #V XOR the first transaction settlement number assigned to the customer. Third key is the second key XOR the second transaction settlement number assigned to the customer, and so on. Hence, each new key incorporates together the customer's biometric and each previously assigned transaction settlement number.

[0077] Returning to the discussion of Fig. 9, if a record in the assignment table is located using #V, then the master pool record stored in the assignment table is used to locate the previously assigned transaction settlement number. The next key is then created by performing an XOR function of #V and the previously assigned transaction settlement number. This key is used to search the assignment table, and if a record is located, the next key in the sequence is created and the table is searched again. This process continues until a search of the assignment table does not return a record. The current key then becomes the key of the new record in the assignment table created at block 922.

[0078] It should now be apparent to those skilled in the art that the next and previous pointer fields may be, at block 914, populated to assist with searches of the assignment table. This will be particularly useful during authorization and dispute resolution processes as will be described in greater detail hereinafter with reference to Figs. 10 and 11.

[0079] Fig. 10 shows a method 1000 for confirming the identity of a user by comparing a received biometric sample and the stored sample to detect for fraudulent transactions according to one embodiment of the invention. The method 1000 shown may be used for any type of transaction settlement identifier, such as, for example, one-time-use credit card numbers and/or MTCN's. In light of the embodiment described in the figure, those skilled in the art will recognize other embodiments well within the scope of the invention.

[0080] At Block 1010 a user contacts issuer to dispute a transaction they consider to be fraudulent. The user's identity may need confirmation because the user may deny requesting and having been issued a one-time-use credit card number and, therefore, deny making a transaction with the one-time-use credit card number. The user may also wish to confirm their identity in order to receive a payout.

[0081] At block 1015, the issuer receives the transaction settlement number from the user as well as a biometric sample at block 1020. After receiving the biometric feature, the issuer creates a hash (#H) of the biometric sample at block 1025 using a hashing algorithm as discussed above. The issuer may then retrieve the record associated with the transaction settlement number at block 1030, for example, from the assignment table.

[0082] The record retrieved at block 1030, may contain the transaction settlement number, and a unique key. The record may also contain previous and next pointers. The previous and next pointers link the records for a particular user in a chain like fashion. As described above, the key associated with each transaction settlement number may be a mathematical combination of the previous key and the previous transaction settlement number. The first key associated with a user is the hash of the biometric sample. Thus, at block 1035, the method determines whether this record associated with the transaction settlement number is the first record in the chain. If the previous pointer is NULL, then the record is the first record in the chin. f it is not the first record the method retrieves the previous record at block 1040. If the previous pointer equals NULL then the record is the first record. Between blocks 1035 and 1040, the method traverses the chain of records to find the first record. Once the first record is found the stored hash of the biometric sample (#V) is the key associated with the first record. At block 1045, the method determines whether the received biometric sample hash (#H) equals the stored hash of the stored biometric sample (#V). If the two hashed samples match, the identity of the user is confirmed at block 1050. If the two hashed samples do not match, the identity of the user is not confirmed.

[0083] The method 1000, for example, may be applicable in a system generating one-time-use credit card numbers, where a one-time-use credit card number is the transaction settlement number. In such systems, a user receives a one-time-use credit card number upon receipt of a biometric sample. If a user claims that they did not request a one-time-use credit card number, the biometric sample received from the user and stored when the one-time-use credit card number was issued may be used to either confirm or deny the users claim. For example, the user contacts the issuer at block 1010, the credit card number is received 1015, and a biometric sample is received 1020. The stored biometric sample used when the one-time-use credit card number was issued is retrieved in blocks 1030, 1035 and 1040 and the chain of records may be traversed. The biometric samples are compared. If the hash of the biometric sample received when the one-time-use credit card number was issued matches the hash of the biometric sample received at block 1020, then the user's claim is denied, because the one-time-use credit card number was issued to the user and not a fraudster. Otherwise, if there is no match, the user may have a genuine fraud claim, whereupon the issuers may initiate procedures to address the fraudulent activity.

[0084] Fig. 11 shows a method 1100 for confirming the identity of a user in a money transfer transaction according to one embodiment of the invention. In such transactions, in order to avoid fraudsters, a payout may only be received by first confirming the identity of the payee. Blocks 1110, 1115, 1120, 1125, 1130, 1135, 1140 and 1145 are similar to blocks 1010, 1015, 1020, 1025, 1030, 1035, 1040 and 1045 of Fig. 10, except in this method 1100 the transaction settlement identifier is a MTCN. At block 1145, if the hash of the received biometric sample does not match the hash of the stored biometric sample, then the payout is denied. If the two hashes match, then the method determines whether the aggregate payout to the user is greater than some predetermined threshold at block 1160. Legally, money transfers greater than a certain amount, must meet certain compliance requirements to deter money laundering. The aggregate payout may be determined by moving through the daisy chain of records and summing the payout of all transaction. If the aggregate payout is greater than the threshold then compliance requirements must be satisfied at block 1165 before payout occurs at block 1151. Those skilled in the art will recognize how to implement various compliance procedures. If the aggregate payout is not greater than the threshold then payout at block 1151 may occur.

[0085] Attention is directed to Figs. 12 and 13, which depict exemplary embodiments of recipient-staged money transfer transaction. In these embodiments, a recipient "stages" a transaction by providing a biometric sample and receiving a transaction control number. The recipient also may provide other transaction details, but this is not necessary. The recipient provides the transaction control number to a sender, who then deposits funds using the transaction control number. The funds can then be released only upon the recipient providing a confirming biometric sample. The embodiments 1200 and 1300 provide two different ways in which this can be accomplished.

[0086] According to the embodiment 1200 of Fig. 12, a recipient stages a transaction at block 1210. This includes providing a biometric sample. The recipient may stage the transaction using a phone and providing a voice sample, visiting a money transfer location and providing another type of biometric sample, or using any of a variety of other ways apparent to those skilled in the art in light of this disclosure. The sample or a derivative thereof is stored in a transaction record, and the recipient is provided with a transaction control number at block 1212, which the recipient provides to a sender at block 1214.

[0087] At block 1216, the sender deposits funds and provides any additional details necessary to create the transaction. The transaction record established by the recipient is accessed using the transaction control number provided to the sender by the recipient. At this point, the ability to receive the funds is closely tied to the recipient via the biometric sample. The blocks 1210, 1212, 1214, and 1216 are substantially similar to the corresponding blocks 1310, 1312, 1314, and 1316 of the embodiment 1300 of Fig. 13.

[0088] The recipient can now receive the funds in any of several ways. According to the embodiment 1200 of Fig. 12, the recipient requests funds at a money transfer location and provides a biometric sample at block 1218. A determination is made at block 1220 whether the sample matches the sample provide at the time the transaction was staged. If is does not, then payout is denied at block 1222. If the sample matches, the payout is made at block 1224.

[0089] According to the exemplary embodiment 1300 of Fig. 13, a recipient is able to receive the funds electronically or at a money transfer location this is not equipped to take a biometric sample. At block 1318, the recipient requests a MTCN by providing a biometric sample. The recipient can request the biometric sample by, for example, phoning the money transfer system operator. At block 1320, a decision is made whether the sample matches the sample obtained at the time the transaction was staged. If is does not, the MTCN is not provided to the recipient, as indicated by block 1322. If, however, the samples match, the a MTCN is provided to the recipient at block 1324.

[0090] Thereafter, the recipient may use the MTCN to access the funds in any of a variety of ways, including by visiting a money transfer location, accessing an account electronically, and the like, as is apparent to those skilled in the art in light of this disclosure.

[0091] Having described several embodiments, it will be recognized by those of skill in the art that various modifications, alternative constructions, and equivalents may be used without departing from the spirit and scope of the invention. Additionally, a number of well known processes and elements have not been described in order to avoid unnecessarily obscuring the present invention. For example, those skilled in the art know how MTCNs are used in money transfer transactions and how one-time-use credit card purchase transactions are settled. Moreover, those skilled in the art will appreciate that the concepts discussed herein may be directed toward other types of transactions. Accordingly, the above description should not be taken as limiting the scope of the invention, which is defined in the following claims.

WHAT IS CLAIMED IS:

1. A money transfer system, comprising:

an input adapted to receive biometric samples;

a storage arrangement configured to store the biometric samples or derivatives thereof; and

a processor;

wherein the processor comprises instructions to:

use a first biometric sample to select a MTCN (money transfer control number) from a pool of predetermined MTCNs; and

link the first biometric sample to the MTCN.

2. The system of claim 1, wherein the biometric sample comprises a selection from the group consisting of: a voiceprint, a fingerprint, a retinal scan, and a DNA sample.

3. The system of claim 1, wherein the processor further comprises instructions to respond to a request to settle a transaction using the MTCN by receiving a second biometric sample and comparing the second biometric sample to the first biometric sample.

4. The system of claim 1, wherein the processor further comprises instructions to determine whether to provide funds to a recipient by determining whether the funds have been paid out.

5. The system of claim 1, wherein the processor further comprises instructions to determine whether to provide the funds to the recipient by determining whether an amount of the funds exceeds a threshold amount of funds transferred for which compliance is required.

6. A method of transferring funds from a sender to a recipient, comprising:

receiving a request to transfer the funds from the sender;

creating a transaction record having a transaction identifier;

providing the transaction identifier to the sender;

receiving the transaction identifier from a recipient;

obtaining a first biometric sample from the recipient;

using the biometric sample to select a MTCN (Money Transfer Control Number) from a pool of predetermined MTCNs;

associating the MTCN with the first biometric sample and the transaction record;

providing the MTCN to the recipient;

thereafter, receiving a request from the recipient to receive the funds;

obtaining the MTCN from the recipient;

obtaining a second biometric sample from the recipient;

using the MTCN and/or the second biometric sample to locate the transaction record;

comparing the second biometric sample to the first biometric sample; and

determining whether to provide the funds based on the comparison.

7. The method of claim 6, wherein determining whether to provide the funds based on the comparison comprises determining whether the funds have been paid out.

8. The method of claim 6, wherein determining whether to provide the funds based on the comparison comprises determining whether an amount of the funds exceeds a threshold amount of funds transferred for which compliance is required.

9. The method of claim 6, wherein the each biometric sample comprises a selection from the group consisting of: a voiceprint, a fingerprint, a retinal scan, and a DNA sample.

10. A method of transferring funds from a sender to a recipient, comprising:

receiving a request from the recipient to stage the transaction;

obtaining a first biometric sample from the recipient;

using the first biometric sample to select a transaction number from a pool of predetermined transaction numbers;

creating a transaction record having the transaction number and the first biometric sample associated therewith;

providing the transaction number to the recipient;

receiving a request from the sender to deposit the funds;

receiving the transaction number from the sender;

modifying the transaction record to indicate that the funds have been deposited;

thereafter, receiving a request from the recipient to receive the funds; and using a second biometric sample, at least in part, to determine whether to provide the funds to the recipient.

11. The method of claim 10, wherein using a second biometric sample, at least in part, to determine whether to provide the funds to the recipient comprises:

receiving the transaction number from the recipient;

obtaining the second biometric sample from the recipient;

using the transaction number and/or the second biometric sample to locate the transaction record;

comparing the first biometric sample to the second biometric sample; and

based on the comparison, determining whether to issue a MTCN (Money Transfer Control Number).

12. The method of claim 11, comprising:

thereafter, receiving the MTCN at a money transfer location; and

providing the funds to the recipient.

13. The method of claim 11, wherein determining whether to issue a MTCN comprises determining whether the funds have been paid out.

14. The method of claim 10, wherein determining whether to issue a MTCN comprises determining whether an amount of the funds exceeds a threshold amount of funds transferred for which compliance is required.

15. The method of claim 10, wherein using a second biometric sample, at least in part, to determine whether to provide the funds to the recipient comprises:

at a money transfer location, receiving a request to receive the funds from the recipient;

receiving the transaction number from the recipient;

using the transaction number to locate the transaction record;

obtaining the second biometric sample from the recipient; and

comparing the first biometric sample to the second biometric sample.

16. The method of claim 10, wherein using a second biometric sample, at least in part, to determine whether to provide the funds to the recipient comprises determining whether the funds have been paid out.

17. The method of claim 10, wherein using a second biometric sample, at least in part, to determine whether to provide the funds to the recipient comprises determining whether an amount of the funds exceeds a threshold amount of funds transferred for which compliance is required.

18. The method of claim 10, wherein the biometric sample comprises a selection from the group consisting of: a voiceprint, a fingerprint, a retinal scan, and a DNA sample.

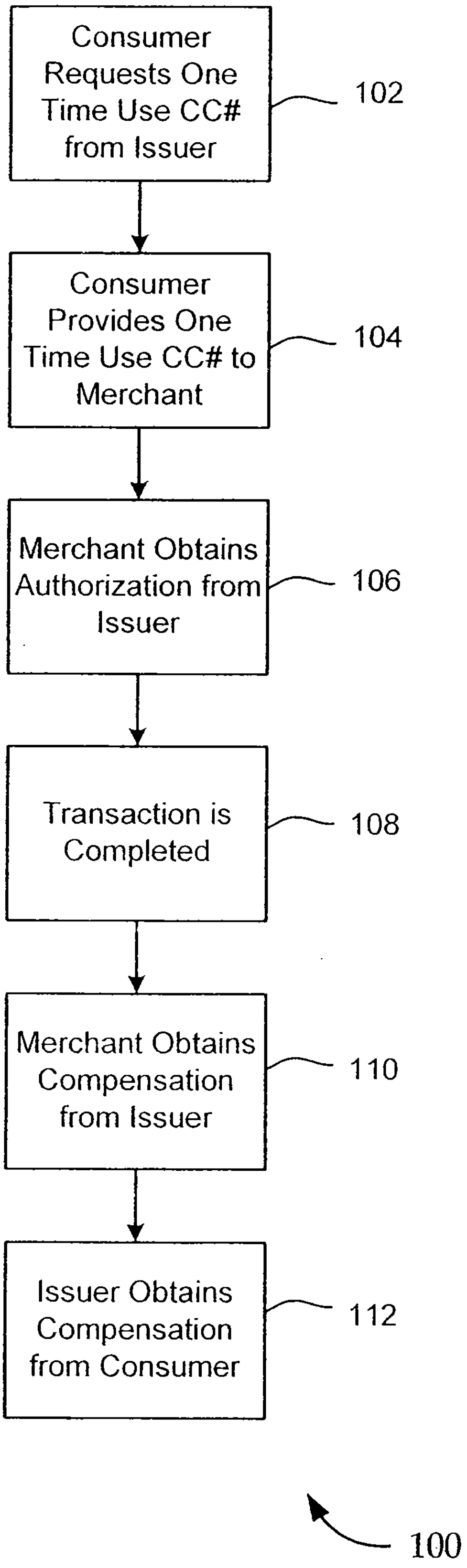

Consumer Requests One Time Use CC# from Issuer
102
Consumer Provides One Time Use CC# to Merchant
104
Merchant Obtains Authorization from Issuer
106
Transaction is Completed
108
Merchant Obtains Compensation from Issuer
110
Issuer Obtains Compensation from Consumer
112
100

FIG. 1A

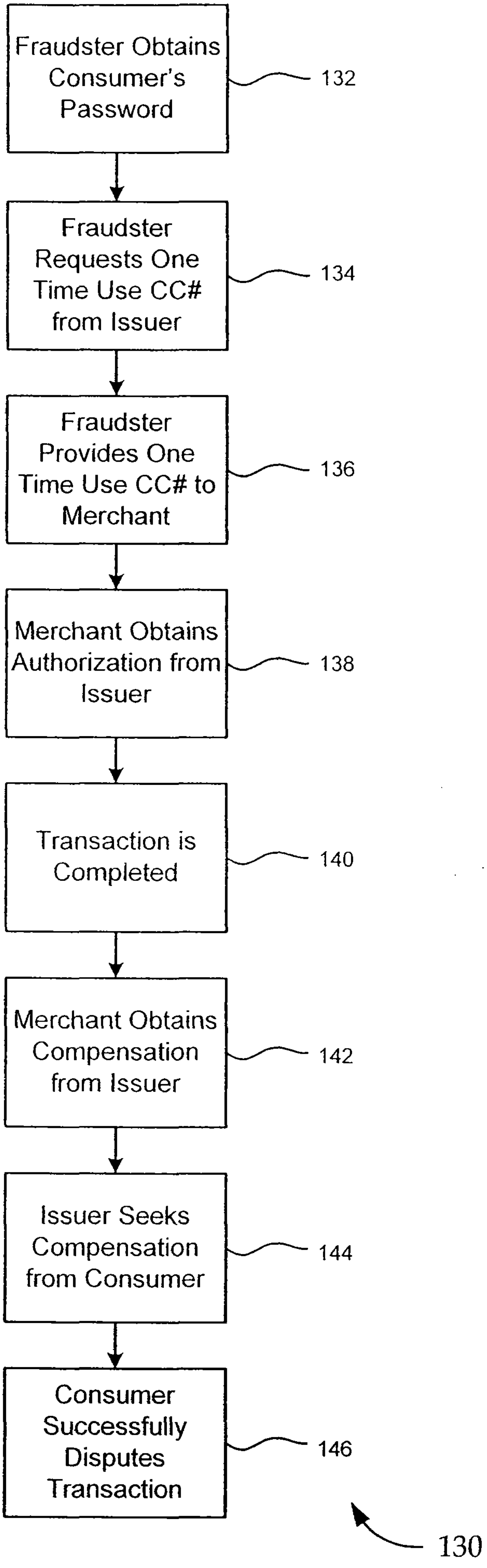

Fraudster Obtains Consumer's Password
132
Fraudster Requests One Time Use CC# from Issuer
134
Fraudster Provides One Time Use CC# to Merchant
136
Merchant Obtains Authorization from Issuer
138
Transaction is Completed
140
Merchant Obtains Compensation from Issuer
142
Issuer Seeks Compensation from Consumer
144
Consumer Successfully Disputes Transaction
146
130

FIG. 1B

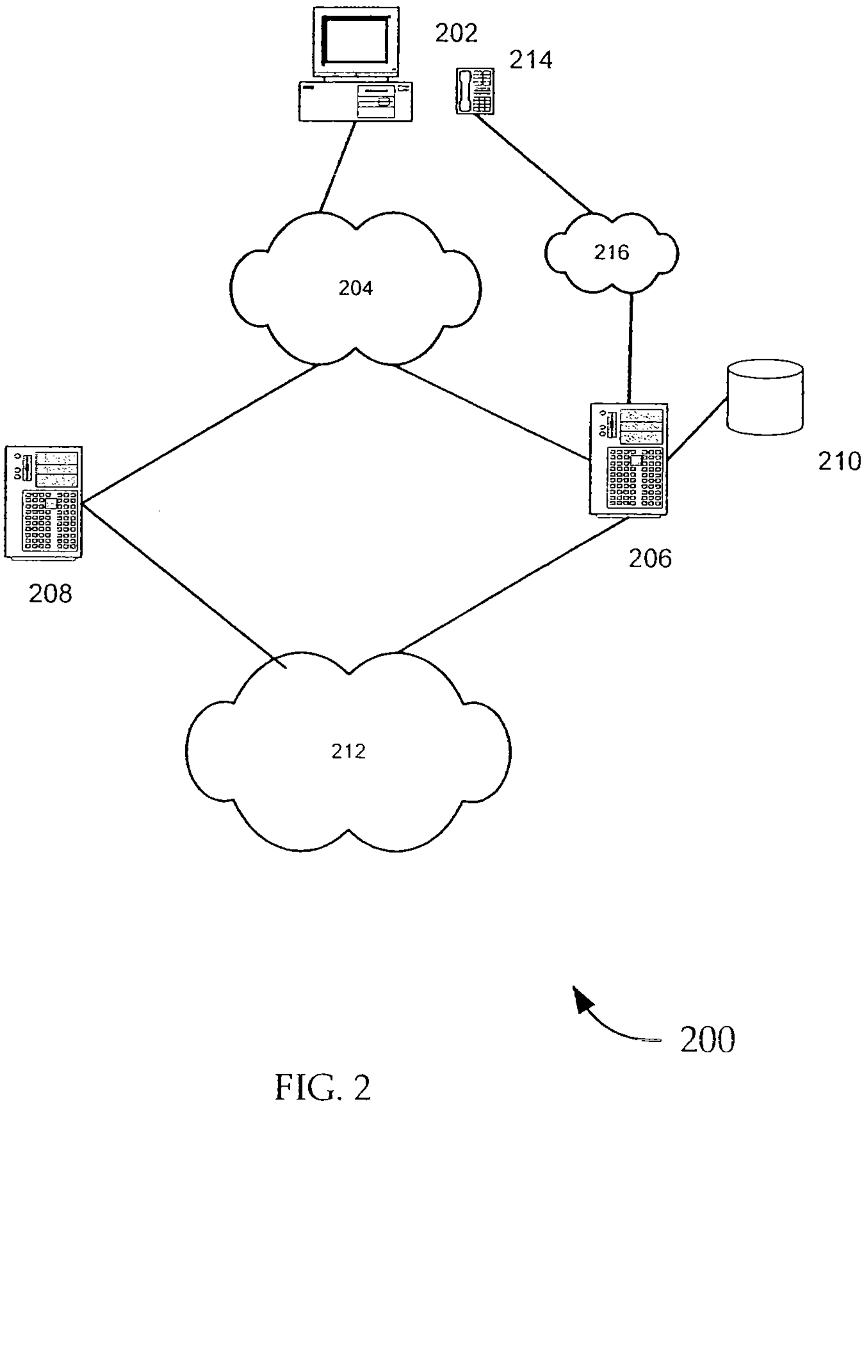


FIG. 2

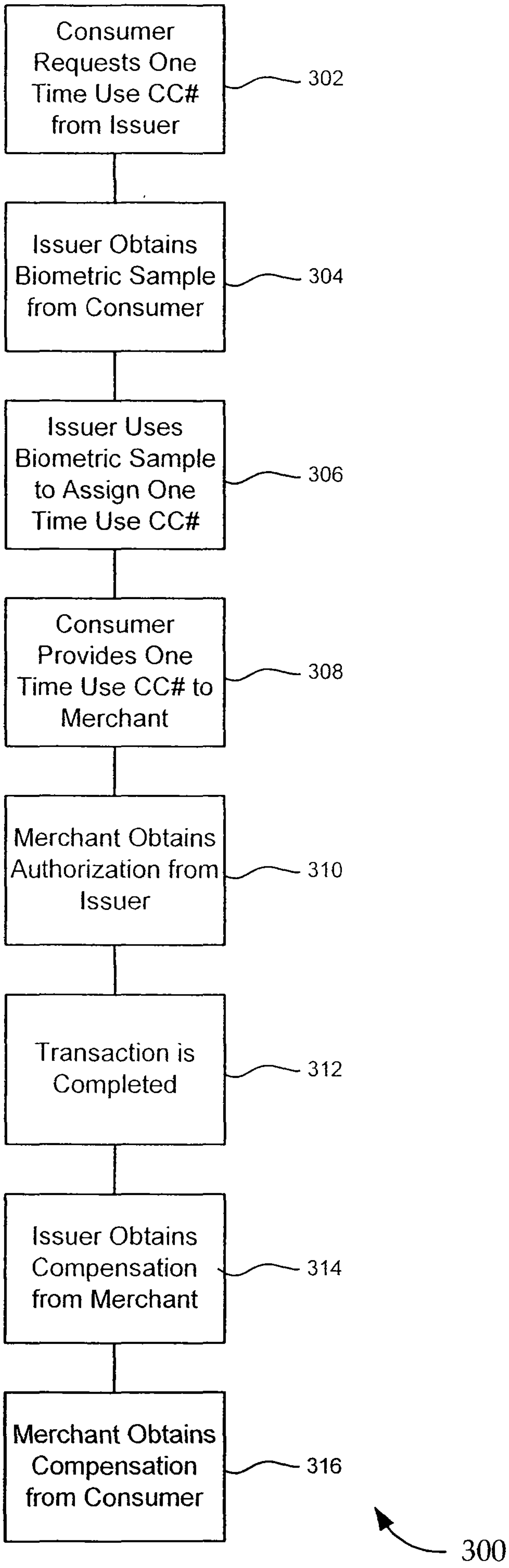

Consumer Requests One Time Use CC# from Issuer
302
Issuer Obtains Biometric Sample from Consumer
304
Issuer Uses Biometric Sample to Assign One Time Use CC#
306
Consumer Provides One Time Use CC# to Merchant
308
Merchant Obtains Authorization from Issuer
310
Transaction is Completed
312
Issuer Obtains Compensation from Merchant
314
Merchant Obtains Compensation from Consumer
316
300

FIG. 3A

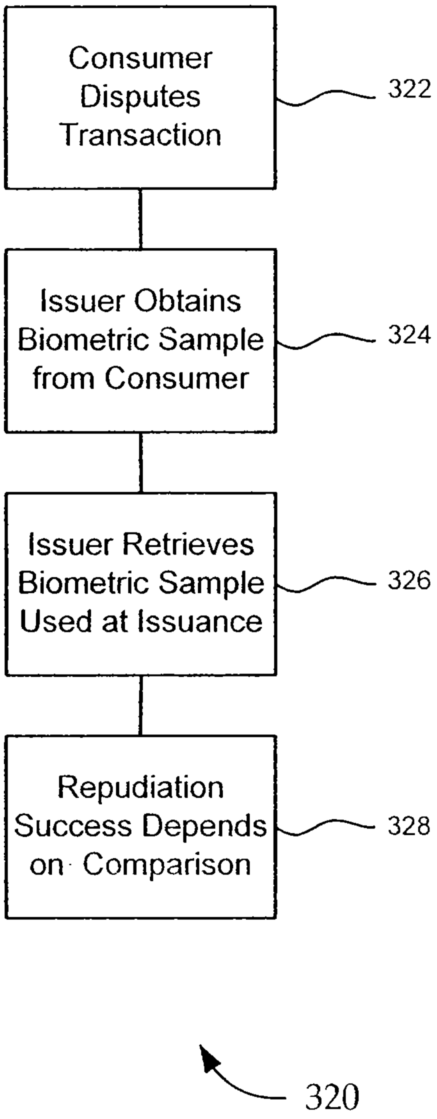

Consumer Disputes Transaction
322
Issuer Obtains Biometric Sample from Consumer
324
Issuer Retrieves Biometric Sample Used at Issuance
326
Repudiation Success Depends on Comparison
328
320

FIG. 3B

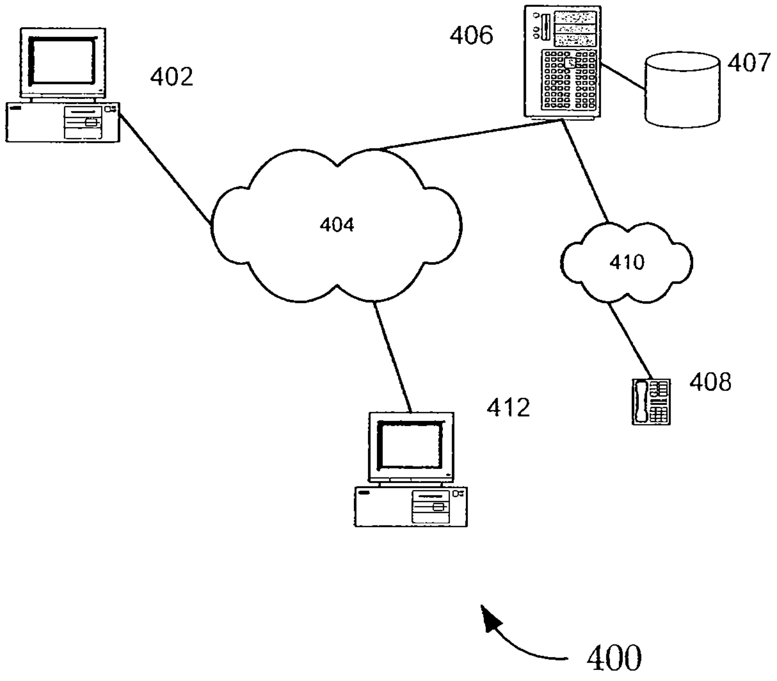


FIG. 4A

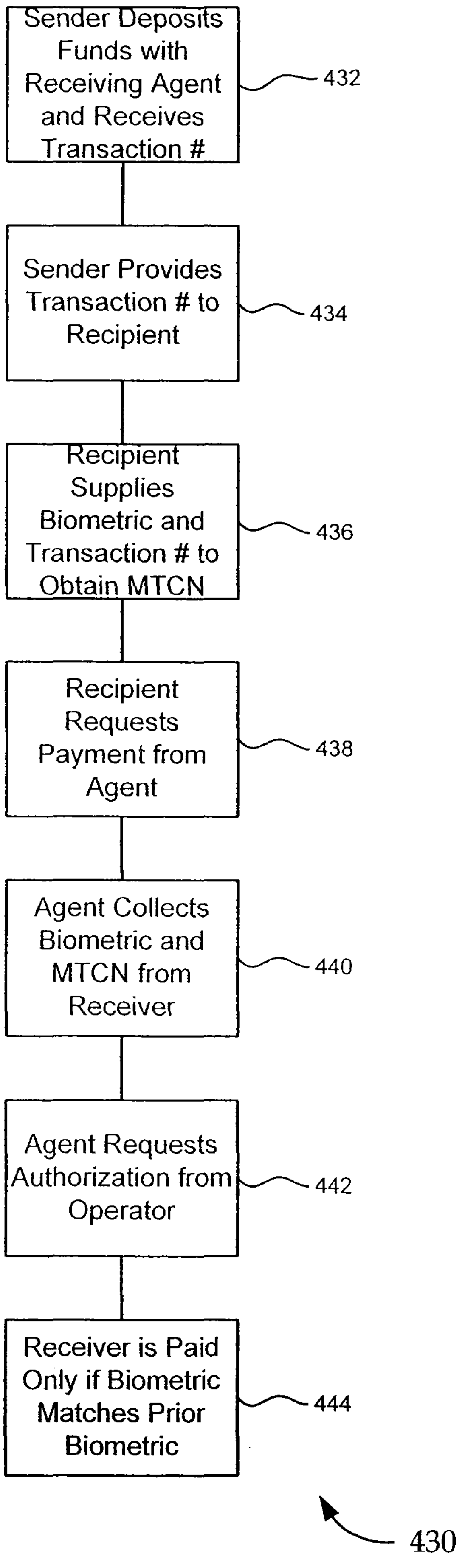

Sender Deposits Funds with Receiving Agent and Receives Transaction #
432
Sender Provides Transaction # to Recipient
434
Recipient Supplies Biometric and Transaction # to Obtain MTCN
436
Recipient Requests Payment from Agent
438
Agent Collects Biometric and MTCN from Receiver
440
Agent Requests Authorization from Operator
442
Receiver is Paid Only if Biometric Matches Prior Biometric
444
430

FIG. 4B

Record #	One Time CC#	Assignment Table Pointer
000,000,001	4891-3280-4378-2190	
000,000,002	1367-9329-4275-0183	
000,000,003	3740-1480-9642-4473	
⋮	⋮	⋮
005,000,001	9416-3551-8814-0178	532

500

FIG. 5A

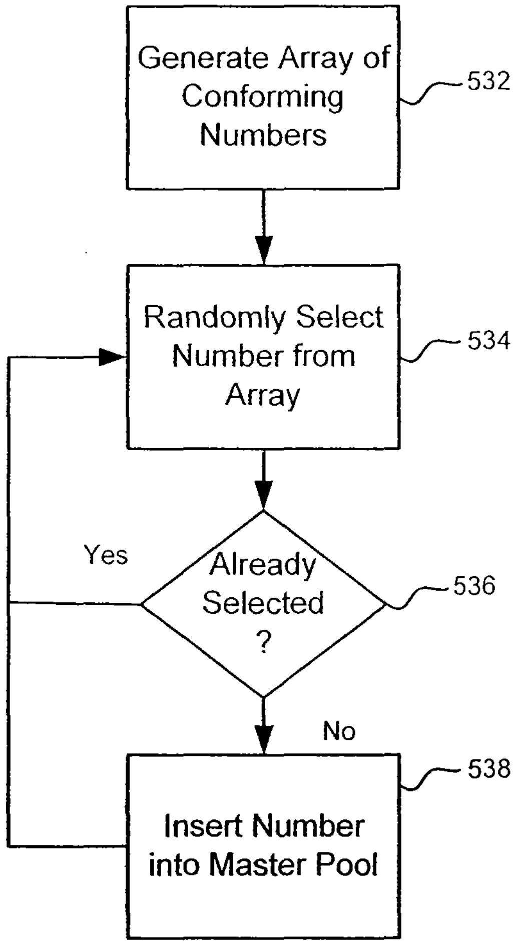

Generate Array of Conforming Numbers
532
Randomly Select Number from Array
534
Yes
Already Selected ?
536
No
538
Insert Number into Master Pool
530

FIG. 5B

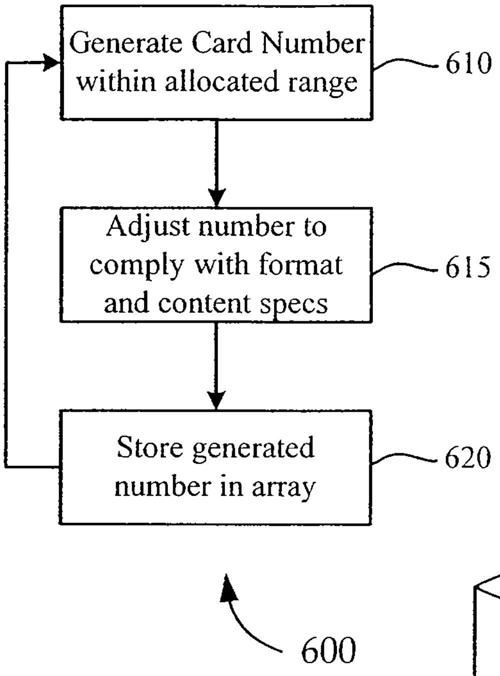

Generate Card Number within allocated range
610
Adjust number to comply with format and content specs
615
Store generated number in array
620
600

FIG. 6A

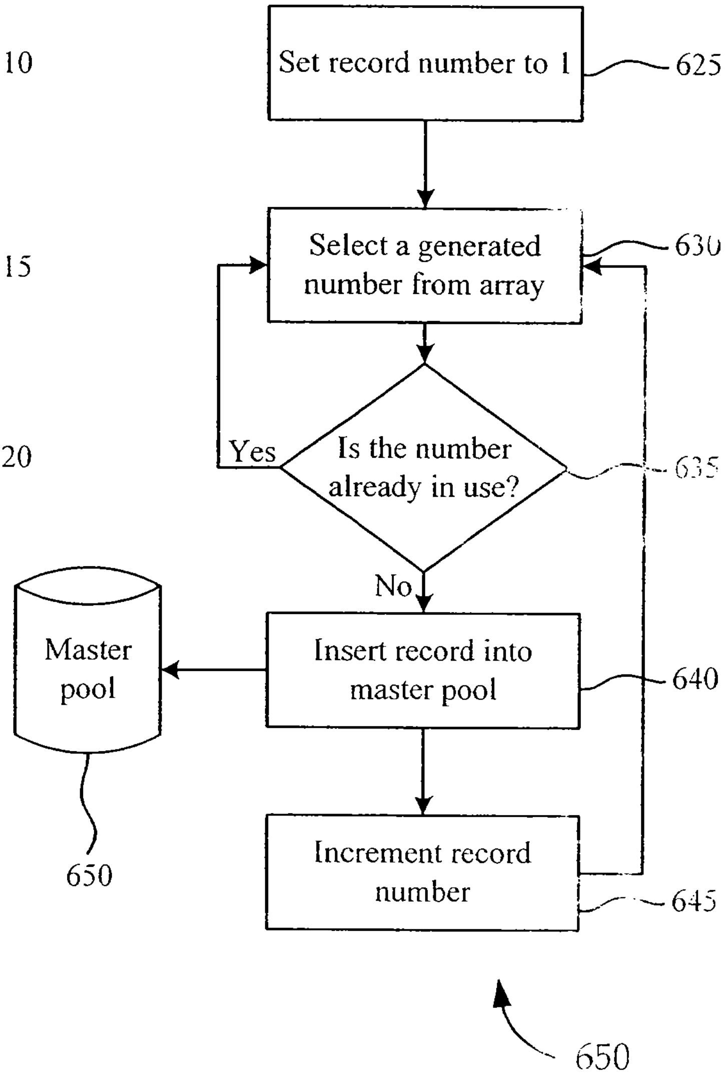

Set record number to 1
625
Select a generated number from array
630
Is the number already in use?
635
Yes
No
Master pool
650
Insert record into master pool
640
Increment record number
645
650

FIG. 6B

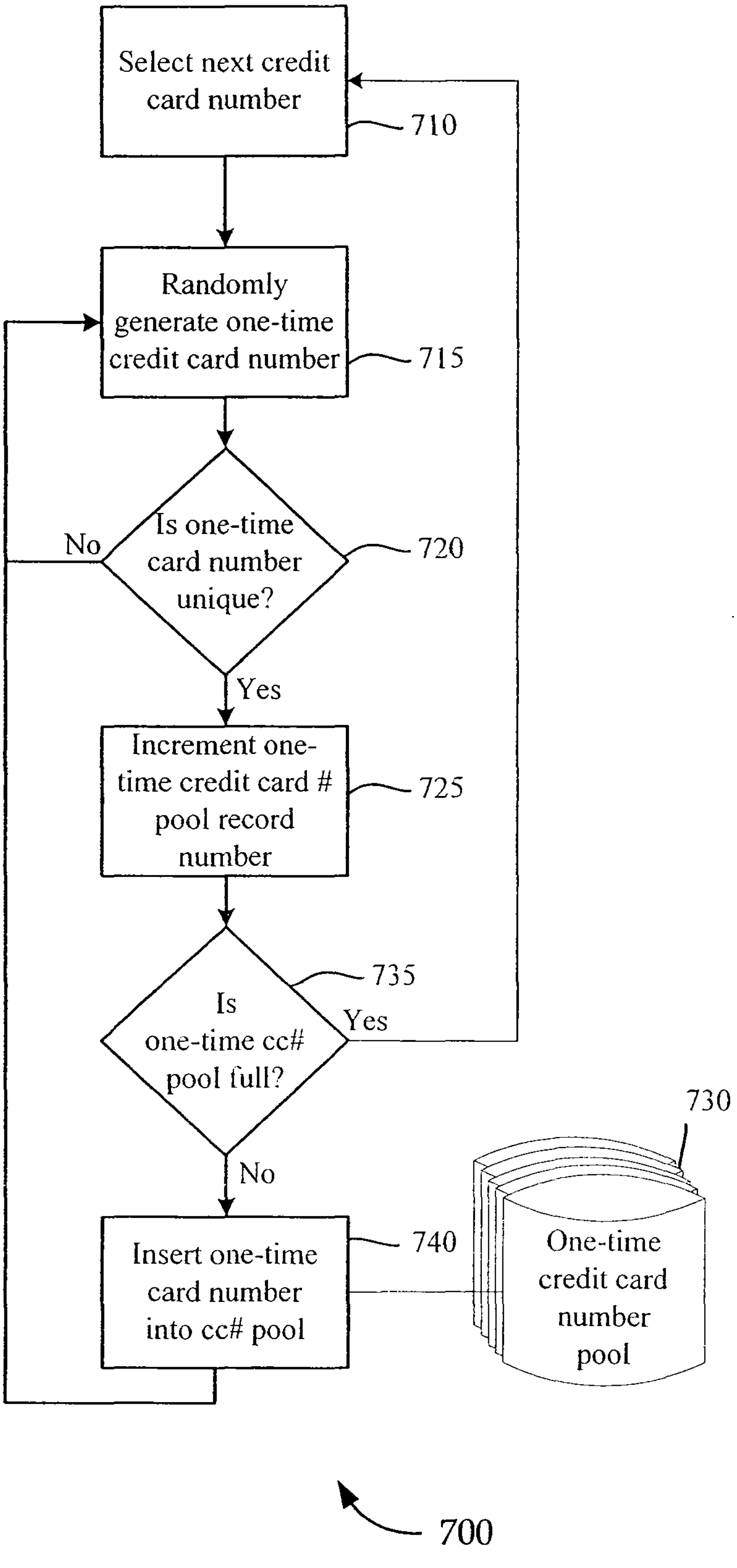
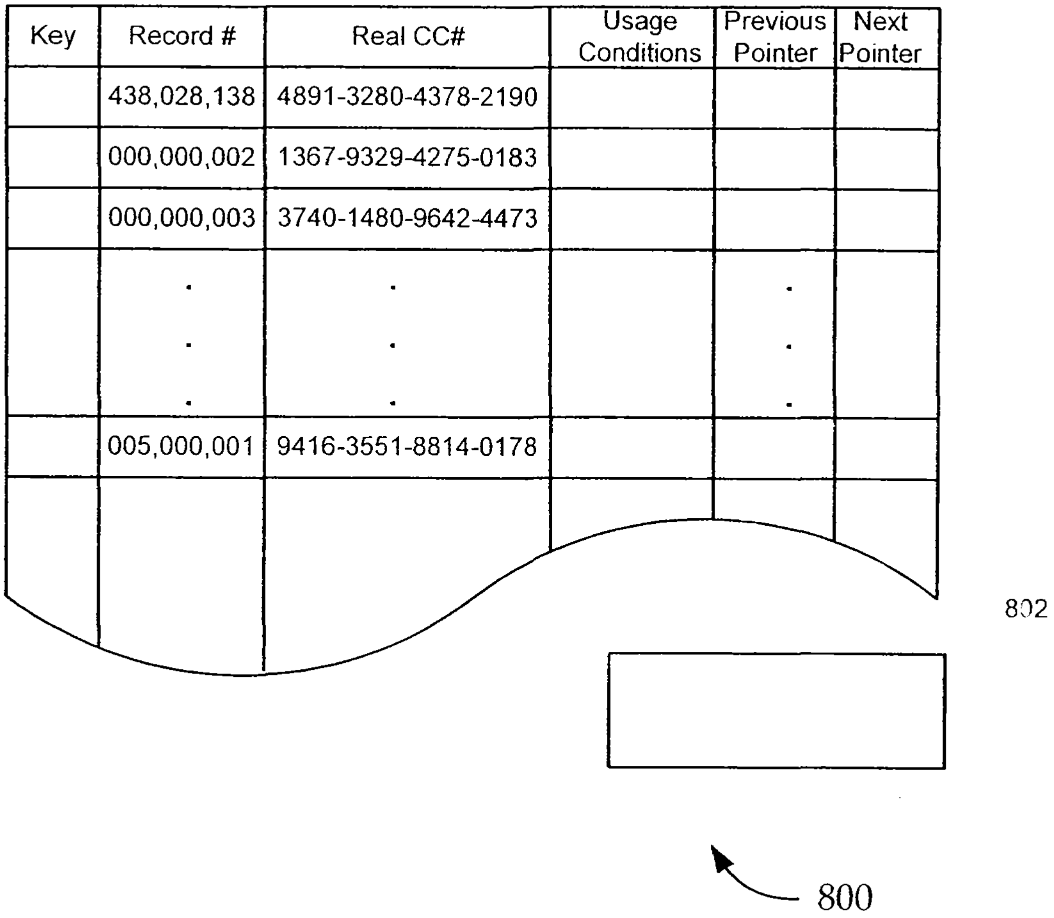

Select next credit card number
710
Randomly generate one-time credit card number
715
Is one-time card number unique?
720
No
Yes
Increment one-time credit card # pool record number
725
Is one-time cc# pool full?
735
Yes
No
730
Insert one-time card number into cc# pool
740
One-time credit card number pool
700

FIG. 7



Key	Record #	Real CC#	Usage Conditions	Previous Pointer	Next Pointer
	438,028,138	4891-3280-4378-2190			
	000,000,002	1367-9329-4275-0183			
	000,000,003	3740-1480-9642-4473			
	. . .	. . .		. . .	
	005,000,001	9416-3551-8814-0178			

FIG. 8

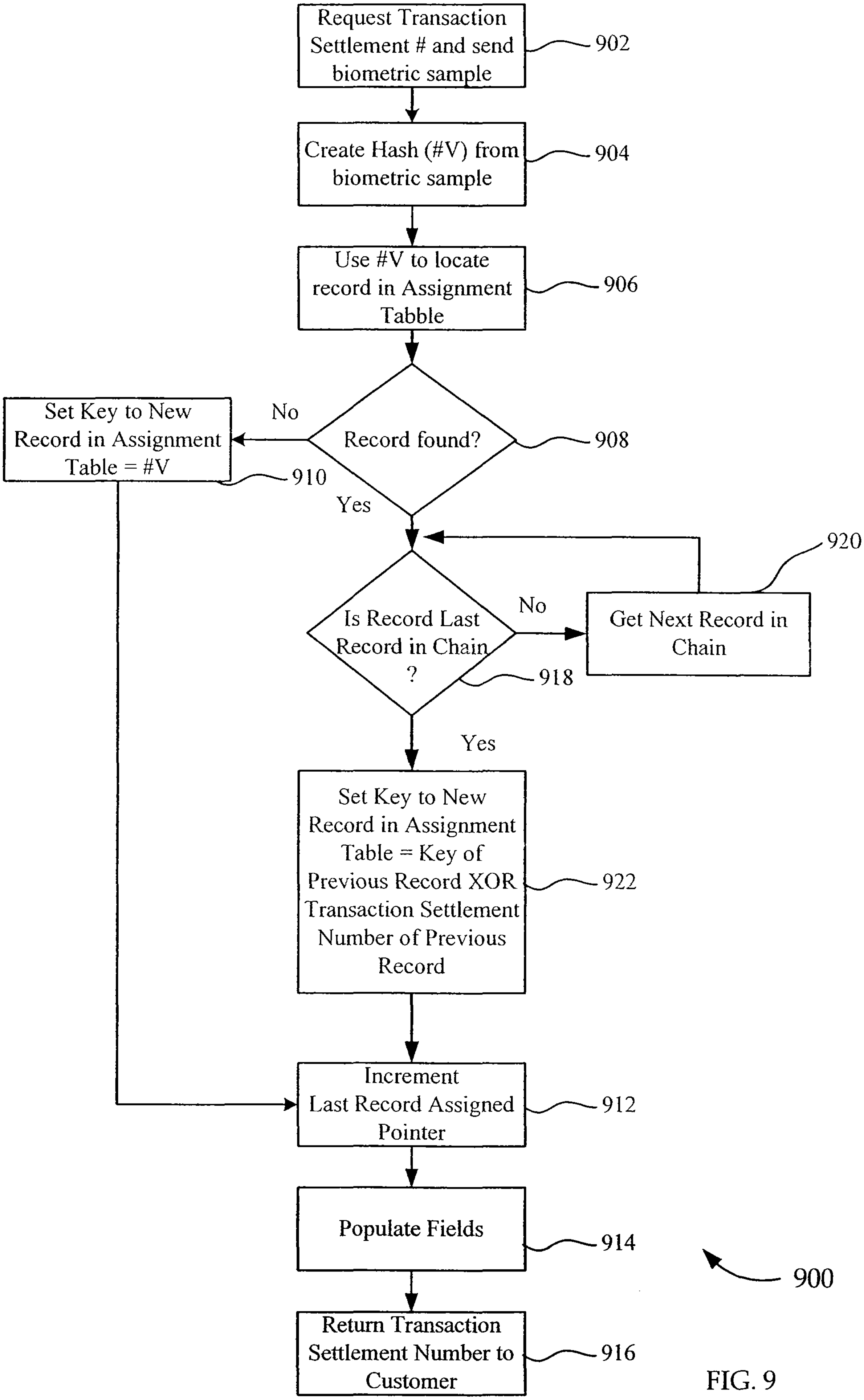

Request Transaction Settlement # and send biometric sample
902
Create Hash (#V) from biometric sample
904
Use #V to locate record in Assignment Tabble
906
Record found?
908
No
Set Key to New Record in Assignment Table = #V
910
Yes
Is Record Last Record in Chain ?
918
No
Get Next Record in Chain
920
Yes
Set Key to New Record in Assignment Table = Key of Previous Record XOR Transaction Settlement Number of Previous Record
922
Increment Last Record Assigned Pointer
912
Populate Fields
914
Return Transaction Settlement Number to Customer
916
900

FIG. 9

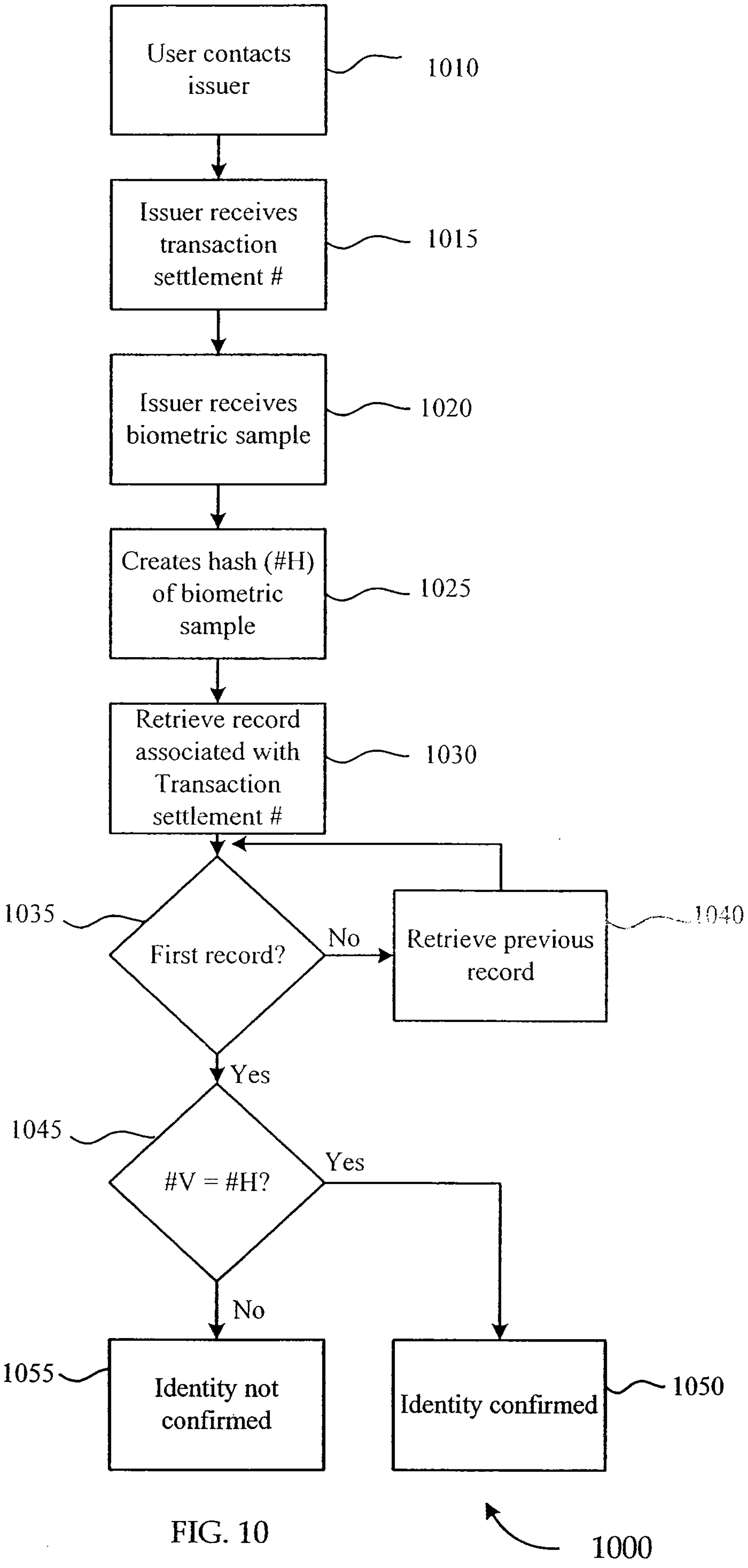

User contacts issuer
1010
Issuer receives transaction settlement #
1015
Issuer receives biometric sample
1020
Creates hash (#H) of biometric sample
1025
Retrieve record associated with Transaction settlement #
1030
1035
First record?
No
Retrieve previous record
1040
Yes
1045
#V = #H?
Yes
No
1055
Identity not confirmed
Identity confirmed
1050
1000

FIG. 10

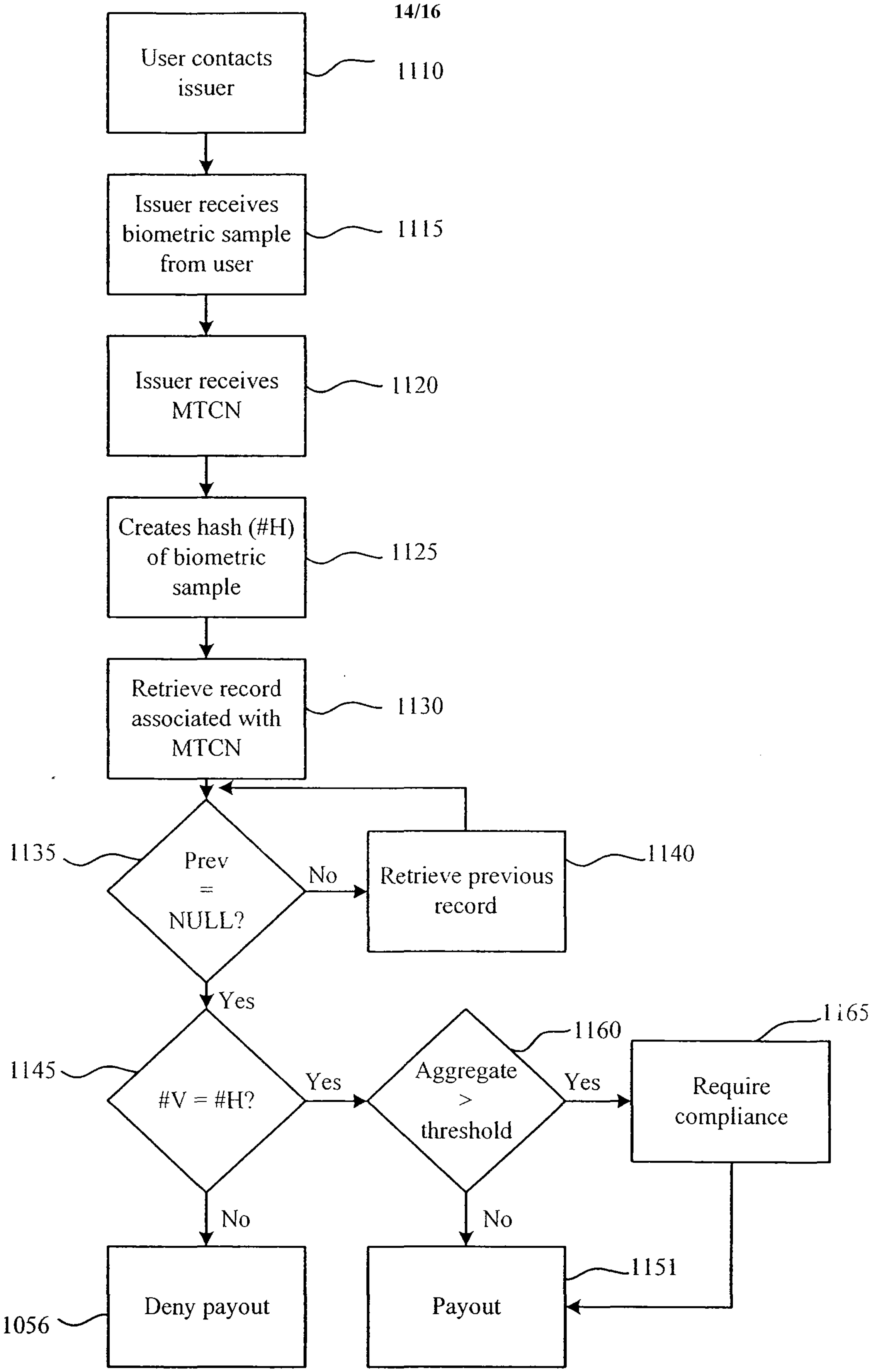

User contacts issuer
1110
Issuer receives biometric sample from user
1115
Issuer receives MTCN
1120
Creates hash (#H) of biometric sample
1125
Retrieve record associated with MTCN
1130
1135
Prev = NULL?
No
Retrieve previous record
1140
Yes
1145
#V = #H?
Yes
Aggregate > threshold
1160
Yes
Require compliance
1165
No
No
Deny payout
1056
Payout
1151

FIG. 11

1100

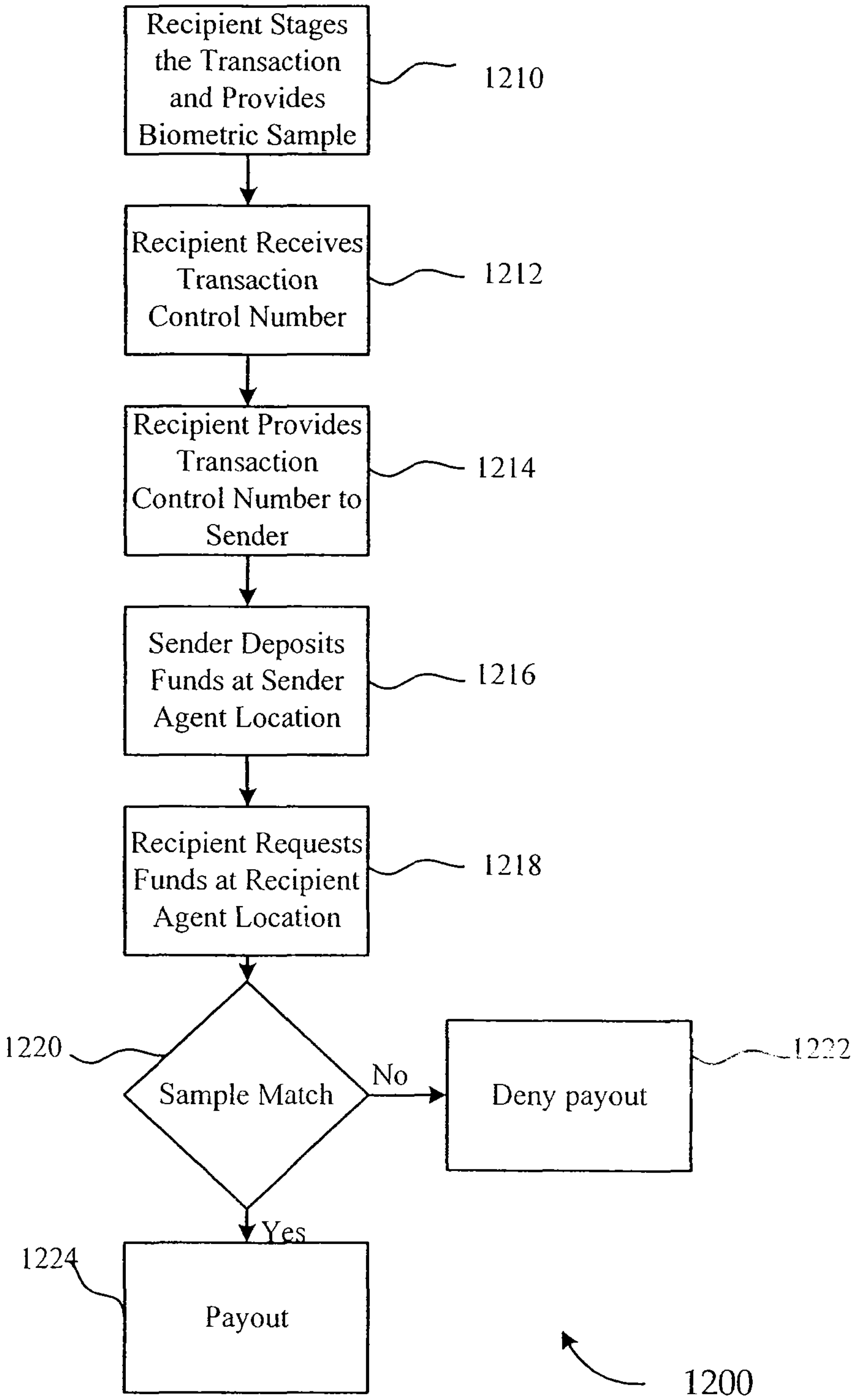

Recipient Stages the Transaction and Provides Biometric Sample
1210
Recipient Receives Transaction Control Number
1212
Recipient Provides Transaction Control Number to Sender
1214
Sender Deposits Funds at Sender Agent Location
1216
Recipient Requests Funds at Recipient Agent Location
1218
1220
Sample Match
No
Deny payout
1222
Yes
1224
Payout
1200

FIG. 12

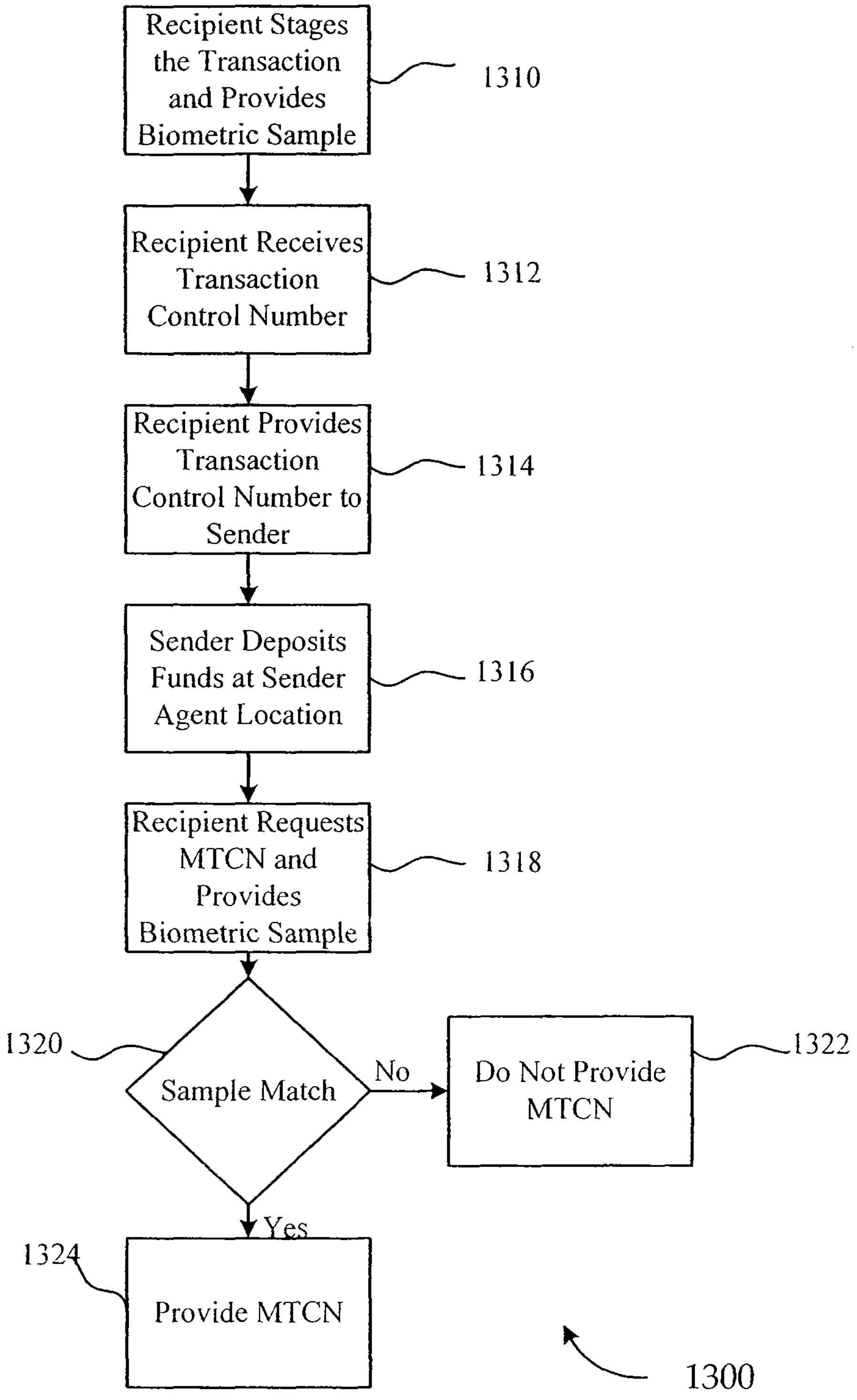

Recipient Stages the Transaction and Provides Biometric Sample
1310
Recipient Receives Transaction Control Number
1312
Recipient Provides Transaction Control Number to Sender
1314
Sender Deposits Funds at Sender Agent Location
1316
Recipient Requests MTCN and Provides Biometric Sample
1318
1320
Sample Match
No
Do Not Provide MTCN
1322
Yes
1324
Provide MTCN
1300

FIG. 13