Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 2996145 A1 2017/02/23

(21) 2 996 145

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2016/08/17
(87) Date publication PCT/PCT Publication Date: 2017/02/23
(85) Entrée phase nationale/National Entry: 2018/02/20
(86) N° demande PCT/PCT Application No.: US 2016/047329
(87) N° publication PCT/PCT Publication No.: 2017/031198
(30) Priorités/Priorities: 2015/08/17 (US62/282,991); 2016/08/17 (US15/239,122)

(51) Cl.Int./Int.Cl. *G06Q 20/08* (2012.01), *G06Q 20/20* (2012.01), *G06Q 20/22* (2012.01), *G06Q 20/40* (2012.01), *G06Q 20/42* (2012.01), *G06Q 40/00* (2012.01)

(71) Demandeurs/Applicants:
TRANSWORLD HOLDINGS PCC LIMITED (S1 TECHNOLOGY CELL), GB;
ABEL, MILLER THOMAS, US;
MAGES, KENNETH, US

(72) Inventeurs/Inventors:
ABEL, MILLER THOMAS, US;
MAGES, KENNETH, US

(74) Agent: BORDEN LADNER GERVAIS LLP

(54) Titre : DISPOSITIFS DE PAIEMENT DOTES DE PLUSIEURS MODES DE CONDUITE DE TRANSACTIONS FINANCIERES

(54) Title: PAYMENT DEVICES HAVING MULTIPLE MODES OF CONDUCTING FINANCIAL TRANSACTIONS

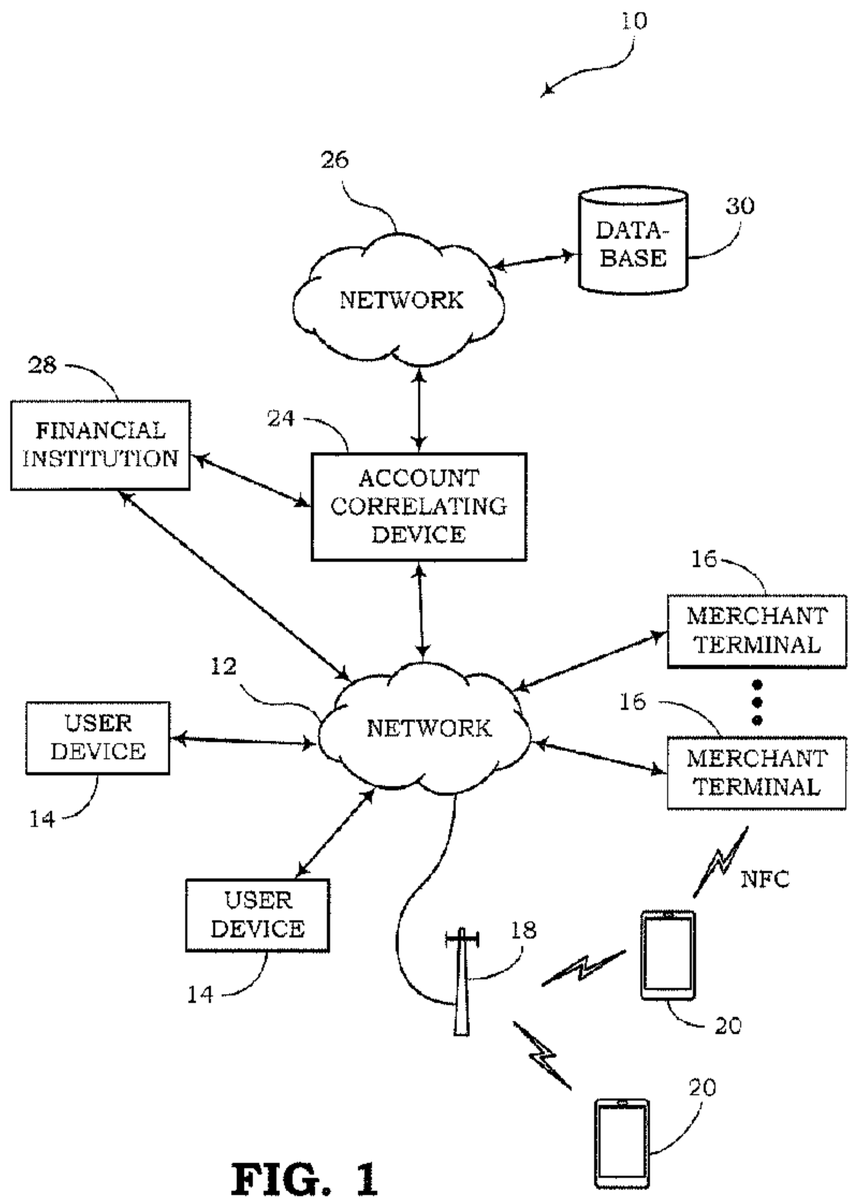


FIG. 1

(57) Abrégé/Abstract:
Payment cards and also the systems and methods for securely managing financial transactions using the payment cards are provided. In one implementation, a payment card includes a first component incorporated into a plastic substrate, wherein the first component is configured to provide details of a first substitute account associated with a cardholder's valid credentials. The payment card also includes at least one additional component incorporated into the plastic substrate. Each of the additional components is configured to provide details of at least one additional substitute account associated with the cardholder's valid credentials. Each substitute account includes details that are distinct from the details of each of the other substitute accounts. Also, at least one of the substitute accounts is provided to a merchant for conducting a financial transaction with the merchant.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 February 2017 (23.02.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/031198 A1

(51) International Patent Classification:
G06Q 20/08 (2012.01) *G06Q 20/22* (2012.01)
G06Q 20/20 (2012.01) *G06Q 20/40* (2012.01)
G06Q 40/00 (2012.01) *G06Q 20/42* (2012.01)

(21) International Application Number:
PCT/US2016/047329

(22) International Filing Date:
17 August 2016 (17.08.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/282,991 17 August 2015 (17.08.2015) US
15/239,122 17 August 2016 (17.08.2016) US

(71) Applicant: **TRANSWORLD HOLDINGS PCC LIMITED (S1 TECHNOLOGY CELL)** [AU/AU]; 69 Athol Street, Douglas, Isle of Man 1M1 1JE (GB).

(72) Inventors; and
(71) Applicants : **ABEL, Miller, Thomas** [US/US]; 8215 SE 41st Street, Mercer Island, WA 98040 (US). **MAGES, Kenneth** [US/US]; 730 South Clark Street, Apt 2709, Chicago, IL 60605 (US).

(74) Agent: **HESPOS, Gerald, E.**; Hespos & Porco LLP, 110 West 40th Street-suite 2501, New York, NY 10016 (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, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

[Continued on next page]

(54) Title: PAYMENT DEVICES HAVING MULTIPLE MODES OF CONDUCTING FINANCIAL TRANSACTIONS

(57) Abstract: Payment cards and also the systems and methods for securely managing financial transactions using the payment cards are provided. In one implementation, a payment card includes a first component incorporated into a plastic substrate, wherein the first component is configured to provide details of a first substitute account associated with a cardholder's valid credentials. The payment card also includes at least one additional component incorporated into the plastic substrate. Each of the additional components is configured to provide details of at least one additional substitute account associated with the cardholder's valid credentials. Each substitute account includes details that are distinct from the details of each of the other substitute accounts. Also, at least one of the substitute accounts is provided to a merchant for conducting a financial transaction with the merchant.

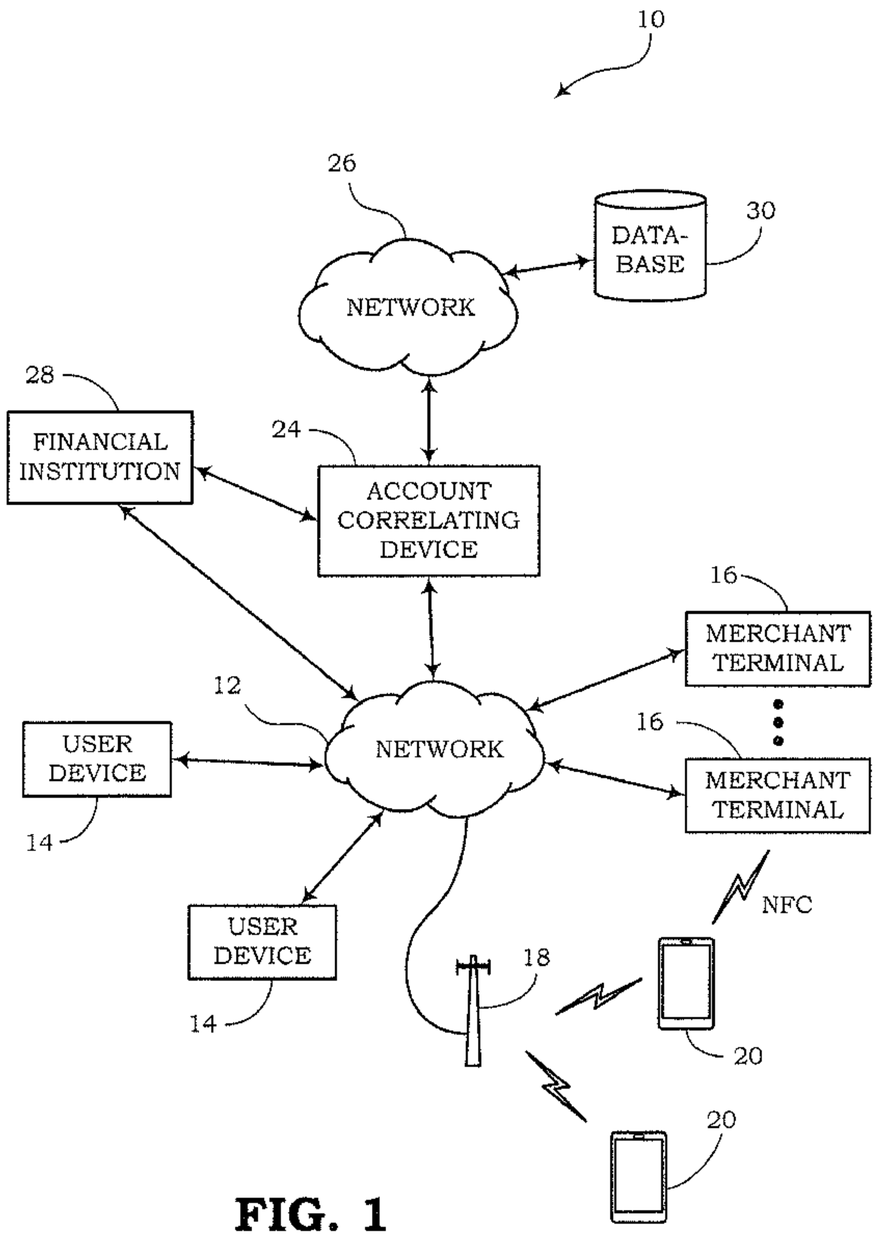


FIG. 1

WO 2017/031198 A1

WO 2017/031198 A1

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

PAYMENT DEVICES HAVING MULTIPLE MODES OF CONDUCTING FINANCIAL TRANSACTIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Application No. 62/282,991, filed August 17, 2015, the entire disclosure of which is incorporated by reference herein.

FIELD OF THE INVENTION

The present disclosure generally relates to financial services, and more particularly relates to payment devices and systems for settling financial transactions.

BACKGROUND

Plastic payment cards, such as credit cards, were introduced in the United States in the late 1940s as a way for a bank's most trusted customers to pay for meals and travel without carrying large amounts of cash. Since then, billions of payment cards have been issued by tens of thousands of banks.

However, several types of illegal activities pose a threat to the security of conventional payment card systems. Identity theft, counterfeit activities, fraud, unauthorized account access, and other illegal activity compromise the integrity of the system. Conventional payment cards, and the networks used to authorize and settle card

transactions, are vulnerable to widespread exploits by identity thieves and other criminals. One major form of payment account fraud is the unauthorized use of payment account details when conducting electronic commerce. Another major form of payment account fraud is the production and use of counterfeit cards at a merchant's point-of-sale (POS) device. These forms of fraud are inherent by the way that the payment cards themselves are produced. Specifically, credit card numbers and other payment account details, which are printed or embossed on a conventional plastic payment card, can easily be copied or stolen. Also, a payment card's magnetic stripe can be counterfeited. In fact, losses to banks, merchants, and consumers caused by payment card fraud is on a rapid rise. Payment card fraud costs the industry close to $20 billion annually.

To combat counterfeit and misappropriation fraud, which is the source of the majority of the financial risk to banks and payment brands, the major card issuing networks have adopted new technologies to ensure only legitimate cards are used at physical points of sale. These technologies, developed by the payment card industry and a consortium of card issuing networks (EMVCo), adds to the plastic card a tamper-resistant computer microchip with confidential storage and computing capability. EMVCo is a payment industry consortium named for EuroPay, MasterCard, and Visa, which are the

original founders of the organization, but now also includes American Express, Discover, JCB, and Union Pay as equity partners.

This microchip confidentially stores the information and programs needed to generate a unique cryptographic signature at the time a transaction is made at a merchant POS. Computing processes are performed securely and confidentially inside the embedded microchip at the time of each transaction and the result is passed along with the payment account data through the existing payment network to the card issuing bank where it is verified using the same information stored in the card. The stored information is never disclosed by the issuer and cannot be extracted from the microchip by any practical means. The microchip-embedded card thus provides a one-time code for each card transaction performed at a physical point of sale. If all merchants honor this new mechanism, the risk that a counterfeit card could be produced by misappropriation of account data is largely eliminated.

Another way that card issuers attempt to combat fraud is by providing cards having near field communication (NFC) components. Cards that are enabled with NFC components allow a user to tap or pass the card near an NFC reader to within about 10 cm.

However, the microchip-embedded cards, also known as EMV cards or smart cards, and NFC-enabled cards must also work in environments that have not yet embraced the new standards. Many

merchants have yet to adopt the EMV-enabled terminals that can activate the microchip cards and read the cryptographic code or the NFC readers that can read the wireless communication signals. To ensure payment cards are universally accepted, the card issuers include a conventional magnetic stripe on the back of the card.

Additionally, to enable electronic and telephone commerce, issuers include the payment account number either printed on the card and/or embossed into the plastic. Therefore, not only can the microchip and NFC components be used in making financial transactions, but also the magnetic stripe can be used in a financial transaction using a POS swiping process or the account numbers can be used in telephone or Internet transaction. The method by which the card communicates the account information to the merchant terminal is known as the mode. In other words, the microchip card can be utilized in at least four different modes of financial transactions, including, for example, magnetic stripe swiping mode, various modes using the EMV chip, NFC mode, and manual card number entry. The microchip may also enable additional modes, which is one reason why there may be more than four different modes of financial transactions.

A thief who encounters one of these new EMV or NFC payment cards and has physical control of the card even for a few brief moments can easily steal the sensitive payment account data without considering the embedded chip or NFC components. This can be done by reading

the payment data from the magnetic stripe, in order to prepare a counterfeit card. The thief can also steal the data by taking a picture of the card and capturing the card numbers for fraudulent electronic commerce. It should be noted that both the magnetic stripe data and the printed data are not protected by digital security means like cryptography. The compromised data may then be used at less secure retail merchants, who have not yet adopted the EMV system, or the thief may go online to perform electronic commerce transactions.

Therefore, a need exists for more secure payment cards. To combat the above-mentioned problems, and to improve customer satisfaction and control of the payment card experience, the present invention introduces several innovative elements for payment cards and financial networks and the authorization and settlement of financial transactions.

SUMMARY

The present disclosure describes payment cards and systems and methods for securely managing financial transactions using the payment cards. A payment card may take such forms as, for example, a plastic payment card, a virtual card, a wearable commerce device, one or more components embedded in a mobile device, an application running on mobile devices or computers, and other payment credential forms. According to one implementation, a payment card comprises a

first component incorporated into a plastic substrate, the first component configured to provide details of a first substitute account associated with a cardholder's primary financial account.

The payment card may also include additional components incorporated into the plastic substrate. The additional components are configured to provide details of additional substitute accounts associated with the cardholder's valid credentials. The first substitute account includes details that are distinct from the details of the second substitute account and are distinct from all additional substitute accounts. At least one of the first, second or additional substitute accounts is provided to a merchant for conducting a financial transaction with the merchant.

According to another implementation, an account correlating device comprises at least one network interface configured to communicate with a plurality of merchant terminals via a first network and to communication with a financial institution via a secure network. The account correlating device also includes a transaction authentication module configured to authenticate a first financial transaction for a first merchant terminal of the plurality of merchant terminals based on a first set of details obtained by the first merchant terminal of a first substitute account associated with a payment card owned by a cardholder. The transaction authentication module is further configured to authenticate additional financial transactions for

additional merchant terminals of the plurality of merchant terminals based on additional, different set of details obtained by the additional merchant terminal of the additional substitute account associated with the payment card owned by the cardholder.

According to yet another implementation, a system for providing security for a payment card is provided. The system includes a first merchant terminal and an additional merchant terminal each connected to a network. The first merchant terminal is configured to obtain details of a first substitute account from a first set of information associated with a payment card owned by a cardholder. The additional merchant terminal is configured to obtain details of an additional substitute account from an additional set of information associated with the payment card. The system further includes an account correlating device connected to the network. The account correlating device is configured to receive the details of the first and additional substitute accounts from the first and additional merchant terminals, respectively. The account correlating device is further configured to associate the first and additional substitute accounts to a valid credential belonging to the cardholder. Furthermore, the account correlating device manages financial transactions between a financial institution, from which the cardholder retains the valid credential, and the first and additional merchant terminals. The first set of information is different from the additional sets of information.

Various implementations described in the present disclosure may include additional systems, methods, features, and advantages, which may not necessarily be expressly disclosed herein but will be apparent to one of ordinary skill in the art upon examination of the following detailed description and accompanying drawings. It is intended that all such systems, methods, features, and advantages be included within the present disclosure and protected by the accompanying claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and components of the following figures are illustrated to emphasize the general principles of the present disclosure and are not necessarily drawn to scale. Corresponding features and components throughout the figures may be designated by matching reference characters for the sake of consistency and clarity.

FIG. 1 is a block diagram illustrating a payment card system according to various implementations of the present disclosure.

FIGS. 2A and 2B are diagrams illustrating a front view and back view, respectively, of a first payment card according to various implementations of the present disclosure.

FIGS. 3A and 3B are diagrams illustrating a front view and back view, respectively, of a second payment card according to various implementations of the present disclosure.

FIG. 4 is a block diagram illustrating the account correlating device shown in FIG. 1 according to various implementations of the present disclosure.

FIG. 5 is a block diagram illustrating the user account module shown in FIG. 4 according to various implementations of the present disclosure.

DETAILED DESCRIPTION

The present invention is directed to payment devices, hereafter referred to as a payment card, such as, for example, plastic payment cards, virtual cards, wearable commerce devices, components embedded in mobile devices, applications running on mobile devices or computers, and other payment credentials. The present invention is also directed to systems and methods for conducting financial transactions using the payment devices. The present invention may include a commercially viable computing service, mobile application, and web site and may be implemented in conjunction with a financial institution using payment cards or other payment devices as described herein. The present invention introduces several novel elements that can be employed by existing card and valid credential issuers to combat various forms of fraud. The term “valid credential” is used in this document to represent a valid funding instrument, which may be, but is not limited to, a credit card, charge card, direct deposit account,

savings account, checking account, loyalty card, gift card, or other cards or devices.

The present invention includes multimodal payment devices, which can be used in various modes for different types of financial transactions. For example, payments cards described herein may include multiple modes for completing a transaction. Some modes may include those involving a microchip embedded in the card, those involving near field communication (NFC) components, those involving the magnetic stripe, those involving entering the card number and card verification value (CVV) in an online transaction, and/or other modes. The present invention includes novel fraud-reducing features, a mobile phone application, and a companion web site to control the novel fraud-reducing features. Also, a computing service can be used in the authorization and settlement networks serving both online and retail merchants.

Current issuing practice for payment cards is to include the cardholder's single primary account number (PAN) details, which correspond directly to the cardholder's actual valid credential, across all the various modes of the payment card (i.e., including magnetic stripe, EMV chip, NFC, etc.). However, by using a substitute account number, or token, in place of a primary account number (PAN), as is described in the present disclosure, an account correlating device can be interposed between the merchant and the issuing bank to

supplement the security of transactions, or called by the issuing bank as part of processing the payment. The payment device systems described herein substitute cardholder PAN details securely, in the network, prior to transaction authorization and settlement. In this way, disclosure of the cardholder's PAN details to the merchant is prevented.

The present invention uses several distinct, anonymous, and unpredictable sets of substitute account details for each payment device. In the example of physical payment cards, one set of substitute account details may be associated with one or more modes of the EMV chip, another set may be associated with another mode of the EMV chip, another set of substitute account details may be associated with the NFC components, another set for the magnetic stripe, and another for use during electronic commerce, and yet another for manual entry. Using several distinct sets of substitute account details can prevent cross-mode payment fraud.

Current practice is to include the same PAN in the EMV chip that is included in the magnetic stripe and that is printed on the card. Financial transactions can then be accepted when any of the multiple modes is presented, which makes cross-modal fraud possible. For example, a thief might intercept the EMV card details and produce a counterfeit magnetic stripe card. Also, a thief might take both EMV and magnetic stripe account details, using card data readers, and perform

unauthorized electronic commerce transactions. However, the present invention is not limited by the same PAN being used for all modes. Instead, the present invention uses multiple distinct sets of substitute account details corresponding to multiple valid credentials, where each substitute account can be associated with a distinct mode. In this way, cross-modal payment fraud can be prevented.

It should be noted that the payment devices described in the present disclosure may be implemented as credit cards, debit cards, virtual cards, wearable devices, Internet of things (IoT) devices, components and/or application embedded in mobile devices, and/or other financial credentials. In other embodiments, the payment devices described in the present disclosure may apply to non-payment devices that are used in other environments besides commerce. For example, non-payment devices (e.g., loyalty cards, mobile devices, and other non-financial credentials) may apply to other functions for standing in as a proxy credential to electronically authenticate identification, such as for health insurance purposes, driver's license purposes, etc., to gain access to a secure location, to provide a photographic identification of the cardholder, and for other purposes. Further, the valid credentials that may be associated with substitute account details may be payment and/or non-payment credentials, such as loyalty credentials, health insurance credentials, and other financial or non-financial credentials.

FIG. 1 is a block diagram illustrating an embodiment of a payment card system 10 in which a financial institution 28 issues a payment card, such as a credit card or debit card, to a customer. In other embodiments, the customer may use another type of proxy credential other than a payment card, such as a mobile device. According to the embodiment of FIG. 1, the payment card system 10 includes a public network 12, one or more user devices 14, one or more merchant terminals 16, one or more wireless communication antennas 18, one or more mobile devices 20, and an account correlating device 24.

The term “merchant terminal” is used to describe a physical terminal, website, or other devices for providing functionality by a merchant at which a payment is originated. Merchant terminals can be embedded in POS equipment and can be “virtual” as in ecommerce website processing. Also, merchant terminals can be background devices where no card, customer, merchant, or goods are involved, such as when recurring payments are initiated for services. The “merchant terminal” may represent POS devices, merchant online systems, and other mechanisms owned/controlled by the merchant to conduct various modes of purchase. The merchant terminals may include any merchant systems used in different payment modes using one or more types of technologies (e.g., EMV chip, magnetic stripe, NFC, e-commerce, etc.).

The network 12 may include a wide area network, the Internet, private networks, and/or other publicly accessible networks. Also, the network 12 may include local area networks associated with various merchants. The network 12 may also be in communication with one or more cellular networks connected to the antennas 18.

The user devices 14, merchant terminals 16, and antennas 18 may be connected by one or more wired or wireless connections to the network 12 to enable electronic communication among the various components. The wireless communication antennas 18 may include one or more cellular towers, orbiting satellites, or other wireless communication hubs for communication with the mobile devices 20.

The account correlating device 24 could be a server, a web server, software running on a server, a hardware appliance, or any suitable intermediary computing device or means for providing various transaction services. The account correlating device 24 is also connected to a secure network 26, which is also connected via wired or wireless connections to one or more financial institutions 28 and one or more databases 30. The secure network 26 may be a private network, local area network, a virtual private network (VPN), or a public network with a high level of encryption. The account correlating device 24 may be configured to store information in the database 30 that directs one or several substitute accounts to an authentic account owned by a cardholder or customer of the financial institution 28.

During a purchasing operation, the customer to whom a payment card has been issued may use the payment card as payment for merchandise or services. The payment card can be presented to a merchant at one of the merchant terminals 16. It should be noted that several merchant terminals 16 may be associated with the same merchant for obtaining account information through various modes. In fact, multiple merchant terminals 16 may be associated with a single device used by a merchant for obtaining information at a single POS device. Accordingly, the POS device may obtain information from the payment card by a first mode utilizing a microchip embedded in the card or by additional modes, which may involve the use of the NFC components or magnetic stripe on the card. In other transactions, such as online or telephone transactions, the card number printed and/or embossed on the card may be entered electronically or by an order-taking representative of the merchant.

According to alternative embodiments, the payment card system 10 may instead be configured as a system for performing non-payment actions. Instead of conducting various functions related to financial accounts as disclosed herein, the non-payment system may process other types of credentials for entities other than financial institutions.

The account correlating device 24 uses the database 30 to associate arbitrary substitute account data values to details of a cardholder's valid credential. The arbitrary substitute account data

values and valid credential details may be provided by the cardholding customer at the time of enrolling in a service provided by the account correlating device 24. In one embodiment, the cardholding customer may change the valid credential details that are associated to the substitute account at any time using a mobile application on one of the mobile devices 20 or via a web service provided by the account correlating device 24 using a user device 14, which may be a conventional computer or web browser. The account correlating device 24 enables multiple valid credentials to be associated with multiple substitute accounts. The valid credentials may be financial or non-financial credentials. In one embodiment, the account correlating device 24 enables valid credentials from the issuing cardholder financial institution 28 to be associated with the multiple substitute accounts. In one embodiment, the account correlating device 24 enables valid credentials from both issuing cardholder financial institution 28 as well as other financials or non-financial institutions to be associated with the multiple substitute accounts.

The account correlating device 24 is deployed into the payment card system 10 such that all transactions presented by a merchant via one of the merchant terminals 16 for authorization against one of the multiple substitute accounts represented on each card are received by the account correlating device 24. The account correlating device 24 associates the multiple substitute accounts with one or more of the

customer's valid credentials using a customizable rules engine, which is sensitive to one or more facts including, but not limited to, the current transaction data. The current transaction data may include, for example, but is not limited to, merchant category code, merchant ID, amount of transaction, substitute account number, service code, card security code, etc.

The account correlating device 24 may also have access by way of the database 30 to data including, but not limited to, prior transactions presented for the specific substitute account, prior transactions presented for another substitute account associated with the same cardholding customer, prior transactions for other customers of the same merchant or merchant location, the geographic location of the cardholding customer's primary mobile phone at the time the transaction is presented. The geographic location may be determined, for example, by the Global Positioning System (GPS), proximity to radio signals such as Wi-Fi™, Bluetooth™, Bluetooth Low Energy beacons, Zigbee™, Z-wave™, or any combination of these and other location-sensitive factors. The substitute accounts, which can be associated with a valid credential, have themselves, unless otherwise associated, no balance or established credit and cannot be used to settle any transactions.

The payment card system 10 may be used to provide security for the use of a payment card. The payment card system 10 may include

a first merchant terminal 16 connected to a public network 12, wherein the first merchant terminal 16 is configured to obtain details of a first substitute account from a first set of information associated with a payment card owned by a cardholder. The payment card system 10 may include a second merchant terminal 16 connected to the public network 12, wherein the second merchant terminal 16 is configured to obtain details of a second substitute account from a second set of information associated with the payment card. In this embodiment, the payment card system 10 also includes an account correlating device 24 connected to the public network 12. The account correlating device 24 is configured to receive the details of the first and second substitute accounts from the first and second merchant terminals 16, respectively. The account correlating device 24 is further configured to associate the first and second substitute accounts to valid credentials belonging to the cardholder. The account correlating device 24 also manages financial transactions between a financial institution 28, from which the cardholder retains the valid credential, and the first and second merchant terminals 16. Also, it should be noted that the first set of information is preferably different from the second set of information.

The payment card system 10 may also include a third merchant terminal 16 connected to the public network 12, wherein the third merchant terminal 16 may be configured to obtain details of a third substitute account from a third and preferably different set of

information associated with the payment card. In some embodiments, the first set of information is obtained from a microchip on the payment card, the second set of information is obtained from NFC components embedded in the payment card, the third set of information is obtained from a magnetic stripe on the payments card, and the fourth set of information is obtained from card numbers printed and/or embossed on the payment card. Additional sets of information obtained from various other modes now known or later developed may also be obtained. The first, second, third, fourth and other sets of information may be generated by the financial institution. Some of these sets of information may be manually entered.

An alternative embodiment includes the payment card system 10 in which the payment card is devoid of a printed and/or embossed account number. Also, the payment card may be devoid of a magnetic stripe, or one of the other modes. In this case, the cardholder may use the payment card at a merchant terminal using only the microchip and/or NFC components, or the modes remaining on the card.

A different set of account details may be communicated to the cardholder for conducting an online or telephone transaction. The different set of details may be mailed, emailed, or texted to the cardholder via a computer (e.g., user device 14) and/or via a mobile device 20.

In some embodiments, the mobile device 20 associated with the cardholder may be incorporated in the system 10. One of the merchant terminals 16 may be an online merchant device configured to conduct an online transaction, and the mobile device 20 may be configured to store, retrieve one generated from the account correlating device 24 or calculate a dynamic card verification value (d-CVV), which is transmitted to, or manually entered into, the online merchant device. In some cases, one or more of the merchant terminals 16 may be embedded within point-of-sale (POS) devices.

The user device 14 associated with the cardholder is configured to enable the cardholder to manage the substitute accounts and the valid credentials via the account correlating device 24. The account correlating device 24 is configured to enable the cardholder to enter enrollment information, monitor the activities of the substitute accounts, enable and disable one or more modes of conducting transactions with the payment card, report if the payment card has been lost or stolen, and provision information related to the various valid credentials. For example, the account correlating device 24 may provide a website including one or more webpages enabling the cardholder to navigate the website potentially using the user device 14.

FIGS. 2A and 2B illustrate a first type of payment card 36 according to various embodiments of the present invention. FIG. 2A shows a front side 38 of the payment card 36 and FIG. 2B shows a

back side 40 of the payment card 36. The payment card 36 may include a name 42 of the financial institution 28, a microchip 44, a card number 46, a customer name 48, and an expiration date 50 on the front side 38 of the payment card 36. In some embodiments, the card number 46 may be embossed in the payment card 36. In addition, the back side 40 of the payment card 36 may include a magnetic stripe 52, a signature box 54, and a card verification value (CVV) 56. The payment card 36 may further include NFC components, which may be embedded under the surface of the payment card 36, for enabling touchless transactions.

In one embodiment, the payment card 36 may be a plastic EMV microchip card that is issued by a card-issuing bank according to the issuing rules for one of several global branded payment card networks. The payment card 36 includes provisioning and personalization such that it may be used at any EMV-enabled merchant POS.

However, the account details included in the microchip 44 are not those of the primary card holder, but rather are arbitrary values generated by the card issuer. The account details may be referred to herein as “substitute account details.” The substitute account details are used as a stand-in for a valid credential but do not identify any particular customer. They refer instead to a substitute account generated by the card issuing bank but not associated with any particular valid credential.

In the embodiment of FIG. 2, the microchip 44 and magnetic stripe 52 contain distinct payment account numbers, expiration dates, and other token account details for two different substitute accounts. Simply, the microchip 44 and magnetic stripe 52 appear to represent completely distinct payment accounts. A transaction performed with the microchip 44 at an EMV-enabled merchant will contain different account details than a transaction performed at a merchant using the magnetic stripe 52 on the same card 36. Also, an NFC transaction may utilize payment account details that differ from the both the EMV-enabled mode and the magnetic stripe mode.

In one embodiment, the financial institution 28 provides the customer with substitute account details for use in electronic commerce and telephone commerce transactions such that the details are distinct from either the substitute account details for the microchip 44 or the magnetic stripe 52. It will be appreciated that facsimile, electronic mail, and other forms of electronic and telephone communication may also be used. It will also be appreciated that the substitute account details may be recorded on a mail order form for transactions conducted through the mail. The electronic commerce substitute account details may not be printed or embossed on the payment card 36 but provided separately to the customer, or may be printed or embossed on the payment card, depending upon the embodiment.

FIGS. 3A and 3B illustrate a second type of payment card 60 according to various embodiments of the present invention. FIG. 3A shows a front side 62 of the payment card 60 and FIG. 3B shows a back side 64 of the payment card 60. The payment card 60 may include a name 66 of the financial institution and a microchip 68 on the front side 62 of the payment card 60. It should be noted that the payment card 60 is devoid of a card number and the customer's name that may normally appear on a conventional payment card. The back side 64 of the payment card 60 may be blank or may simply include a name and address of the financial institution. The back side 64 is therefore devoid of a conventional magnetic stripe and CVV number. The payment card 60 has no pre-printed account number, embossed account data, expiration data, cardholder name, or other account data. By making the card anonymous and without including a human-readable account number, the trivial theft of account data from the face and back of the card can be prevented.

Currently, Visa™ and MasterCard™ include rules for their credit and debit cards that require the cardholder's name and account number to be displayed on the card. Therefore, the embodiment of FIG. 3 does not follow these present day rules. Nevertheless, the payment card 60 as described in the present disclosure can be carried in public without the risk of being lost or stolen, since the cardholder name and account number cannot be retrieved visually. For online,

mail order, telephone, and similar transactions, a separate card or electronic file can be safely stored at the cardholder's home.

In some embodiments, the payment card 36, 60 may be formed from a plastic substrate. A first component (e.g., the microchip 44) may be incorporated into the plastic substrate on the cards shown in FIGS. 2 and 3. The first component may be configured to provide details of a first substitute account associated with a cardholder's valid credentials. The payment card 36 of Fig 2 may also include additional components incorporated into the plastic substrate. The additional components are configured to provide details of additional substitute accounts associated with the cardholder's valid credentials. The first substitute account includes details that are distinct from the details of the second substitute account and are distinct from all additional substitute accounts. At least one of the first, second or additional substitute accounts is provided to a merchant (e.g. using a merchant terminal 16) for conducting a financial transaction with the merchant

The merchant is configured to communicate the details of the at least one of the substitute accounts to the account correlating device 24 via the network 12. The account correlating device 24 is configured to associate at least one of the substitute accounts to one of the cardholder's valid credentials, and wherein the account correlating device 24 is further configured to manage financial transactions between the financial institution 28 associated with the cardholder's

primary financial account and the merchant terminal 16 associated with the merchant.

According to some embodiments, the payment card 36 of FIG. 2 may further include an additional component (e.g., card number 46) incorporated in the plastic substrate. The card number can be printed and/or embossed on the plastic substrate. In alternative embodiments, the payment card (e.g., payment card 60) may be devoid of at least one of a printed or embossed account number, a magnetic stripe, and or other modes.

The details of the first, second and additional substitute accounts may be read from the first, second, and additional components by a point-of-sale (POS) device, such as the merchant terminal 16. In order to conduct a financial transaction, some implementations may include use of the mobile device 20, which is associated with the cardholder.

FIG. 4 is a block diagram showing an embodiment of the account correlating device 24 shown in FIG. 1. In the embodiment of FIG. 4, the account correlating device 24 includes a security module 74, one or more web pages 76, a user account module 78, one or more network interfaces 80, and a transaction authentication module 82.

The one or more network interfaces 80 are configured to enable communication on the first public network 12 and also to enable communication on the secure network 26. The user account module 78 allows a user, or customer, to perform a number of different actions

related to the financial account and how the payment card 36, 60 can be used. The user account module 78 is described in more detail below with respect to FIG. 5.

The security module 74 may include a random number generator for generating a temporary dynamic card verification value (d-CVV). The d-CVV may be communicated to the mobile device. Also, the security module 74 may include an encryption engine for encrypting data transmitted over the public network 12. The account correlating device 24 may be configured as a web server that allows one or more users to access information from the web pages 76 and to establish a secure connection to enable the transfer of sensitive data, such as customer information, card numbers, etc. The transaction authentication module 82 is configured to authenticate a financial transaction using the payment card 36, 60.

In one embodiment, the token account details are protected by encryption using a cryptographic key, which can be provided by the security module 74. In one embodiment, the cryptographic key is derived from a customer created password. In another embodiment, the cryptographic key may instead depend on other data, including, but not limited to, the identity of the mobile device 20, the cardholding customer's identity number known to the security module 74 of the account correlating device 24, the country in which the cardholding customer registered for the computing service, a master key controlled

by biometric authentication of the cardholder, such as fingerprint, iris scan, facial or voice recognition, or biorhythmic pattern matching one or more body rhythms including, but not limited to, pulse rate, epidermal conductivity, iris size, blink rate, encephalography, electrocardiography, or other factors that are independently or in combination considered as biomarkers for individuality.

Normal plastic cards may have a single three- or four-digit CVV imprinted on either the back or front of the card. Electronic commerce sites now routinely ask for this value to ensure the customer has the card in their possession. But since the CVV is a short number printed on the card, it can easily be stolen together with the card account data. Therefore, use of a dynamic CVV (d-CVV), which may be generated by the security module 74 at the time of the transaction, and good for only one transaction, prevents this form of theft. In some embodiments, instead of using the generated d-CVV for only one transaction, the d-CVV may apply to multiple transactions associated with a specific merchant or may be used multiple times according to other criteria, such as a range of days, certain days of the week, area code of merchant, category of purchase, etc. According to some embodiments, a mobile application running on a mobile device 20 associated with the cardholder may be configured to retrieve the d-CVV on demand. Alternatively, a web site provided by the account correlating device 24

may be used when the mobile device 20 is unavailable. Therefore, in this case, the account correlating device 24 may generate the d-CVV.

In addition to use during financial transactions, the system 10 may alternatively be applied to non-payment uses. For example, the system 10 may be used for replacing some form of identifier with a token or substitute identifier. Such identifiers might include social security numbers (in the U.S.), public health identification numbers, loyalty programs, other forms of account numbers where a risk of disclosure, identity theft, or other fraud might be possible using the genuine number.

The account correlating device 24 may also find application to provide limited transaction access to protected record sets such as medical records requests, laboratory results, credit inquiries, professional licensing, commercial licensing, and other forms of relying party inquiries which utilize a government or enterprise issued identifying account number.

The payment card system 10 may also be used in some transactions for non-payment uses which could include driving licenses, border control documents, building and resource access cards, and gift cards. In this embodiment, the payment card 36, 60 may use one or more of the modes for non-payment uses while still using one or more of the modes for payment transactions using separate substitute account details for different modes.

In some embodiments, the account correlating device 24 may include at least one network interface 80 configured to communicate with a plurality of merchant terminals 16 via the first public network 12 and to communication with the financial institution 28 via the secure network 26. For example, the financial institution 28 may be a bank that issues the payment card 36, 60 to the cardholder. The account correlating device 24 may also include the transaction authentication module 82 configured to authenticate a first financial transaction for a first merchant terminal of the plurality of merchant terminals 16 based on a first set of details obtained by the first merchant terminal of a first substitute account associated with a payment card 36, 60 owned by a cardholder. The transaction authentication module 82 may be further configured to authenticate a second financial transaction for a second merchant terminal of the plurality of merchant terminals 16 based on a second, different set of details obtained by the second merchant terminal of a second substitute account associated with the payment card 36, 60 owned by the cardholder.

The transaction authentication module 82 may be further configured to determine if the substitute accounts correspond to valid credential of the cardholder. The transaction authentication module 82 may be further configured to determine if the received substitute account details correspond to the expected substitute account details for the mode of payment card that was used. The transaction

authentication module 82 is further configured to manage financial transactions between the financial institution 28 and the first and second merchant terminals 16. The transaction authentication module 82 is further configured to authenticate additional financial transactions for additional merchant terminals of the plurality of merchant terminals 16 based on additional set of details obtained by the additional merchant terminals of additional substitute accounts associated with the primary account of the payment card 36, 60 owned by the cardholder. The first set of details may be obtained from a microchip 44 on the payment card 36, 60, the second set of details may be obtained from a magnetic stripe 52 on the payment card 36, and a third set of details may be obtained from card numbers 46 printed and/or embossed on the payment card 36.

The network interface 80 may be further configured to communicate with a remote device (e.g., user device 14 or mobile device 20) associated with the cardholder via the network 12. The network interface 80 may be further configured to receive instructions from the remote device 14, 20 to enable the cardholder to manage a primary account associated with the payment card 36, 60, wherein managing the primary account includes at least one of entering enrollment information 86, monitoring 94 the activities of the primary account, enabling and disabling 90 one or more modes of conducting transactions with the payment card, reporting 92 that the payment card

has been lost or stolen, and provisioning 88 information related to the first and second substitute accounts.

FIG. 5 is a block diagram showing an embodiment of the user account module 78 shown in FIG. 4. In this embodiment, the user account module 78 includes an enrollment module 86, a provisioning module 88, an enabling module 90, a reporting module 92, and a monitoring module 94. A user may access the user account module 78 using a mobile application running on the cardholder's mobile device 20 or by accessing a web site provided by the account correlating device 24 using the cardholder's user device 14.

The user account module 78 enables the cardholding customer to establish and manage rules which the account correlating device 24 implements on the cardholding customer's behalf. Such rules may be sensitive to one or more facts known to the cardholding customer, including, but not limited to, payment value, merchant ID, local time and date encoded in a transaction message, the distance of registered location of the merchant from the geographic location of the cardholding customer's mobile device at the time of the transaction, the local currency of the transaction, the country in which the transaction is presented, the country in which the merchant is established, whether the transaction is presented as a magnetic stripe transaction, as an EMV transaction, or as an electronic commerce, telephone, or mail order transaction, and the method of cardholder verification such as

one or more of, but not limited to, entry of a personal identification number (PIN) code into the merchant POS terminal, signing a receipt, entering a passcode into a mobile device, and fingerprint or other biometric identification method.

The enrollment module 86 may be configured to enable a cardholder to enroll additional substitute accounts and additional valid credentials. The enabling module 90 may be used to allow the cardholder to enable or disable certain modes or types of transactions depending on the various uses that the cardholder may anticipate based on various criteria, or to enable or disable specific transactions themselves, prior to their authentication. The enabling module 90 may be used to allow the cardholder to nominate which valid credential a payment will be charged against in a variety of scenarios or criteria. The reporting module 92 allows the user to report if the payment card 36, 60 has been lost or stolen. One embodiment of the reporting module 92 may enable the account correlating device 24 to report manually or automatically relevant information to the user or financial institution 28, including reporting potentially fraudulent activity across the substitute account details and/or payment card. The monitoring module 94 allows the user to view previous transactions to monitor all activity of the card.

The provisioning module 88 may allow the user to separately distinguish the multiple different sets of substitute account details.

Conventional card issuing systems may assume that certain data elements are shared among the microchip, magnetic stripe, and printed/embossed card number. However, as opposed to the conventional card issuing systems, the provisioning module 88 allows the provisioning of each of these and further elements using separate data elements. The provisioning module 88 is configured to separately identify these multiple distinct sets of substitute account data, which may be stored in a common provisioning data file conveyed during card provisioning steps.

A cardholder may become subject to unauthorized use of their payment card 36, 60 if it is lost or stolen. However, although in some countries a thief may be able to use the NFC features for purchases under to certain spending threshold (e.g., $100), the thief will normally not be able to use the EMV features of the card without the cardholder's PIN code, which can be entered during the provisioning process using the provisioning module 88. Also, the stolen card cannot be used for electronic or telephone commerce due to the distinct account details for this separate transaction mode.

The provisioning module 88 may further include receiving identifying information of the cardholder that is not printed on the payment card 36, 60. According to some embodiments, the provisioning module 88 may set up the cardholder's usage rules by requiring the presence of the cardholder's mobile device 20 in

conjunction with the transaction using the payment card 36, 60. Also, the mobile application of the mobile device 20 may be used to instantly block transactions from a stolen card that is reported stolen by the reporting module 92. The user account module 78 might configure its rules to prevent magnetic stripe transactions unless they are unlocked each time by the cardholder using the mobile application on the mobile device 20. This latter method would effectively prevent the use of counterfeit magnetic stripe cards. The user account module 78 might also configure its rules to prevent transactions from any and all different modes, or to prevent transactions that fall under certain criteria, unless they are unlocked each time by the cardholder.

In one embodiment, a mobile application is available on the cardholding customer's primary mobile device 20. The mobile application may be used by the cardholding customer to enroll a substitute account or valid credential into the account correlating device 24, control the provisions or associations of the valid credentials with the one or more substitute account details provisioned to the payment card. The mobile application also allows the user to enable or disable the authorization of transactions presented with any of the substitute accounts provisioned to the plastic payment card, report the payment card as lost or stolen, and as an additional authentication factor for sensitive or high-value or high-risk transactions.

The mobile device 20 may also store substitute account details, which may be associated with “card present” transactions and “card not present” transactions, in memory. These substitute account details may be stored in the memory and can be recalled by the customer by entering a password and/or another authentication factor into the mobile device 20. As a means for interacting with electronic commerce sites, the mobile application securely holds the electronic commerce substitute account details and displays them for the user upon proper authentication with password, biometrics, and/or other factors. In another embodiment, the substitute account details are transmitted by account correlating device 24 and are received by the mobile device 20, which can then be recalled by the customer by entering a password and/or another authentication factor into the mobile device 20.

The implementations described herein represent a number of possible implementations and examples and are not intended to necessarily limit the present disclosure to any specific implementations. Instead, various modifications can be made to these implementations as would be understood by one of ordinary skill in the art. Any such modifications are intended to be included within the spirit and scope of the present disclosure.

WHAT IS CLAIMED IS:

1. A payment card comprising:

a first component incorporated into a plastic substrate, the first component configured to provide details of a first substitute account associated with a cardholder's valid credentials; and

at least one additional component incorporated into the plastic substrate, each of the at least one additional component configured to provide details of at least one additional substitute account associated with the cardholder's valid credentials;

wherein each substitute account includes details that are distinct from the details of each of the other substitute accounts; and

wherein at least one of the substitute accounts is provided to a merchant for conducting a financial transaction with the merchant.

2. The payment card of claim 1, wherein the merchant is configured to communicate the details of at least one of the substitute accounts to an account correlating device via a network, wherein the account correlating device is configured to associate at least one of the substitute accounts to the cardholder's valid credentials, and wherein the account correlating device is further configured to manage financial transactions between a financial institution associated with the cardholder's valid credentials and a merchant terminal associated with the merchant.

3. The payment card of claim 1, wherein the first component is one of a microchip, a near field communication (NFC) device, and a magnetic stripe incorporated in or on the plastic substrate and the at least one additional component is another of the microchip, NFC device, and a magnetic stripe.

4. The payment card of claim 3, wherein one of the at least one additional component includes a card number printed or embossed on the plastic substrate.

5. The payment card of claim 1, wherein the payment card is devoid of at least one of a printed or embossed account number and a magnetic stripe.

6. The payment card of claim 1, wherein a mobile device associated with the cardholder is used to complete a financial transaction.

7. The payment card of claim 1, wherein the details of the substitute accounts are read from the components by merchant terminals.

8. An account correlating device comprising:

at least one network interface configured to communicate with a plurality of merchant terminals via a network and to communicate with a financial institution via a network; and

a transaction authentication module configured to authenticate a financial transaction for a merchant terminal of the plurality of merchant

terminals based on a set of details obtained by the merchant terminal of a substitute account associated with a payment card owned by a cardholder;

wherein the transaction authentication module is further configured to authenticate additional financial transaction for additional merchant terminal of the plurality of merchant terminals based on an additional, different set of details obtained by the additional merchant terminal of an additional substitute account associated with the payment card owned by the cardholder.

9. The account correlating device of claim 8, wherein the transaction authentication module is further configured to determine if substitute accounts correspond to an expected account identifier for the mode used for the transaction, and reject, process, or suspend the transaction if needed.

10. The account correlating device of claim 8, wherein the financial institution issues the payment card to the cardholder, and wherein the transaction authentication module is further configured to manage financial transactions between the financial institution and the first and second and additional merchant terminals, and process payments to a valid credential as nominated in the user account module.

11. The account correlating device of claim 8, wherein the transaction authentication module is further configured to authenticate

an additional financial transaction for an additional merchant terminal of the plurality of merchant terminals based on an additional, different set of details obtained by the additional merchant terminal of an additional substitute account associated with the payment card owned by the cardholder.

12. The account correlating device of claim 11, wherein the first, second and third sets of details are obtained from a microchip, a near field communication (NFC) device, and a magnetic stripe on the payments card, and the fourth set of details is obtained from card numbers printed or embossed on the payment card, and additional sets of details obtained via other modes as available.

13. The account correlating device of claim 11, wherein at least one of the first and second merchant terminals is a point-of-sale (POS) device.

14. The account correlating device of claim 8, wherein the network interface is further configured to communicate with a remote device associated with the cardholder via the first network.

15. The account correlating device of claim 14, wherein the network interface is further configured to receive instructions from the remote device to enable the cardholder to manage a valid credential associated with the payment card, wherein managing the valid credential includes at least one of entering enrollment information, monitoring the activities of the valid credential, enabling and disabling

one or more modes of conducting transactions with the payment card, reporting that the payment card has been lost or stolen, and provisioning information related to the multiple substitute accounts associated with the card.

16. The account correlating device of claim 8, further comprising one or more webpages of a website enabling the cardholder to manage the details or navigate the website using the user device.

17. A system for providing security for a payment card, the system comprising:

a first merchant terminal connected to a network, the first merchant terminal configured to obtain details of a first substitute account from a first set of information associated with a payment card owned by a cardholder;

a second merchant terminal connected to the network, the second merchant terminal configured to obtain details of a second substitute account from a second set of information associated with the payment card;

additional merchant terminals connected to the network, the additional merchant terminals configured to obtain details of additional substitute accounts from additional sets of information associated with the payment card; and

an account correlating device connected to the network, the account correlating device configured to receive the details of the first

and subsequent substitute accounts from the first and subsequent merchant terminals, respectively, the account correlating device further configured to associate the first and subsequent substitute accounts to valid credentials belonging to the cardholder;

wherein the account correlating device manages financial transactions between a financial institution, from which the cardholder retains the valid credentials, and the first and subsequent merchant terminals; and

wherein the first set of information is different from the subsequent sets of information.

18. The system of claim 17, further comprising additional merchant terminals connected to the network, the additional merchant terminals configured to obtain details of additional substitute accounts from additional sets of information associated with the payment card.

19. The system of claim 18, wherein the first, second and third sets of information is obtained from a magnetic stripe, a microchip and a near field communication (NFC) device on the payment card, and the fourth set of information is obtained from card numbers printed or embossed on the payment card.

20. The system of claim 17, wherein the payment card is devoid of at least one of a printed or embossed account number and a magnetic stripe.

21. The system of claim 17, further comprising a mobile device associated with the cardholder.

22. The system of claim 21, wherein the mobile device calculates, stores or receives a dynamic card verification value (d-CVV) to verify a transaction.

23. The system of claim 22, wherein at least one of the first, second and additional merchant terminals is an online merchant device configured to conduct an online transaction, and wherein the mobile device or the user, via manual entry or other method, transmits the d-CVV to the online merchant device.

24. The system of claim 17, wherein at least one of the first and second merchant terminals is embedded within a physical point-of-sale (POS) device.

25. The system of claim 17, further comprising a user device associated with the cardholder, the user device enabling the cardholder to manage the valid credentials via the account correlating device, and wherein the account correlating device is configured to enable the cardholder to enter enrollment information, monitor the activities of the valid credentials and associate them to various substitute accounts, enable and disable one or more modes of conducting transactions with the payment card, report that the payment card has been lost or stolen, and provision information related to the first and second substitute accounts.

26. The system of claim 25, wherein the account correlating device provides a website including one or more webpages enabling the cardholder to navigate the website using the user device.

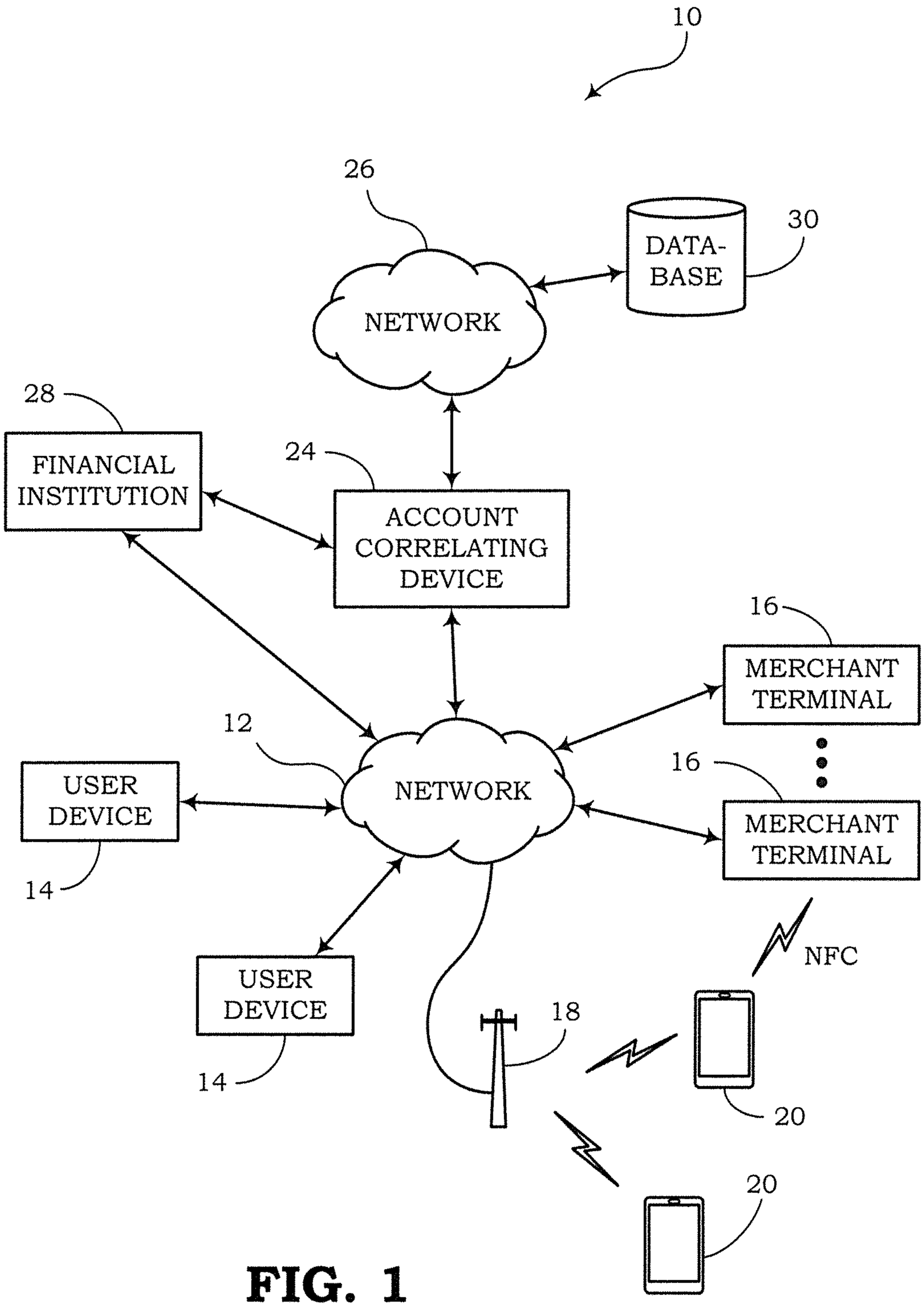

10
26
NETWORK
DATA-
BASE
30
28
FINANCIAL
INSTITUTION
24
ACCOUNT
CORRELATING
DEVICE
16
MERCHANT
TERMINAL
12
NETWORK
16
MERCHANT
TERMINAL
USER
DEVICE
14
NFC
USER
DEVICE
14
18
20
20

FIG. 1

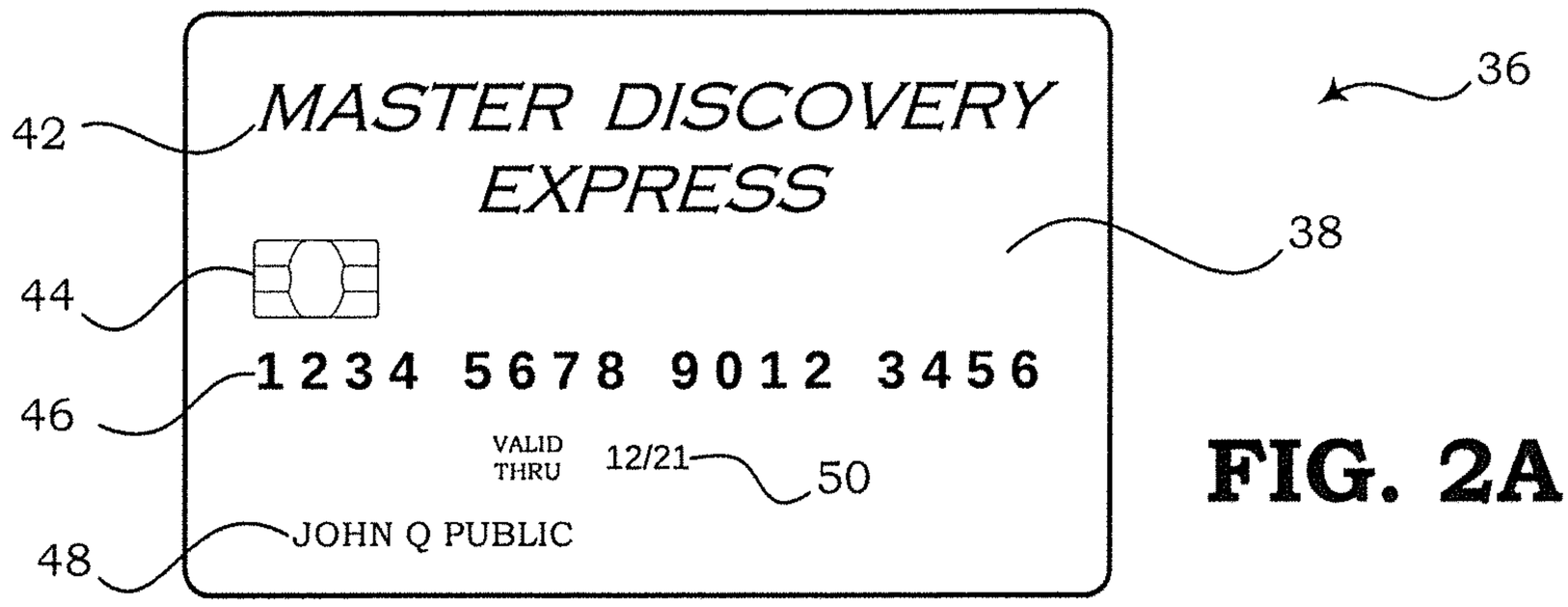


FIG. 2A

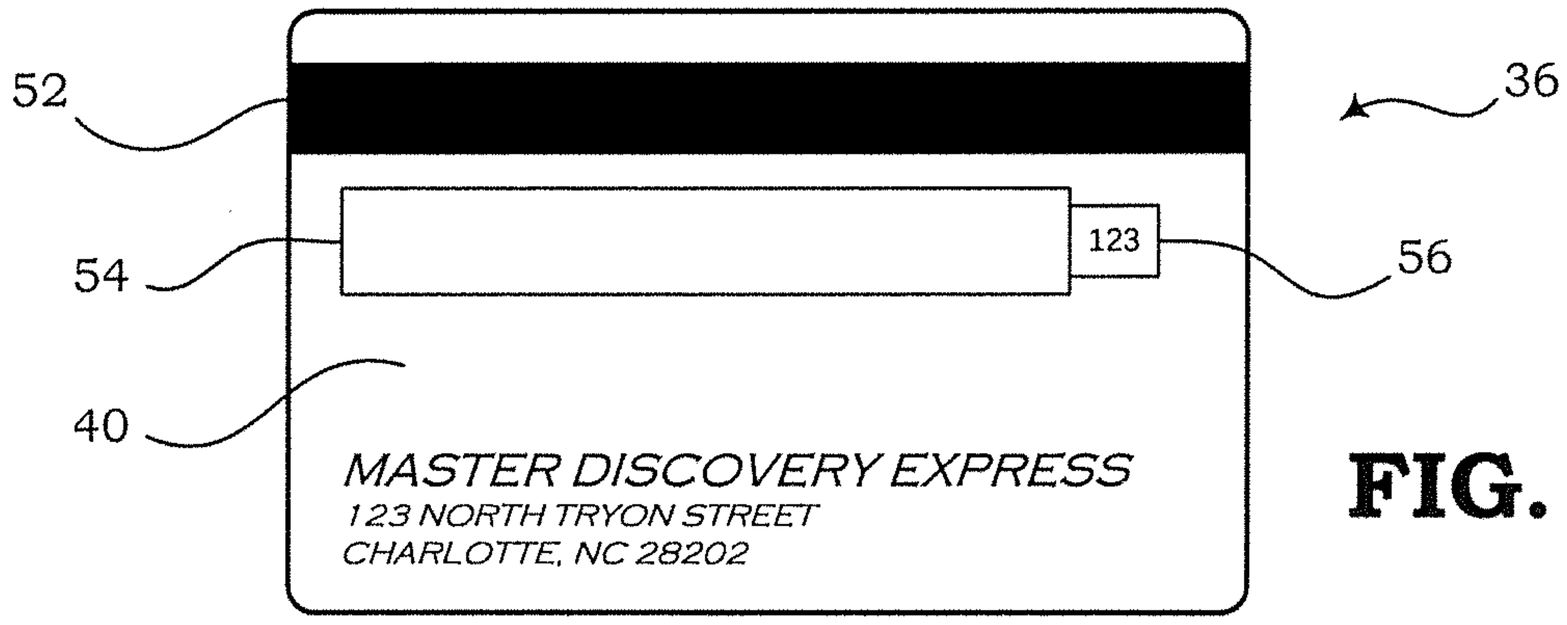


FIG. 2B

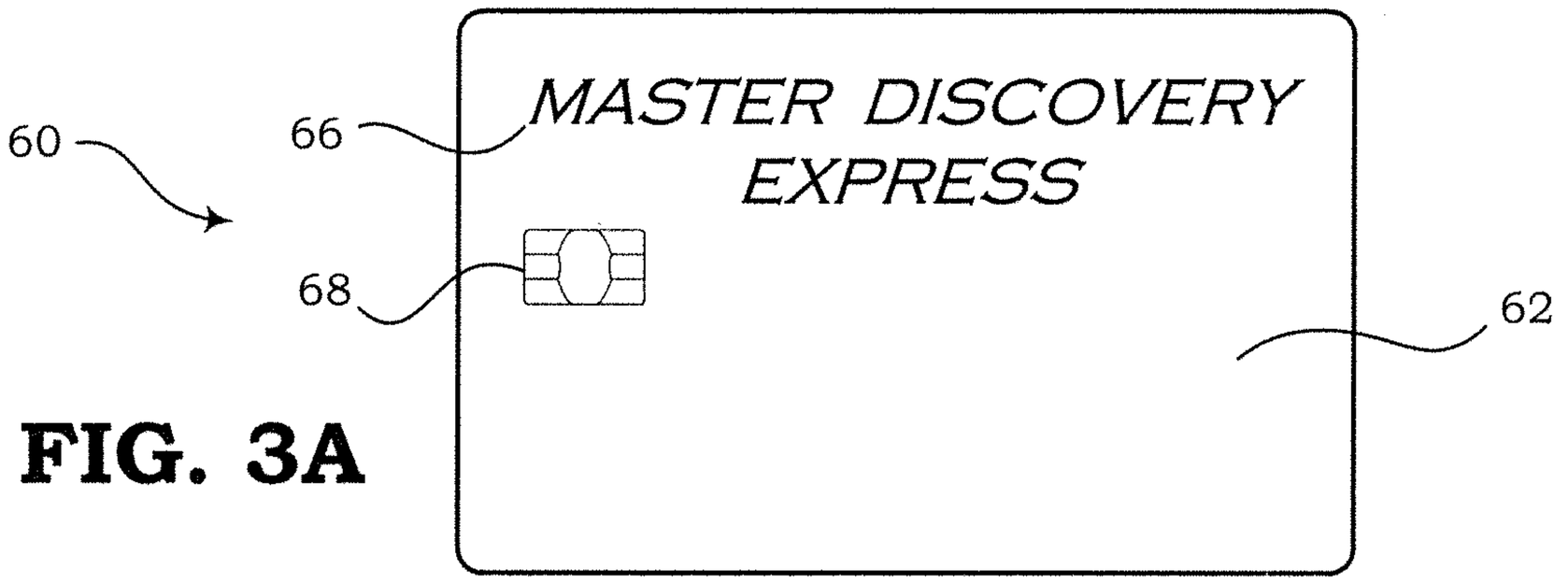


FIG. 3A



FIG. 3B

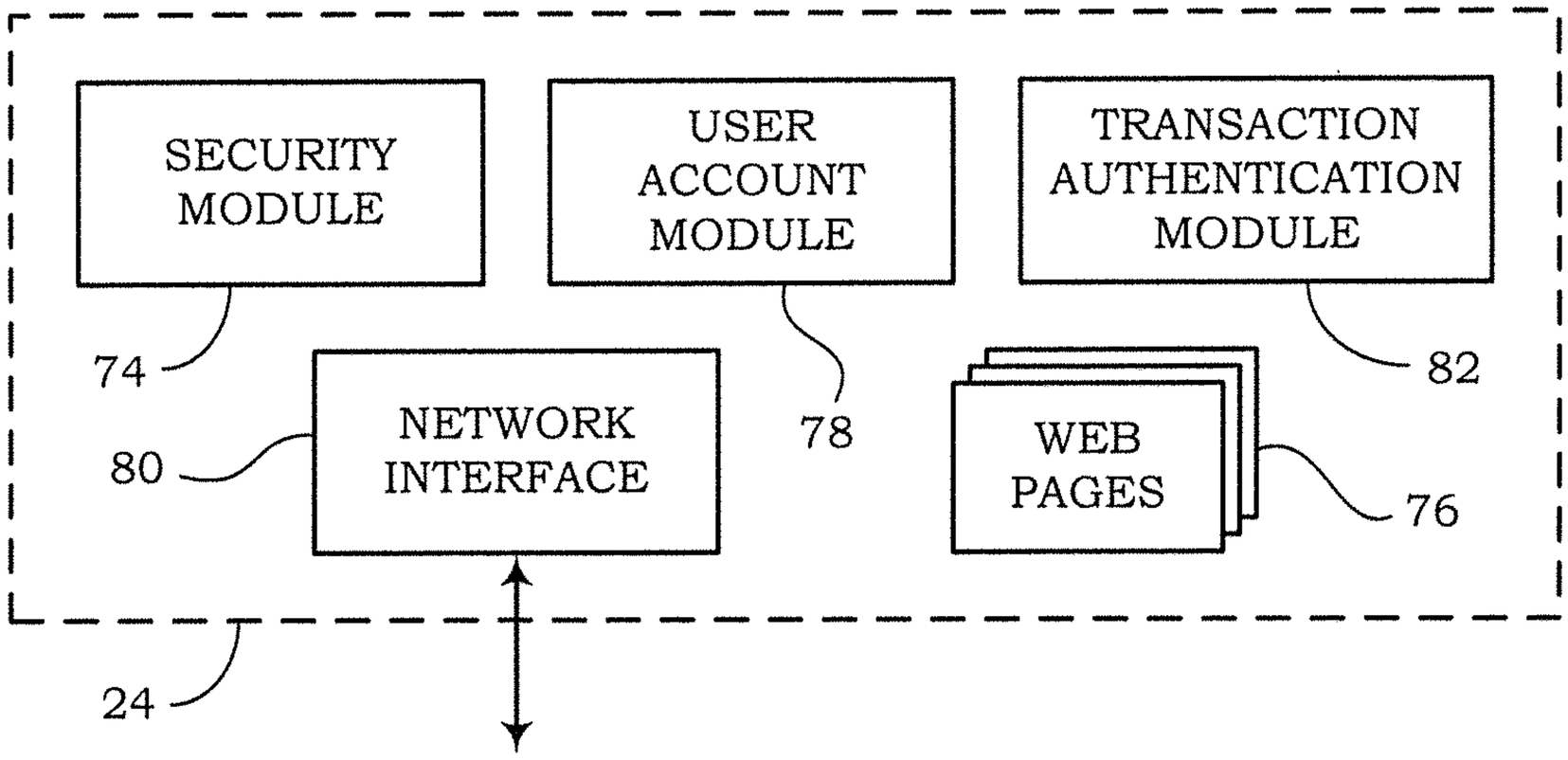

SECURITY MODULE
USER ACCOUNT MODULE
TRANSACTION AUTHENTICATION MODULE
74
78
82
NETWORK INTERFACE
80
WEB PAGES
76
24

FIG. 4

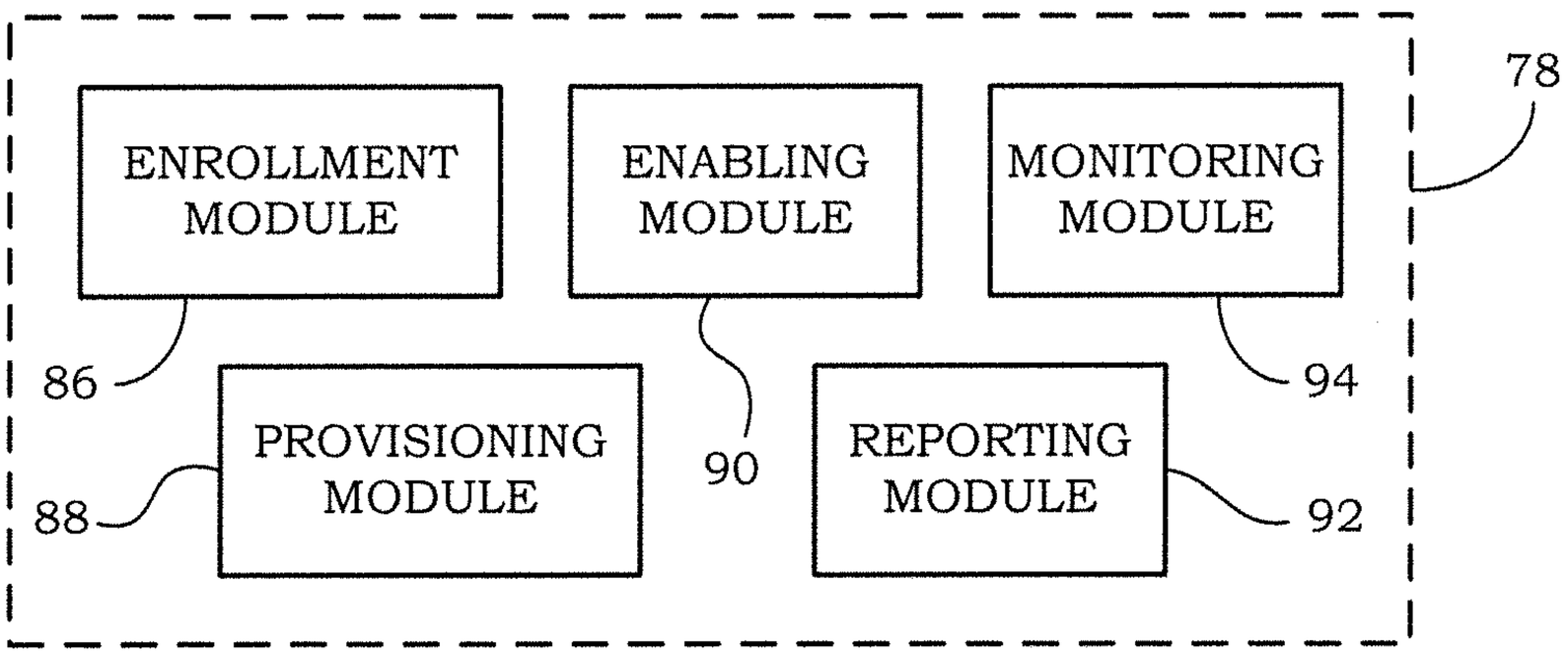

78
ENROLLMENT MODULE
ENABLING MODULE
MONITORING MODULE
86
90
94
PROVISIONING MODULE
REPORTING MODULE
88
92

FIG. 5

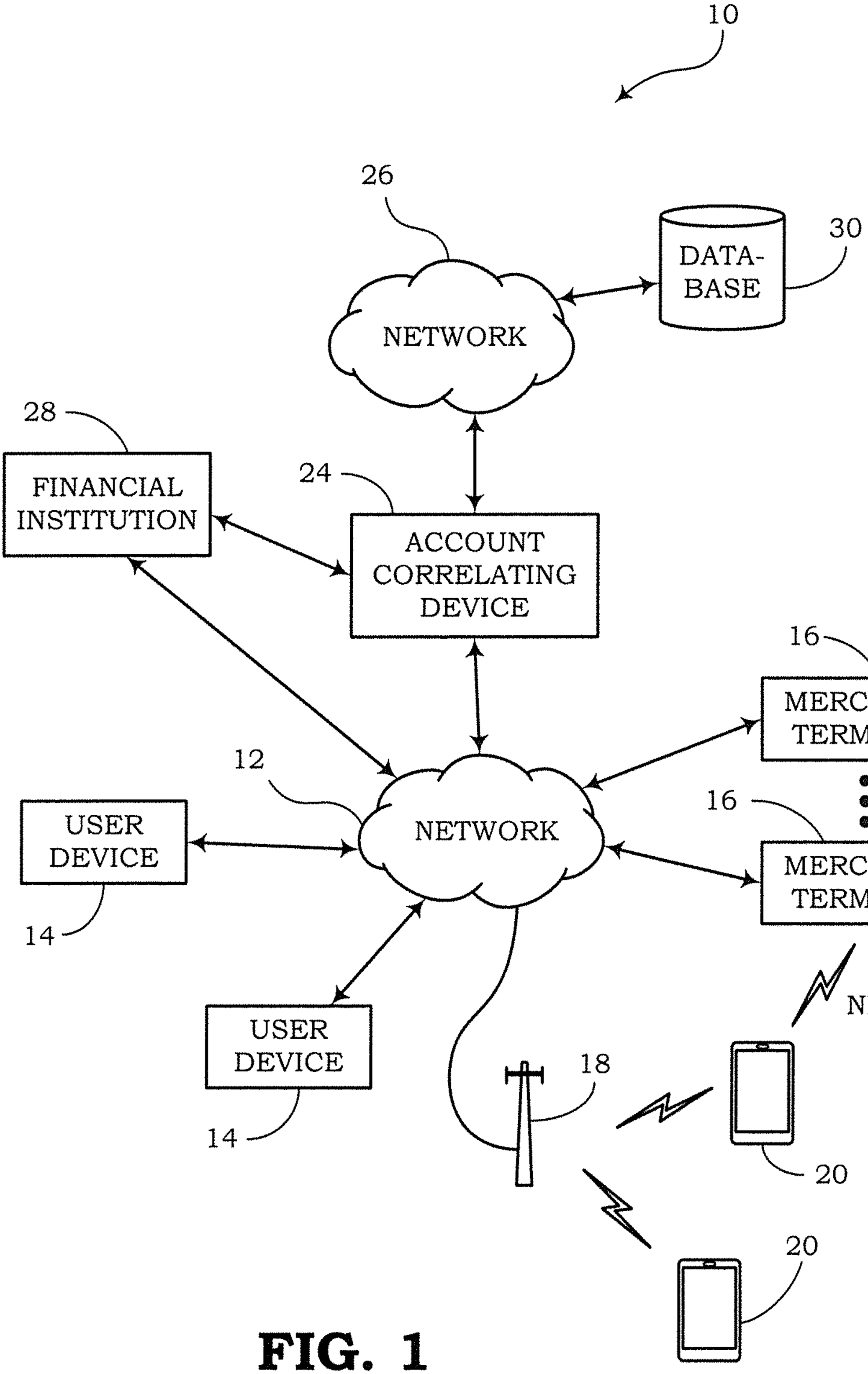

10
26
NETWORK
DATA-
BASE
30
28
FINANCIAL
INSTITUTION
24
ACCOUNT
CORRELATING
DEVICE
16
MERCHANT
TERMINAL
12
NETWORK
USER
DEVICE
14
MERCHANT
TERMINAL
NFC
USER
DEVICE
14
18
20
20

FIG. 1