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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 November 2010 (11.11.2010)

PCT

(10) International Publication Number
WO 2010/129357 A2

(51) International Patent Classification:
G06Q 20/00 (2006.01)

(21) International Application Number:
PCT/US2010/032825

(22) International Filing Date:
28 April 2010 (28.04.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/173,371	28 April 2009 (28.04.2009)	US
61/178,636	15 May 2009 (15.05.2009)	US
12/768,661	27 April 2010 (27.04.2010)	US

(71) Applicant *(for all designated States except US)*: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, MS M1-11F, San Francisco, CA 94128-8999 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **HAMMAD, Ayman** [US/US]; 6981 Corte Mercado, Pleasanton, CA 94566 (US).

(74) Agents: **YEAGER, Hal, R.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111-3834 (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, 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, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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, 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, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, 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 (Rule 48.2(g))*

(54) **Title**: VERIFICATION OF PORTABLE CONSUMER DEVICES

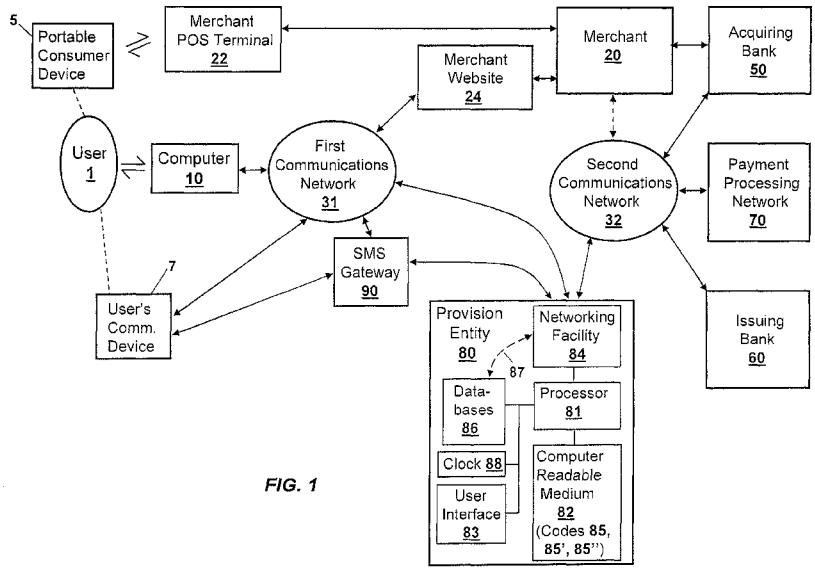


FIG. 1

(57) **Abstract**: Embodiments of the invention are directed to methods, systems, and computer program products pertaining to obtaining, providing, and using dynamic card verification values for portable consumer devices, such as credit cards and debit cards. An exemplary method comprises receiving, at a server, a request for a device verification value for a portable consumer device associated with a user; obtaining, at the server, a datum indicative of a device verification value for a portable consumer device; and sending, from the server, the datum to at least one of a phone number or network address of a personal communication device associated with the user.

WO 2010/129357 A2

VERIFICATION OF PORTABLE CONSUMER DEVICES

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application claims priority from United States Patent Application No. 12/768,661, entitled "Verification of Portable Consumer Devices," filed April 27, 2010, United States Provisional Patent Application No. 61/178,636, entitled "Dynamic Data Authentication," filed May 15, 2009, and from United States Provisional Patent Application No. 61/173,371, entitled "Alerts Based Systems and Method," filed April 28, 2009, the contents of all of which are hereby incorporated in their entirety by reference for all purposes. For the United States, this application is also a continuation-in-part of United States Patent Application No. 12/768,661, entitled "Verification of Portable Consumer Devices," filed April 27, 2010.

BACKGROUND

[0002] As methods and devices for engaging in financial transactions have increased, old problems such as fraud and counterfeiting persist.

[0003] One of the primary sources of fraud, which is prevalent in the credit card industry, is skimming. Skimming refers to the electronic copying of a card's magnetic stripe data to create counterfeit cards.

[0004] Skimming is predominantly a phenomenon afflicting static magnetic stripe based transactions. This is because the magnetic stripe, which is placed on the back of a transaction card and stores a variety of data on three separate tracks, is a passive medium. In other words, the digital content of the magnetic stripe can be perfectly copied, without any difference between the copy and the original.

[0005] One of the primary means by which skimming can be prevented is for the consumer to closely monitor the whereabouts of his transaction card. This may allow the consumer to prevent the card from being swiped through inappropriate devices. However, as contactless cards evolve, the classic skimming problem comes along with it when using static data. In fact, in a wireless environment, the opportunity to skim magnetic stripe data is more prevalent. In a wireless environment, a potential skimmer

need not physically possess the card to be skimmed nor have access to any of the physical equipment (e.g. POS terminal, communication lines, etc.) which is required for skimming in a wire-based environment. A skimmer can, without the knowledge of the consumer or merchant, intercept the wireless transaction and copy the data being transmitted from the card to POS terminal.

[0006] To address the above problems, a dCVV or a dynamic card verification value can be used. For example, various systems and methods for generating dCVVs are discussed in U.S. Pat. App. No. 10/642,878 entitled "Method and System for Generating a Dynamic Verification Value" filed on August 18, 2003, and in U.S. Pat. App. No. 11/764,376 entitled "On-Line Payment Transactions" filed on January 29, 2008. Both of these applications are hereby incorporated in their entirety for all purposes.

[0007] In addition to generating a dCVV, a dCVV can be more effective for preventing fraud when it is securely received by a consumer. However, securely receiving and using a dCVV cannot overly interfere with a consumer's experience conducting a transaction. A consumer might not use the dCVV or a consumer might conduct fewer transactions if the inconvenience of receiving and using a dCVV is too great.

[0008] Embodiments of the invention address the above problems, and other problems, individually and collectively.

SUMMARY

[0009] Embodiments of the invention are directed to methods, systems, and computer program products pertaining to obtaining, providing, and using dynamic card verification values for portable consumer devices.

[0010] One exemplary embodiment of the invention is directed to a method of providing a device verification value for a portable consumer device. The exemplary method comprises receiving, at a server, a request for a device verification value for a portable consumer device associated with a user; obtaining, at the server, a datum indicative of a device verification value for a portable consumer device; and sending, from the server, the datum to at least one of a phone number or network address of a personal communication device associated with the user.

[0011] Another exemplary embodiment of the invention is directed to a server for providing device verification values for portable consumer devices. The server comprises a data processor, a networking facility coupled to the processor, a computer-readable medium coupled to the processor, and a plurality of codes embodied on (*e.g.*, stored in) the computer readable medium. A first exemplary code directs the data processor to receive a request for a device verification value for a portable consumer device associated with a user. A second exemplary code directs the data processor to obtain a datum indicative of a device verification value for a portable consumer device. A third code directs the data processor to send the datum to at least one of a phone number or network address of a personal communication device associated with the user.

[0012] Another exemplary embodiment of the invention is directed to a computer program product embodied on a tangible computer-readable medium that directs a data processor to provide device verification values for portable consumer devices. The exemplary computer program product comprises a first code that directs the data processor to receive a request for a device verification value for a portable consumer device associated with a user; a second code that directs the data processor to obtain a datum indicative of a device verification value for a portable consumer device; and a third code that directs the data processor to send the datum to at least one of a phone number or network address of a personal communication device associated with the user.

[0013] Another exemplary embodiment of the invention is directed to a method of providing a device verification value for a portable consumer device. The exemplary method comprises receiving, at a server, a request for a device verification value for a portable consumer device associated with a user, the request originating from a personal communication device associated with the user; obtaining, from the received request, a phone number or network address of the personal communication device from which the received request was originated; obtaining an account record that contains the obtained phone number or network address, the account record associating a consumer account of a portable consumer device with the obtained phone number or network address; obtaining a datum indicative of a device verification value for the consumer account of the obtained account record; and sending the obtained

datum to at least one of a phone number or network address of a personal communication device associated with the consumer account of the obtained account record.

[0014] Another exemplary embodiment of the invention is directed to a server for providing device verification values for portable consumer devices. The server comprises a data processor, a networking facility coupled to the processor, a computer-readable medium coupled to the processor, and a plurality of codes embodied on (*e.g.*, stored in) the computer readable medium. A first code directs the data processor to receive a request for a device verification value for a portable consumer device associated with a user, the request originating from a personal communication device associated with the user. a second code directs the data processor to obtain, from the received request, a phone number or network address of the personal communication device from which the received request was originated. A third code directs the data processor to obtain an account record that contains the obtained phone number or network address, the account record associating a consumer account of a portable consumer device with the obtained phone number or network address. A fourth code directs the data processor to obtain a datum indicative of a device verification value for the consumer account of the obtained account record. A fifth code directs the data processor to send the obtained datum to at least one of a phone number or network address of a personal communication device associated with the consumer account of the obtained account record.

[0015] Another exemplary embodiment of the invention is directed to a computer program product embodied on a tangible computer-readable medium that directs a data processor to provide device verification values for portable consumer devices. The computer program product comprises: code that directs a data processor to receive a request for a device verification value for a portable consumer device associated with a user, the request originating from a personal communication device associated with the user; code that directs the data processor to obtain, from the received request, a phone number or network address of the personal communication device from which the received request was originated; code that directs the data processor to obtain an account record that contains the obtained phone number or network address, the account record associating a consumer account of a portable consumer device with the

obtained phone number or network address; code that directs the data processor to obtain a datum indicative of a device verification value for the consumer account of the obtained account record; and code that directs the data processor to send the obtained datum to at least one of a phone number or network address of a personal communication device associated with the consumer account of the obtained account record.

[0016] Another exemplary embodiment of the invention is directed to a method of providing a device verification value for a portable consumer device. The exemplary method comprises: receiving, at a server, a request for a device verification value for a portable consumer device associated with a user; obtaining, from the received request, a unique identification code assigned to the user; obtaining an account record that contains the obtained unique identification code, the account record associating a consumer account of a portable consumer device with the obtained unique identification code, the consumer account having an account number associated with it that identifies the consumer account within a payment processing network, the obtained unique identification code being different from the account number of the consumer account of the obtained account record; obtaining a datum indicative of a device verification value for the consumer account of the obtained account record; and sending the obtained datum to at least one of a phone number or network address of a personal communication device associated with the consumer account of the obtained account record.

[0017] Another exemplary embodiment of the invention is directed to a server for providing device verification values for portable consumer devices. The server comprises a data processor, a networking facility coupled to the processor, a computer-readable medium coupled to the processor, and a plurality of codes embodied on (*e.g.*, stored in) the computer readable medium. A first code directs the data processor to receive a request for a device verification value for a portable consumer device associated with a user. A second code directs the data processor to obtain, from the received request, a unique identification code assigned to the user. A third code directs the data processor to obtain an account record that contains the obtained unique identification code, the account record associating a consumer account of a portable consumer device with the obtained unique identification code, the consumer account

having an account number associated with it that identifies the consumer account within a payment processing network, the obtained unique identification code being different from the account number of the consumer account of the obtained account record. A fourth code directs the data processor to obtain a datum indicative of a device verification value for the consumer account of the obtained record. A fifth code directs the data processor to send the obtained datum to at least one of a phone number or network address of a personal communication device associated with the consumer account of the obtained account record.

[0018] Another exemplary embodiment of the invention is directed to a computer program product embodied on a tangible computer-readable medium that directs a data processor to provide device verification values for portable consumer devices. The computer program product comprises: code that directs a data processor to receive a request for a device verification value for a portable consumer device associated with a user; code that directs the data processor to obtain, from the received request, a unique identification code assigned to the user; code that directs the data processor to obtain an account record that contains the obtained unique identification code, the account record associating a consumer account of a portable consumer device with the obtained unique identification code, the consumer account having an account number associated with it that identifies the consumer account within a payment processing network, the obtained unique identification code being different from the account number of the consumer account of the obtained account record; code that directs the data processor to obtain a datum indicative of a device verification value for the consumer account of the obtained record; and code that directs the data processor to send the obtained datum to at least one of a phone number or network address of a personal communication device associated with the consumer account of the obtained account record.

[0019] Another exemplary embodiment of the invention is directed to a method of obtaining and using a device verification value for a portable consumer device. The exemplary method comprises: sending, using a portable communication device, a message to a provision entity requesting a device verification value for a consumer account, the consumer account having an account number that identifies the consumer account within a payment processing network, the message comprising at least one of a

code phrase or identification code that is different from said account number; receiving, at the portable communication device, a device verification value for the consumer account; and providing information related to the consumer account to a merchant for a transaction with the merchant, the information including the received device verification value.

[0020] Another exemplary embodiment of the invention is directed to a method of obtaining and using a device verification value for a portable consumer device. The exemplary method comprises: sending, using a portable communication device, a message to a provision entity requesting a device verification value for a consumer account, the consumer account having an account number that identifies the consumer account within a payment processing network, the message comprising an incomplete part of said account number; receiving, at the portable communication device, a device verification value for the consumer account; and providing information related to the consumer account to a merchant for a transaction with the merchant, the information including the received device verification value

[0021] Other exemplary embodiments of the invention are directed to computer program products embodied on tangible computer-readable medium that direct a personal communications device to send a request for a device verification value for a portable consumer device to a server that provides device verification values. Yet other embodiments are directed to personal communication devices that have these computer program products.

[0022] Further details regarding embodiments of the invention are provided below in the Detailed Description with reference to the Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] FIG. 1 shows a block diagram illustrating the components of various systems according various embodiments.

[0024] FIG. 2 shows a diagram of an exemplary user account record according to various embodiments.

[0025] FIG. 3 shows a flow diagram illustrating general actions of various method embodiments.

[0026] FIG. 4 shows a block diagram illustrating the components of various personal communication devices useable with various embodiments.

[0027] FIG. 5 shows a flow diagram illustrating general actions of various method embodiments.

[0028] FIG. 6 shows a flow diagram illustrating general actions of various method embodiments.

DETAILED DESCRIPTION

[0029] Embodiments of the present invention are able to maintain or improve existing user experiences, minimize the impact on merchant processes/systems, leverage existing network data transport mechanisms, utilize existing issuer validation infrastructure, support multiple forms of implementation, and maintain consistency with broader authentication strategy.

[0030] Generally, embodiments of the present invention pertain to methods, systems, and computer-program products of generating dynamic card verification values, referred to herein as the "dCVV" values, for portable consumer devices. The dCVV value can be provided along with the payment information of the portable consumer device to increase the confidence that the use of the portable consumer device is authentic and not fraudulent *(e.g.*, not skimmed). The embodiments described below can be applied for both card present and card-not-present (CNP) transactions.

[0031] A portable consumer device comprises a device that holds identification information pertaining to an account held by a user with another entity, which is typically an entity that holds, extends, or credits items of value to the user (*e.g.,* monetary funds, credits, debts, *etc.*). Portable consumer devices encompass credit cards, charge cards, debit cards, bank cards, prepaid cards, access cards, security cards, and other cards that identify an account held by a user with another entity. The cards are capable of existing in both passive forms (*e.g.,* cards with a magnetic stripe) and active forms (*e.g.,* integrated circuit cards, smartcards), and further encompass portable electronic devices

that, in whole or in part, function as such cards. Such portable electronic devices can include memory cards, account tokens, fobs, stickers, cellular telephones (including near-field communications phone), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), personal digital assistants, other mobile electronic devices, transponders, smart media, and pagers.

[0032] A typical credit card transaction flow using a portable consumer device at a point-of-sales location is described next. The user's portable consumer device is provided to the user by or on behalf of an issuing bank. The issuing bank extends credit to the user, represents the user in credit card transactions, and pays merchants for the purchases made by the user. A user presents his or her portable consumer device to a merchant at a point-of-sales location to pay for an item or service. The merchant uses a reader to read the user's portable consumer device, and sends the payment information read from the device along with merchant's information and the transaction amount to an acquiring bank. The merchant may also read the portable consumer device for the printed card verification value (*e.g.,* the CVV value printed on the backs of many credit cards), and may send this along as part of the transaction information sent to the acquiring bank. The acquiring bank represents, and vouches for, the merchant in credit card transactions. The acquiring bank forwards the transaction information to a payment processing network, such as VisaNet™, for authorization. A payment processing network generally encompasses a collection of one or more data processing server computers, subsystems, networks, and operations used to support and deliver one or more of the following: authorization services, exception file services, and clearing and settlement services. Payment processing networks encompass bank processing networks, credit-card payment processing networks, etc. An exemplary payment processing network may include VisaNet™. Exemplary payment processing networks are able to process one or more of the following: credit-card transactions, debit-card transactions, and other types of commercial transactions. A payment processing network may use any suitable wired or wireless network, including the Internet, to communicate with acquiring banks and issuing banks.

[0033] Prior to the occurrence of a credit-card transaction, the payment processing network has established a protocol with each issuing bank on how the bank's transactions are to be authorized. In some cases, such as when the transaction amount

is below the threshold value, the payment processing network will authorize the transaction based on information that it has about the user's account without consulting the issuing bank, and will accept the liability if the transaction turns out to be fraudulent. In other cases, such as when the transaction amount is above a threshold value, the payment processing network will forward the transaction information on to the issuing bank for verification and authorization. As part of the authorization process, the payment network or the issuing bank may verify the printed CVV value, which is stored at the issuing bank, and may be securely provided by the issuing bank to the payment processing network for storage and subsequent use. The degree to which the payment processing network is involved in the verification of the consumer portable device and the authorization of the transaction is typically configured according to the wishes of the issuing bank. Once the transaction is authorized, the payment processing network sends an authorization indication to the acquiring bank, which sends the authorization indication on to the merchant. In order to reduce fraud, merchants are not allowed to store printed card verification values (CVVs) for more than 24 hours.

[0034] When a user wishes to make an online purchase with a merchant over the Internet, the user types in the credit card account number, cardholder name, expiration date, and the printed CVV value of the portable consumer device into respective fields on the merchant's checkout page. This is the payment information associated with the portable consumer device. When the user confirms the purchase on the merchant's website, the merchant sends payment information along with merchant's information and the transaction amount to the acquiring bank for the merchant. The acquiring bank forwards the transaction information to a payment processing network, such as VisaNet™, for authorization, just as in the point-of-sales example.

[0035] In both purchasing environments, there is risk of fraudulent activity through skimming of the payment information. For example, a store clerk can copy down the payment information during a transaction at a point-of-sales location, and can later use the copied information to make an online purchase. As another example, a hacker can install spyware on the user's computer to intercept the payment information, and use it to make fraudulent purchases at other online merchants. Other avenues of potential fraud exist. Embodiments of the invention are directed to mitigating these types of fraudulent activity by replacing the use of the printed CVV value with a dynamically

changing value, which may change for each transaction or group of transactions, or may change according to a time schedule, that may be regular or irregular.

[0036] FIG. 1 illustrates several exemplary embodiments of the invention in the contexts of both an online purchase and in-store purchase at a point-of-sales (POS) terminal. A general overview description of the embodiments and components shown in the figure will be given, followed by more detailed descriptions. Shown in the figure are icons for a user **1**, the user's portable consumer device **5**, the user's personal communication device **7** (such as a cell phone), and the user's computer **10**. Also shown in the figure are a merchant entity **20**, a point-of-sales terminal **22** for merchant **20**, a website **24** for merchant **20**, and a first communications network **31** that enables the user's computer and the merchant's website to communicate with one another. The first communications network **31** may include the Internet, a telecommunications network (*e.g.*, a wireless network, cell phone network, a telephone network, a cable network, or any combination thereof), a wide area network (WAN), a local area network (LAN), a home router or gateway coupled to one of the above networks, or any combination of the above. Also shown in FIG. 1 is an acquiring bank **50** for the merchant, an issuing bank **60** for the portable consumer device **5**, a payment processing network **70**, and a second communications network **32** that enables the payment processing network **70** to communicate with each of the banks **50** and **60**. The second communications network **32** may comprise the Internet (and therefore may overlap and share facilities with the first communications network **31**), or may comprise one or more private networks, or combination of one or more private networks with the Internet. A private network may comprise a telecommunications network, a wide area network (WAN), a local area network (LAN), or any combination thereof. In some instances, the first and second communications networks **31** and **32** may be the same (such as a network using the Internet as the backbone). A communications network generally comprises a network of one or more communications links and two or more nodes that pass messages from one part of the network to another part. Each node comprises one or more pieces of electrical machinery, and each link may comprise one or more of the following: optical fibers, optical links, radio links, electrical wires. The components described so far are, for the most part, conventional and arranged in a conventional manner.

[0037] Also shown in FIG. 1 is a provision entity **80** and an SMS gateway **90**. SMS gateway **90** provides an interface between personal communications devices **7** and entities that are coupled to communications network **31** so that text messages can be conveyed between communication devices **7** and the entities coupled to network **31**. The entities coupled to network **31** include web sites and provision entity **80**. Provision entity **80** provides device verification values to user **1** by way of the user's personal communication device **7** under various conditions and/or circumstances, according to various embodiments of the invention as described below. For the sake of clarity, and without loss of generality, we can refer to the device verification value provided by provision entity **80** as a "dCVV2" value, so as to distinguish it from the dynamic "CVC3" and "dCVV" values generated by smartcards, from the printed CVV values on the backs of many credit cards, and from the CVV field found on a checkout page of a typical merchant website. The dCVV2 values may be conveyed to the user's personal communications device **7** by way of SMS gateway **90**, or by way of communications network **31**. In the former case, provision entity **80** may send dVCC2 values to SMS gateway **90** directly or via communications network **31**. In the latter case, personal communications device **7** may be network-capable and may have a network address that is accessible via communications network **31**. A network address for personal communications device **7** may comprise any one of: a uniform resource locator (URL), an Internet-protocol address (IP-address), an e-mail address, or any other type of identifier that can identify an entity on a communications network.

[0038] The dCVV2 values provided by provision entity **80** for a particular portable consumer device **5** vary with time in some manner. They therefore are dynamic, as opposed to the static nature of a printed CVV value on the back of a credit card. When conducting an in-store purchase, user **1** can provide a received dCVV2 value to the store clerk to be entered in at POS terminal **22** as the card verification value for the transaction. When conducting an on-line purchase, user **1** can enter a received dCVV2 value into the CVV field of the checkout page of merchant website **24**. According to various embodiments, the dCVV2 values provided to user **1** by provision entity **80** can be obtained from issuing bank **60** or payment processing network **70**, or can be generated by entity **80** and provided to issuing bank **60** and/or payment processing network **70**. In each of the configurations, user **1**, merchant **20**, and the entity that will

authorize the transaction, which may be payment processing network **70** and/or issuing bank **60**, know the particular dCVV2 value that is to be used for the transaction. Since the dCVV2 values vary with time, a fraudster who intercepts and tries to use a prior dCVV2 value can be thwarted. In this manner, the provision of varying dCVV2 values increases the confidence that the use of the portable consumer device is authentic, and not fraudulent *(e.g.*, not skimmed). The provision of varying dCVV2 values also maintains or improves existing user experiences, minimizes the impact on merchant processes and systems, leverages existing network data transport mechanisms, utilizes existing issuer validation infrastructure, and maintains consistency with broader authentication strategies.

[0039] Provision entity **80** can process requests from a plurality of different personal communication devices **7** (*e.g.*, millions of cell phones), and can process any number of requests by a particular personal communication device **7**. Provision entity **80** may apply one or more validation tests to the request to obtain a level of confidence that the request is not fraudulent before sending a datum indicative of a dCVV2 value to a requesting device **7**. Provision entity **80** comprises a system having one or more servers coupled to a communications network that can receive requests for device verification values. One of the servers of entity **80** is shown in FIG. 1; the server comprises one or more processors **81** electrically coupled to each of a tangible computer-readable medium **82**, a user interface **83**, one or more databases **86**, and a networking facility **84**, the latter of which is coupled to first and second communications networks **31** and **32**. User interface **83** comprises one or more video output devices (*e.g.*, displays, screens) and one or more input devices (*e.g.*, keyboard, mouse, trackball, *etc.*), which enable an administrator of entity **80** to receive information from the server and to provide input to the server. Computer-readable medium **82** may comprise a combination of semiconductor memory and non-volatile storage, such as one or more disk drives and/or non-volatile memory.

[0040] Computer-readable medium **82** stores an operating system for the server, which enables processes and applications to be run by processor(s) **81**, and enables codes for directing the operation of processor(s) **81** to be run. Computer-readable medium **82** also stores a plurality of codes that direct processor(s) **81** to perform various tasks to process requests for dCVV2 values and to provide datum indicative of dCVV2

values. The codes and tasks can vary among the various sets of embodiments described herein, and are described in greater detail below with the description of each set of embodiments. The operating system provides services to these processes, applications, and codes, and enables them to access components of user interface **83**, portions of computer-readable medium **82**, networking facility **84**, databases **86**, and other components of entity **80**. Specifically, the operating system provides one or more I/O communications modules that enable processor(s) **81** to communicate with user interface **83** and databases **86**. Each I/O communications module has an application programming interface (API) with a collection of functions that a processor **81** can call in order to access the components. The operating system of entity **80** also comprises one or more network services modules that can access networking facility **84** and set up communication sessions to entities on communications networks **31** and **32**, and with SMS gateway **90**. Such network services modules include Microsoft's Windows Communications Foundation (*e.g.*, .NET 3.0, .NET 4.0, *etc.*), Apple's CFNetwork Framework, the networking section of the Unix and Linux operating system kernels, and the OS Services Layer and the Base Services Layer of the Symbian operating system, and the like. Each of these network services modules is non-exclusive (*e.g.*, capable of serving more than one processor and more than one process/application) and provides an application programming interface (API), which has a collection of functions that a processor **81** can call in order to manage communications with another entity. With these API facilities, a collection of function calls can be readily constructed for a processor to execute that enables the processor to establish a communications channel with an entity on a communications network coupled to networking facility **84**, and to exchange messages and data with the entity. The above operating system, modules, and APIs all include instructions that direct the operation of processor(s) **81**.

[0041] One or more databases **86** may be configured as database servers, which processor(s) **81** can access via networking facility **84** over a private communications network **87**, which is illustrated by the dashed line in FIG. 1. Provision entity **80** conventionally has a clock **88** for tracking time and dates for various applications. Clock **88** may be a simple counter of seconds, or fractions thereof, that can be read by processor **81** by an I/O operation, or may comprise a more complex arrangement of hardware or firmware that can provide the various components of the current date and

time (year, month, day, hour, minute, and second) in various registers that can be read by processor **81** through the execution of one or more I/O operations.

[0042] In a first set of embodiments, user **1** creates a management account with provision entity **80**, or an associate thereof, such as issuing bank **60** or payment network **70**. In some configurations, provision entity **80** may be part of issuing bank **60** or part of payment processing network **70**. With the management account, the user can associate the consumer accounts (*e.g.*, account numbers and related information) of one or more corresponding portable consumer devices **5** with a mobile phone number and/or network address of personal communications device **7**. The account number of consumer account identifies the consumer account within at least one payment processing network, and may comprise a primary account number (PAN). The associations specified in the management account are stored as an account record in a database **86** of entity **80**. If the management account is set up with issuing bank **60** or payment processing network **70**, the association of the consumer accounts of one or more portable consumer devices **5** with a mobile phone number and/or network address provided in the management account is securely transmitted to provision entity **80** over communications network **32**, and is stored as an account record in a database **86** of entity **80**. This database **86** of account records enables provision entity **80** to find the consumer accounts (*e.g.*, account numbers and related information) of the user's portable consumer devices **5** based on the mobile phone number or network address of the user's personal communication device **7**.

[0043] An exemplary embodiment of an account record in the aforementioned database **86** is shown in FIG. 2. The exemplary account record is embodied on a computer-readable medium and comprises three data fields (shown as the top row of the record) to store a mobile phone number, a network address, and a unique identification code for user **1**. All three of these data fields are indexed and searchable. The data fields for the mobile phone number and network address are to store the mobile phone number (if available) and network address (if available) of the user's personal communications device **7**. At least one of these fields is filled. If device **7** does not have both a mobile phone number and a network address, then one of the fields is filled with a NULL indicator. The third data field holds a unique identification code that is uniquely assigned to the user by provision entity **80** (or an affiliated entity)

upon enrollment, such as during the creation of the user's management account. The next three rows in the account record shown in FIG. 2 hold data fields for three example consumer accounts for user **1**, which the user has associated with the mobile phone number and/or network address provided in the data fields of the first row. The first data field (*e.g.*, "Consumer Account A") holds information about the consumer account, such as the identity and contact information of the issuing bank, and such as the conditions of use of the account (*e.g,*, expiration date). The second data field (*e.g.*, "Account Number for Account A") holds the account number for the consumer account, such as a 16-digit number of a credit-card consumer account. The third data field (*e.g.*, "Code phrase for Account A") holds a code phrase (*e.g.*, a text string of alphanumeric characters) that user **1** provides to identify the consumer account without referring to the account number for the consumer account (the code phrase is different from the account number). The fourth data field stores an indication of which route the dCVV2 value is to be conveyed back to user **1** (Reply Route data field). This indication may be set to any of the following values: (1) the dCVV2 value is to be sent to the mobile phone number given in the account record, (2) the dCVV2 value is to be sent to the network address given in the account record, (3) the dCVV2 value is to be sent to both the mobile phone number and the network address given in the account record, (4) the dCVV2 value is to be sent back to the source of the request message, (5) the dCVV2 value is to be sent back to the opposite of the request message (*e.g.*, sent to mobile phone number if the request was sent from the network address). The fifth data field indicates the method to be used to obtain the dCVV2 value, and may include one or more actual dCVV2 values to use, or an algorithm and any associated parameters to use to generate dCVV2 values. The sixth data field holds various parameters for the consumer account, such as a status designation that indicates whether the account is the primary account, and which validation tests, if any, are to be applied to dCVV2 requests for the consumer account. The sixth data field can also hold indication of whether an e-mail will be sent the user's e-mail address under one or more of the following conditions: when a dCVV2 value is requested, when a dCVV2 value is sent, when a request for the dCVV2 value is denied.

[0044] To enable user **1** to set up a management account, provision entity **80** or an affiliated entity (*e.g.*, issuing bank or payment processing network) may comprise a

website accessible to the user **1** that enables the user: (1) to create a password-protected management account; (2) to associate an e-mail address with the management account to receive messages and alerts; (3) to associate a mobile number and/or URID (*e.g.*, network address) of the user's personal communications device **7** to be used to receive dCVV2 values; (4) to associate one or more consumer accounts and corresponding account numbers of the user's one or more corresponding portable consumer devices **5**; and (5) to associate a code phrase and reply route with each consumer account, and to activate the sending of an e-mail to the user's e-mail address when a dCVV2 value is requested and/or sent or denied, as indicated above. One of databases **86** may be assigned to hold the management accounts of the users. Code associated with the website can direct the processor of the entity to create an account record shown in FIG. 2 for the user by copying the data from the management account into the corresponding data fields of the account record, by assigning a unique identification code to the user and copying it to the corresponding data field of the account record, and by contacting the issuing bank for each consumer account to get the method for obtaining dCVV2 values for the consumer account and copying the method to the corresponding data field of the account record. Thereafter, when provision entity **80** receives a request for a dCVV2 value, it can query the database of account records for the user's account record using the mobile phone number or network address of the user's personal communications device **7**, and determine the consumer accounts of the portable consumer devices **5** that are associated with the user's personal communication device **7**. The above codes and actions can be implemented with HTML page codes, XML page codes, and the like (*e.g.*, web pages), conventional I/O instructions, memory access instructions, database function calls, CPU arithmetic instructions, CPU logic instructions, and CPU control instructions. In view of this disclosure, the codes may be implemented by one of ordinary skill in the software art without undue experimentation.

[0045] As one approach for requesting a dCCV2 value, when user **1** wishes to complete an on-line or in-store purchase, user **1** can send a request in the form of a text message from personal communication device **7** to a short mobile code (*e.g.*, 5 digit number) or long mobile code (*e.g.*, 10 digit number) associated with provision entity **80**. The body of the text message may be blank or may contain a code phrase for portable

consumer device **5** or a selected number of digits of the account number for portable consumer device **5** (*e.g.*, incomplete account number). The protocol of the text message, which is separate from the body of the text message and which typically includes the header of the text message, includes the mobile phone number of personal communications device **7**. The text message is received by an SMS gateway **90**, which may be operated by the service provider for communications device **7**. Looking at the received mobile code, SMS gateway **90** determines that the text message is to be forwarded to provision entity **80**, and forwards the text message to entity **80** via communications network **31** using a uniform resource identifier (URID) for entity **80**. (A URID may comprise a uniform resource locator (URL), an Internet-protocol address (IP-address), an e-mail address, or any other type of identifier or network address that can identify an entity on a communications network.) Prior to this, the short code, long code, and URID for entity **80** may be provided to SMS gateway **90**. SMS gateway **90** performs any needed conversion of the message format for the text message, and includes the mobile phone number in the body and/or protocol (*e.g.*, header) of the message going to entity **80**. SMS gateway **90** may encrypt the message with a key provided by provision entity **80**. The Short Message Peer-to-Peer protocol (SMPP) may be used to route the message from gateway **90** to provision entity **80** over communications network **31**, and methods of converting to and from the SMP and SMPP message formats are well known to the art. In addition, SMS gateway **90** and its routing operations are known to the art and are commercially available. In some implementations, SMS gateway **90** may be coupled to networking facility **84** of provision entity **80** with a direct connection, and may communicate with provision entity **80** without the need to use first communications network **31**.

[0046] As another communication approach, personal communications device **7** may be network-enabled, having its own network address, and may send the request message directly to provision entity **80** by way of communications network **31**. The message may be sent by any number of well known Internet protocols, such as User Datagram Protocol (UDP), Datagram Congestion Control Protocol (DCCP), Stream Control Transmission Protocol (SCTP), and Transmission Control Protocol (TCP), each of which includes the network address of device **7** in the message protocol (*e.g.*, the message header, or packet header).

[0047] The various actions occurring at provision entity **80** are illustrated in the method flow diagram **120** shown in FIG. 3. Once provision entity **80** receives the request message from SMS gateway **90** or from communication device **7** via network **31** (action **121** shown in FIG. 3), it obtains the mobile phone number or network address of communications device **7** from the protocol of the message (*e.g.*, message header) or the body of the message, and obtains a code phrase (if present) or any digits of the account number associated with portable consumer device **5** from the body of the message (if present), as illustrated in action **122** shown in FIG. 3. It then accesses, as illustrated by action **123** in FIG. 3, the database **86** of account records to locate and obtain an account record that contains the obtained mobile phone number, network address, or unique user identification code, the account record having one or more consumer accounts of portable consumer devices that have been associated with the obtained mobile phone number, network address, or user identification code, as described above. In one embodiment, this database **86** may store the account records of all the users **1** that can request dCVV2 values from provision entity **80**. As indicated above, each account record is indexed by mobile phone numbers, network addresses, and user identification codes, and can be located by phone number, network address, and user identification code (*e.g.*, the database is searchable based on these datum). Each account record also contains information pertaining to the method of how the dCVV2 values for each consumer account are to be obtained (*e.g.*, generated). In this manner, provision entity **80** can obtain all of the consumer accounts and account numbers of the portable consumer devices **5** that are associated with the mobile phone number or network address of personal communications device **7** that sent the request for the dCVV2 value, and information on how the dCVV2 values are to be obtained.

[0048] If a code phrase or an account number (or portion thereof) is present in the request message, provision entity **80** may be configured to find a match of this code phrase or account number (or portion thereof) to a code phrase or account number (or portion thereof) stored in the accessed and obtained account record. If no match is found, provision entity **80** may be configured to take no further action, or to send an error message in the form of a text message back to communications device **7** via SMS gateway **90** or communications network **31**. If a match is found, provision entity **80** can select the consumer account for which the match was found, and can then access the

data field that stores the dCCV2 method for the selected consumer account (action **124** shown in FIG. 3). If an account number, incomplete account number, and code phrase were not obtained from the request message, then provision entity **80** can examine the parameter data fields of the account record (shown in FIG. 2) to see if one of the consumer accounts is indicated as being the primary consumer account for the user. If so, provision entity **80** can select the primary consumer account and access its data field that stores the dCCV2 method for the account (action **124** shown in FIG. 3). As another option for the case when the dCVV2 request message does not contain an account number, incomplete account number, or code phrase, provision entity **80** may be configured to take no action or to send an error message in the form of a text message back to communications device **7**.

[0049] Provision entity **80** may then obtain a datum indicative of a dCVV2 value for the selected consumer account using information from the above-mentioned data field that stores the dCCV2 method for the selected consumer account (action **126** shown in FIG. 3). The obtained datum may be the dCVV2 value itself, an encoded form of the dCVV2 value, or an indication of a methodology to use to generate the dCVV2 value at the user's personal communication device **7**. Exemplary methods of obtaining datum of dCVV2 values are described below in greater detail.

[0050] To enhance security of the service, the full account number of the user's portable consumer device **5** is not transmitted to entity **80** in the request message. Instead, only the code phrase or a small portion of the account number (*e.g.*, an incomplete account number) of the user's portable consumer device **5** is transmitted. This prevents an eavesdropping fraudster from intercepting the complete account number and using the information in another financial channel. In this regard, the transmission of the mobile phone number or network address of device **5**, and the action of locating the consumer account in a secure database **86** of provision entity **80** as described above, is significantly more secure than the case of transmitting the complete account number.

[0051] The above-described finding of a match by provision entity **80** between the code phrase or account number (or portion thereof) obtained from the request message and a code phrase or account number stored in the obtained account record serves as

a first validation test that helps to ensure that the request for the dCVV2 value has not been spoofed by a fraudster. As a second validation test, provision entity **80** may check the mobile phone number or network address obtained from the received request message against one of its databases **86** that tracks mobile phone numbers and network addresses that have been used in fraudulent activities. If the obtained mobile phone number or network address is found in the database, provision entity **80** does not send the dCVV2 value. As a third validation test, provision entity **80** may check the matched consumer account against one of its databases **86** that tracks consumer accounts that have been used in fraudulent activities. If the matched consumer account is found in this database, provision entity **80** does not send the dCVV2 value.

[0052] As another security measure, the dCVV2 request message may include the user's unique identification code (which may comprise a number or alphanumeric name). The unique identification code is different from each of the account numbers (*e.g.*, PANs) of the user's portable consumer devices **5** and corresponding consumer accounts. As a fourth validation test, provision entity **80** may compare the identification code received in the request message against the unique identification code stored in the account record that entity **80** has for the user (which has been located by the mobile phone number or network address obtained from the request message). This validation test is passed if the received code matches the stored code, and failed if the two codes do not match. It may be appreciated that the account records in database **86** may be indexed by the unique identification codes so that provision entity **80** can find the consumer accounts of the user's devices **5** according to the identification code provided in the dVCC2 request message sent by the user. In this case, as a corresponding validation test, provision entity **80** may compare the mobile phone number or network address obtained from the request message to the mobile phone number or network address stored in the account record that entity **80** has for the user. This validation test is passed if the obtained phone number or network address code matches a phone number or network address stored in the account record.

[0053] As a fifth validation test for request messages sent via SMS messaging, provision entity **80** may obtain the network address (*e.g.*, IP-address) of the SMS gateway **90** that sent the dCVV2 request message, and compare the obtained network address to a list of trusted SMS gateways for a match. If a match is found, the

validation test is passed; otherwise the test is failed. The network address of SMS gateway **90** is provided in the protocol information, such as header information, in the request message sent from the SMS gateway.

[0054] Typically, one or more of the validation tests are preformed in accordance with the desired level of security, but it is not necessary to perform any or all of the tests. The optional performance of the validation tests is indicated at action **125** in FIG. 3, which can occur before or after the action of obtaining the dCVV2 datum. If a selected set of validation tests are passed, provision entity **80** may send the datum of the dCVV2 value in a response text message to the network address of personal communications device **7** and/or to the mobile phone number of device **7** via SMS gateway **90**, which may be determined by the data in the Reply Route data field of the account record (shown in FIG. 2) for the selected consumer account. This action is shown at **127** in FIG. 3. To thwart snooping by fraudsters, the datum of the response message may send the dCVV2 value in encoded form, such as with a selected number of dummy digits being added before and/or after the dCVV2 value, with user **1** being advised beforehand on which digits to select for the dCVV2 value (and which digits are the dummy digits). The datum may also comprise an indication of a methodology for user **1** to use to generate the dCVV2 value at the user's personal communication device **7**, such as indications of a row and column of a table of dCVV2 values for the user to look up. The dCVV2 request message from device **7** and the response message from entity **80** may be sent in the same communications route (*e.g.*, both routed as SMS messages through SMS gateway **90**, or both directly routed as network messages through communications network **31** using network addresses), or may be sent by different communication routes (*e.g.*, one message send via SMS gateway **90**, the other sent directly through communications network **31**). Finally, provision entity **80** may examine the parameter data field of the accessed account record to determine if there is any indication that one or more alerts are to be sent by e-mail to the user's e-mail account. If the parameters data field has an indication that an alert is to be sent if a request for a device verification value has been made, and such a request has in fact been made, provision entity **80** sends an alert message by e-mail to the user's e-mail account indicating the time and date that a request for device verification value has been made, and optionally providing an indication of the consumer account on which

the request was made. If the parameters data field has an indication that an alert is to be sent if a device verification value has been sent, and if the value has actually been sent, provision entity **80** sends an alert message by e-mail to the user's e-mail account indicating the time and date that a device verification value was sent, and optionally providing an indication of the consumer account for which the value was intended. If the parameters data field has an indication that an alert is to be sent if a request for a device verification value has been denied, and such a request has in fact been denied (such as for failing one or more validation tests), provision entity **80** sends an alert message by e-mail to the user's e-mail account indicating the time and date that a request for device verification value was made and/or denied, and optionally providing an indication of the consumer account on which the request was denied. If the user has elected that two or more of the above alerts be generated, the alerts may be combined into a single e-mail message.

[0055] To implement the above embodiments, computer-readable medium **82** may store an application **85** having the following codes embodied thereon. A first code directs processor(s) **81** to receive a request message from personal communication device **7** (via network **31**) and/or from SMS gateway **90** for a device verification value for a portable consumer device associated with a user, the request originating from personal communication device **7** associated with user **1** as described above. A second code directs processor(s) **81** to obtain and place in temporary memory storage the following data from the request message: the network address or phone number of the personal communication device **7** that originated the request message, the network address of the SMS gateway **90** that sent the request message if the request was sent via the SMS route, digits of an account number (if present) in the body or header of the message, a code phrase (if present) in the body or header of the message, and a user identification code (if present) in the body or header of the message. The first and second codes may comprise function calls to the network services module of the operating system and conventional I/O instructions to networking facility **84**, memory access instructions, CPU logic instructions, and CPU control instructions. A third code directs processor(s) **81** to obtain an account record of user **1** that contains the mobile phone number or network address obtained from the request message, the account record having one or more consumer accounts of portable consumer devices that have

been associated with the obtained network address or mobile phone number, as described above. The third code may comprise conventional I/O instructions or function calls to one of databases **86** that holds the account records (*e.g.*, a function call directly to the database or via networking facility **84**), memory access instructions, and CPU control instructions.

[0056] A fourth code of application **85** directs processor(s) **81** to select a consumer account from the obtained account record. This code may direct the data processor(s) **81** to compare the account number, incomplete account number, or code phrase obtained from the request message to the account number(s) and/or code phrase(s) stored in the account record to find a matching item. The data processor selects the consumer account with the matched item as the selected consumer account. If an account number, incomplete account number, and code phrase were not obtained from the request message, then the fourth code may direct data processor(s) **81** to examine the parameter data fields of the account record to see if one of the consumer accounts is indicated as being the primary consumer account for the user. If so, the code directs data processor(s) **81** to select the primary consumer account as the selected consumer account. The fourth code may comprise conventional memory access instructions, CPU logic instructions, and CPU control instructions.

[0057] A fifth code directs processor(s) **81** to obtain a datum indicative of a device verification value for the selected consumer account (*e.g.*, for the portable consumer device). In some implementations, the fifth code may include directing the processor(s) **81** to identify, from information in the obtained account record, the method to be used to obtain the datum of the dCVV2 value for the selected consumer account, and to execute the identified method. As indicated above, this information may be stored in the dCVV2 method data field for the selected consumer account, as shown in FIG. 2. This data field may contain parameters to be used in the method, and the fifth code may direct processor(s) **81** to read and use the parameters in the execution of the method. In other implementations, an application different from application **85** may pre-store one or more dCVV2 values in the dCVV2 method data fields of the consumer accounts, and the fifth code of application **85** may read the dCVV2 method data field for a dCVV2 value to use. This other application may update the dCVV2 values in these data fields according to a selected time schedule, and optionally in consultation with the

issuing banks, to keep the values dynamic. In yet other implementations, the fifth code may direct processor(s) **81** to execute a common method to generate the dCVV2 value, where the common method is applied to all account records handled by provision entity **80**, or to all of the account records for devices issued by a given issuing bank. The common method may include, as inputs, parameters specific to the user or the selected consumer account, as read from the obtained account record. The fifth code may further instruct data processor(s) **81** to send the obtained dCVV2 value to payment processing network **70** and/or issuing bank **60** (*e.g.*, an entity different from personal communications device **7**), along with an indication of the selected consumer account (*e.g.*, the account number). In view of this disclosure, the fifth code can be implemented with conventional I/O instructions, function calls to databases, memory access instructions, CPU arithmetic instructions, CPU logic instructions, and CPU control instructions. Aspects of various implementations of the fifth code are described below in greater detail.

[0058] A sixth code directs processor(s) **81** to send a fulfillment message having the datum of the dCVV2 value back to the network address or mobile phone number of device **7**, the latter being routed through SMS gateway **90**. For these actions, the processor can be directed to use the network address or mobile phone and URID (*e.g.*, the network address) of SMS gateway **90** that processor(s) **81** had previously stored under the direction of the first and second codes. In other implementations, the sixth code may direct processor(s) **81** to read the Reply Route data field for the selected consumer account (shown in FIG. 2) to determine which route(s) to use, and to then use network address and/or mobile phone number stored in the obtained account record. The sixth code may further direct processor(s) **81** to include in the fulfillment message a representation of the consumer account for which the dCVV2 value is being provided. The representation may comprise the incomplete account number or code phrase that was sent in the request message, or may include a different representation. The sixth code may comprise function calls to the network services module of the operating system and conventional I/O instructions to networking facility **84**, memory access instructions, CPU logic instructions, and CPU control instructions.

[0059] An optional seventh code directs processor(s) **81** to perform the above-described second validation test prior to the execution of one or both of the above-

described fifth and sixth codes. The seventh code directs the processor(s) to access one of databases **86** that tracks mobile phone numbers and network addresses that have been used in fraudulent activities to determine if the mobile phone number or network address provided in the request message is found in the accessed database. If it is found, the seventh code directs the processors(s) to not execute the sixth code, and optionally to not execute either or both of the fourth and fifth codes. The seventh code may comprise conventional I/O instructions or function calls to one of databases **86** (direct or via networking facility **84**), memory access instructions, CPU logic instructions, and CPU control instructions. An optional eighth code directs processor(s) **81** to perform the above-described third validation test prior to the execution of one or both of the above-described fifth and sixth codes. The eighth code directs the processor(s) to access one of databases **86** that tracks consumer accounts or account numbers that have been used in fraudulent activities to determine if the selected consumer account or its corresponding account number is found in the accessed database. If it is found, the eighth code directs the processors(s) to not execute the sixth code, and optionally to not execute the fifth code. An optional ninth code directs processor(s) **81** to perform the above-described fourth validation test prior to the execution of one or more of the above-described fourth, fifth, and sixth codes. The ninth code directs processor(s) **81** to compare the identification code received in the request message (as obtained and stored by the processor(s) under the direction of the first and second codes) against the unique identification code stored in the obtained account record. If the two identification codes are not equal, the ninth code directs processors(s) **81** to not execute the sixth code, and optionally to not execute the fourth code and/or fourth code. An optional tenth code directs processor(s) **81** to perform the above-described fifth validation test prior to the execution of one or more of the above-described fourth, fifth, and sixth codes. The tenth code directs processor(s) **81** to obtain from the received request message the network address of the SMS gate **90** that routed the request message to entity **80**, to access one of databases **86** that stores the network addresses of trusted SMS gateways **90** to determine if the network address of the SMS gate **90** that routed the request message to entity **80** is found in the accessed database. If it is not found, the tenth code directs the processors(s) to not execute the sixth code, and optionally to not execute the fourth code and/or fifth code. Each of the eighth, ninth, and tenth codes

may comprise conventional I/O instructions or function calls to one of databases **86** (direct or via networking facility **84**), memory access instructions, CPU logic instructions, and CPU control instructions.

[0060] An optional eleventh code directs processor(s) **81** to examine the parameter data field of the accessed account record to determine if there is any indication that one or more alerts are to be sent by e-mail to the user's e-mail account. If the parameters data field has an indication that an alert is to be sent if a request for a device verification value has been made, and such a request has in fact been made, the eleventh code directs processor(s) **81** to send an alert message by e-mail to the user's e-mail account indicating the time and date that a request for device verification value has been made, and optionally providing an indication of the consumer account on which the request was made. If the parameters data field has an indication that an alert is to be sent if a device verification value has been sent, and if the value has actually been sent, the eleventh code directs processor(s) **81** to send an alert message by e-mail to the user's e-mail account indicating the time and date that a device verification value was sent, and optionally providing an indication of the consumer account for which the value was intended. If the parameters data field has an indication that an alert is to be sent if a request for a device verification value has been denied, and such a request has in fact been denied (such as for failing one or more validation tests), the eleventh code directs processor(s) **81** to send an alert message by e-mail to the user's e-mail account indicating the time and date that a request for device verification value was made and/or denied, and optionally providing an indication of the consumer account on which the request was denied. If the user has elected that two or more of the above alerts be generated, the eleventh code may further direct processor(s) **81** to combine alerts into a single e-mail message. The eleventh code may comprise conventional I/O instructions or function calls to one of databases **86** (direct or via networking facility **84**), memory access instructions, CPU logic instructions, and CPU control instructions.

[0061] In view of this disclosure, the above codes of provision entity **80** may be implemented by one of ordinary skill in the software art without undue experimentation.

[0062] Various exemplary methods of obtaining datum of dCVV2 values that can be executed by provision entity **80** with the above-described fifth code are now described.

In a first implementation, the issuing bank **60** for the portable consumer device **5** may provide provision entity **80** with a list of datums indicative of dCVV2 values that are to be used, and one or more conditions under which the listed datums are to be given out. For example, a condition may specify that the listed datums are to be given out as follows: (1) one listed datum per request (per transaction), (2) one listed datum per group of N requests (N transactions), or (3) one listed datum for all requests (transactions) occurring within a selected time period (such as 12 hours, 1 day, two days, three days, *etc*). Provision entity **80** may store the listed datums and condition(s) in the dCVV2 method data field of the user's account record (shown in FIG. 2), or may store the listed datums and condition(s) in an auxiliary record located in another one of databases **86** along with an indication of the consumer account. The auxiliary record and the user's account record (shown in FIG. 2) may be linked to one another. Provision entity **80** may be configured to request additional listed datums when needed, or the issuing bank may periodically send listed datums. The listed datums may comprise the actual dCVV2 values, or information that can be used to generate dCVV2 values at the communication device **7**. When provision entity **80** receives a request for a dCVV2 value, it obtains a user account record and selects a consumer account of a portable consumer device **5** as described above, and thereafter locates the listed datum and condition(s) from the user account record (e.g., dCVV2 method data field) or the auxiliary record. In this manner, provision entity **80** may obtain the datum of the dCVV2 value to be sent. In further implementations, the issuing bank **60** may provide provision entity **80** with the actual dCVV2 values, and provision **80** may generate the datum as an encoding of the actual dCVV2 value, which may be done by an algorithm determined by the issuing bank or provisioning entity **80**. For these tasks related to obtaining datum of dCVV2 values, provision entity **80** may comprise code embodied on computer-readable medium **82** that directs data processor **81** to communicate with the issuing bank to receive the listed datum and condition(s), to store the listed datum and condition(s) in the user account record or the auxiliary record (both of which includes a computer-readable medium), and to look up the listed datum and condition(s) in response to receiving a request for a dCVV2 value (including identifying and selecting the consumer account from the request). The above codes can be implemented with conventional I/O instructions, memory access instructions, database function calls, networking function

calls, CPU arithmetic instructions, CPU logic instructions, and CPU control instructions. In view of this disclosure, the codes may be implemented by one of ordinary skill in the software art without undue experimentation.

[0063] In a second implementation of obtaining the datum of dCVV2 values that can be executed by provision entity **80**, the issuing bank **60** for the portable consumer device **5** may provide provision entity **80** with an algorithm or indication thereof for generating the datums indicative of dCVV2 values that are to be used. The algorithm provides a new datum for each request (transaction), a new datum for each group of N requests (N transactions), or a new datum for all requests (transactions) occurring within a selected time period (such as 12 hours, 1 day, two days, three days, *etc*). Provision entity **80** may store the algorithm (or indication thereof) and any associated parameters in the dCVV2 method data field of the user's account record (shown in FIG. 2), or may store the algorithm (or indication thereof) and associated parameters in an auxiliary record located in another one of databases **86** along with an indication of the consumer account. The auxiliary record and the user's account record (shown in FIG. 2) may be linked to one another. Since many issuing banks will use the same algorithm for its card holders (but use different parameters), it is more memory efficient to store the algorithm once in one of databases **86**, and to store indications of the algorithm (such as in the form of a record pointer) in the user's account record (shown in FIG. 2) or auxiliary record, along with individualized parameters. However, the algorithm can be stored as a script or a method data object in the dCVV2 method data field of the user's account record. When provision entity **80** receives a request for a dCVV2 value, it obtains a user account record and selects a consumer account of a portable consumer device **5** as described above, and thereafter locates the stored algorithm or algorithm indication, and any associated parameters, from the user account record (*e.g.*, dCVV2 method data field) or the auxiliary record, and executes the located algorithm. In this manner, provision entity **80** may obtain the datum of the dCVV2 value to be sent. The algorithm may include generating the actual dCVV2 value and/or encoding the dCVV2 value. For these tasks related to obtaining datum of dCVV2 values, provision entity **80** may comprise code embodied on computer-readable medium **82** that directs data processor **81** to communicate with the issuing bank to receive the algorithm (or indication thereof) and any associated parameters, to store the

algorithm (or indication thereof) and any associated parameters in an account record or auxiliary record of database **86** (which includes a computer-readable medium), and to look up the algorithm in response to receiving a request for a dCVV2 value (including identifying the consumer account number from the request). The above codes can be implemented with conventional I/O instructions, memory access instructions, database function calls, networking function calls, CPU arithmetic instructions, CPU logic instructions, and CPU control instructions. In view of this disclosure, the codes may be implemented by one of ordinary skill in the software art without undue experimentation.

[0064] In a third implementation of obtaining datum of dCVV2 values that can be executed by provision entity **80**, provision entity **80** may generate the datum values by determining the identity of the issuing bank from the selected consumer account, sending an electronic message to the issuing bank through a secure channel to request a dCVV2 datum for use, receiving a dCVV2 datum from the issuing bank through a secure channel, and sending the received dCVV2 datum to personal communications device **7**, and optionally sending the received dCVV2 datum to payment processing network **70**. For this implementation, provision entity **80** may comprise code embodied on computer-readable medium **82** that directs data processor **81** to determine the identity of the issuing bank from the selected consumer account, to send an electronic message to the issuing bank (preferably through a secure channel) to request a dCVV2 datum for use, to receive a dCVV2 datum from the issuing bank (preferably through a secure channel), and to send the received dCVV2 datum to personal communications device **7**, and optionally to payment processing network **70**. The above codes can be implemented with conventional I/O instructions, memory access instructions, database function calls, networking function calls, CPU arithmetic instructions, CPU logic instructions, and CPU control instructions. In view of this disclosure, the codes may be implemented by one of ordinary skill in the art without undue experimentation.

[0065] In a fourth implementation of obtaining datum of dCVV2 values that can be executed by provision entity **80**, provision entity **80** may generate the datum values by any process, and send the generated datum to both personal communications device **7** and the authorizing entities for the transaction, which may be one or both of payment processing network **70** and issuing bank **60**. The process may be specific to a particular portable consumer device **5**, specific to a particular user **1** (*e.g.*, all of the

user's devices **5**), specific to a group of users, specific to a group of devices (such as devices issued by a particular bank **60**), or general to all devices **5**. An exemplary process may include the user of a pseudorandom number generator. For this implementation, provision entity **80** may comprise code embodied on computer-readable medium **82** that directs data processor **81** to generate the datum for the dCVV2 value in response to a request according to the selected process, and to communicate the datum to personal communication device **7** and payment processing network **70** and/or issuing bank **60**. The code may include code that directs data processor **81** to determine the identity of the issuing bank from the selected consumer account (as determined from the obtained account record), and to send an electronic message to the issuing bank (preferably through a secure channel) with an indication of the device verification value and the selected consumer account. The above codes can be implemented with conventional I/O instructions, memory access instructions, database function calls, networking function calls, CPU arithmetic instructions, CPU logic instructions, and CPU control instructions. In view of this disclosure, the codes may be implemented by one of ordinary skill in the art without undue experimentation.

[0066] A second set of embodiments is similar to the above-described first set of embodiments, except that a code application is provided on personal communications device **7** to send requests for dCVV2 values to provision entity **80**. As an example, device **7** may comprise an Apple™ iPhone™, and the code application may comprise a third-party iPhone™ application offered or provided to user **1** by the operator of provision entity **80** or issuing bank **60**. FIG. 4 illustrates a generic personal communications device **200** that may be used for these embodiments with an exemplary code application **205**. Device **200** comprises a processor **201**, a computer-readable medium **202** that stores data, an operating system (which may be relatively minimal), and instructions that direct the operation of processor **201**, a telecommunication facility **203** that communicates with a telecommunication network (such as through a cell tower), an antenna **204** coupled to telecommunications facility **203**, and a user interface **206** that has a touch screen display **207**, speaker **SPK**, and microphone **MIC**. As an option, personal communications device **200** may also comprise a networking facility **210** capable of communicating with a wireless router or gateway that is coupled to the Internet (*e.g.*, WiFi station), and an antenna **211** coupled

to networking facility **210**. Processor **201** is electrically coupled to computer-readable medium **202**, user interface **206**, telecommunications facility **203**, and networking facility **210**. Finally, personal communications device **200** conventionally has a clock **212** for tracking time and dates for various applications. Clock **212** may be a simple counter of seconds, or fractions thereof, that can be read by processor **201** by an I/O operation, or may comprise a more complex arrangement of hardware or firmware that can provide the various components of the current date and time (year, month, day, hour, minute, and second) in various registers that can be read by processor **201** using one or more I/O operations.

[0067] Application **205** can be stored on computer-readable medium **202**. Application **205** directs processor **201** to present a graphical-user interface (GUI) button **208** with a suitable image or text that the user can associate with requesting dCVV2 values. In response to GUI button **208** being activated, application **205** directs processor **201** to send a text message to provision entity **80** to request a dCVV2 value. The short or long message code for provision entity **80** may be stored in the code of application **205** (and in turn may be stored in medium **202**). As indicated above, the text message need not provide an account number or code phrase of a portable consumer device **5**. However, application **205** may be further configured to provide a configuration screen to user **1** to receive one or more account numbers (or portions thereof, such as the last 3-5 digits) of the user's portable consumer devices **5** and/or a code phrase that the user has created and entered into his or her management account, and to thereafter store the account numbers (or portions thereof) and/or code phrases in computer-readable medium **202** of personal communications device **200**. The configuration screen may also prompt user **1** to enter the unique identification code that was assigned to the user during the creation of the user's management account, as described above, to read the entered code, and to store the entered code in computer-readable medium **202**. The configuration screen may be activated upon first use of application **205**, as well as upon a double activation of GUI button **208** (*e.g.*, two taps of the button in rapid succession, similar to a "double click" on a computer mouse). When multiple account numbers (or portions thereof) and/or code phrases are stored by application **205**, application **205** may present a selection screen to the user in response to a single tap of the button, where the selection screen presents selection buttons next

to representations of the stored account numbers (or portions thereof) and/or code phrases. In response to the user tapping one of these selection buttons, application **205** directs processor **201** of device **200** to send a text message to provision entity **80** that contains the selected account number (or portion thereof, *i.e.*, an incomplete account number) or the selected code phrase, and optionally the user's unique identification code. Application **205** may then leave it to user **1** to wait for a text message from provision entity **80** providing the datum of the dCVV2 value, and to determine (*e.g.*, read, decode, *etc.*) the dCVV2 value from the text message. As an option, application **205** may further direct processor **201** to scan the SMS inbox of communications device **200** for SMS messages from provision entity **80**, and delete such messages that have been in the SMS inbox for more than a selected period of time. The SMS inbox may be stored as a data structure in computer-readable medium **202**.

[0068] Computer-readable medium **202** also stores an operating system for the server, which enables processes and applications, such as application **205**, to be executed by processor **201**. The operating system provides services to these processes and applications, and enables them to access components of telecommunications facility **203**, networking facility **210**, user interface **206**, clock **212**, and portions of computer-readable medium **202**. Specifically, the operating system provides an I/O communications module that enables processor **201** to communicate with user interface **206** and portions of computer-readable medium **202** (such as those used by application programs). The I/O communications module has an application programming interface (API) with a collection of functions that processor **201** can call in order to access the components. The operating system also comprises a telecommunications service module that enables processor **201** to access telecommunications facility **203**, to send and receive SMS messages, to store messages in an organized manner (*e.g.*, inbox and send box), to search stored messages, to access stored messages, and to delete stored messages. The telecommunications service module has an application programming interface (API) with a collection of functions that a processor **201** can call in order to perform the above tasks. With the above API facilities, a collection of API function calls and other instructions can be readily constructed for processor **201** to execute to carry out the

above actions of application **205**. The operating system also comprises one or more network services modules that can access networking facility **210** and set up communication sessions to entities on communications networks **31**. Such network services modules include Microsoft's Windows Communications Foundation (*e.g.*, .NET 3.0, .NET 4.0, *etc.*), Apple's CFNetwork Framework, and the OS Services Layer and the Base Services Layer of the Symbian operating system, and the like. Each of these network services modules is non-exclusive (*e.g.*, capable of serving more than one process/application) and provides an application programming interface (API), which has a collection of functions that a processor **201** can call in order to manage communications with another entity. The above operating system, modules, and APIs all include instructions that direct the operation of processor **201**.

[0069] An exemplary embodiment of application **205** may comprise the following codes stored in computer-readable medium **202**. A first code directs processor **201** to present (GUI) button **208** on touch screen display **207** of user interface **206**. This code may comprise a graphical icon and identifier therefor that are provided to operating system when application **205** is installed on the operating system, with a direction that the icon be loaded onto the "desktop" or equivalent thereof of the user interface **206** (and as shown on touch screen **207**). When user **1** taps or clicks on the icon, the operating system starts and executes application **205**. A second code of application **205** may be executed immediately upon the operating system starting application **205**, or a short duration thereafter to allow the execution of a third code (as explained below). The second code may direct data processor **201** to send an SMS text message to provision entity **80** to request a dCVV2 value, such as by directing the networking facility to do so. The mobile code for entity **80** may be embedded in the second code, or may be stored in a segment of computer-readable medium **202** and accessed by processor **201** under the direction of the second code. The second code may comprise one or more function calls to the API of the telecommunications services module to send an SMS text message, wherein the telecommunication services module may include the mobile phone number of communications device **200** in the protocol (*e.g.*, header) of the SMS text message. The mobile phone number of device **200** may be stored in computer-readable memory **202**, which may have both volatile and non-volatile memory components, with the mobile phone number being stored in the non-

volatile component. The second code may further direct data processor **201** to access a segment of computer-readable medium **202** for stored code phrases and/or account numbers, or portions thereof, and for the user's unique identification code (if stored), before sending the SMS text message. If only one stored code phrase or account number is found, the second code may further direct data processor **201** to include the code phrase or account number (or portion thereof) in the SMS text message that is sent to provision entity **80**. The second code may also direct processor **201** to include the user's unique identification code in the SMS text message. If two or more stored code phrases and/or account numbers are found, the second code may include instructions that direct data processor **201** to present a selection screen to the user on touch screen **207** that displays representations of the stored code phrases and/or account numbers (or portions thereof) along with corresponding selection buttons, and to obtain a selection of an consumer account from user **1**. The representations may be the actual code phrases and/or account numbers (or portions thereof), or text or graphical icons for the corresponding consumer accounts provided by the user or an issuing bank **60** that provided application **205** to the user. The representations may be stored in computer-readable medium **202** along with the code phrases and/or account numbers in a linked manner. In some embodiments, application **205** may be downloaded from an issuing bank **60** for user **1**, and may be personalized by the issuing bank before or during downloading to include the code phrases and/or account numbers of the consumer accounts of user **1** and representations of the consumer account so that the user does not need to provide this information to application **205**. The representations may also serve as the selection buttons, or may be displayed within the selection buttons. After processor **201** receives a selection of a consumer account from user 1, the second code directs processor **201** to include the code phrase or account number (or portion thereof) of the selected consumer account in the SMS text message that is sent to provision entity **80**. The second code may also direct processor **201** to include the user's unique identification code in the SMS text message. For these tasks, the second code may comprise API function calls to the I/O communications module and telecommunication services module of the operating system, memory access instructions, CPU logic instructions, and CPU control instructions. In view of this

disclosure, the above codes may be implemented by one of ordinary skill in the software art without undue experimentation.

[0070] The exemplary embodiment of application **205** may further comprise, as an option, a third code that is executed before the second code is executed. The third code directs data processor **201** to monitor touch screen **207** to detect a second tap within a selected time of the start of the application. If such a second tap is detected, the third code directs data process **201** to present a configuration screen that receives input from user **1** to provide one or more code phrases and/or account numbers (or portions thereof), and optionally the user's unique identification code. The configuration screen may include a numeric key pad of the Arabic numbers 0-9, and optionally alphabetic letter keys A-Z, for the user to tap in the input, areas to display the inputted codes and/or numbers, a "back" key to delete the last entered number or letter, an "enter" key to enter the code and/or account number (or portion thereof) into storage, and a "cancel" key to allow the user to exit the configuration screen. For these tasks, the third code may comprise API function calls to the I/O communications module of the operating system, memory access instructions, CPU logic instructions, and CPU control instructions. In view of this disclosure, the above codes may be implemented by one of ordinary skill in the software art without undue experimentation.

[0071] As another possible option, provision entity **80** may be configured to send an SMS text message to personal communications device **200** when the management account of user **1** is created or updated to include or change the account numbers, code phrases, and unique user identification code that are associated with the mobile phone number of device **200**. The exemplary embodiment of application **205** may further comprise a fourth code that directs processor **201** to check the SMS text inbox of device **200** for such messages, to update the consumer account information stored in computer-readable medium **202** when such a message is found, and to delete the message after updating the consumer account information. Such messages can be located by examining the protocol information of the message for the mobile number of entity **80**, and/or further by a particular sequence of text characters placed in a selected location of the message or message header. Processor **201** may be directed to check the SMS text inbox upon the starting of application **205** before the second code is executed, or periodically. For these tasks, the fourth code may comprise API function

calls to the telecommunication services module of the operating system, memory access instructions, CPU logic instructions, and CPU control instructions. In view of this disclosure, the above codes may be implemented by one of ordinary skill in the software art without undue experimentation.

[0072] The exemplary embodiment of application **205** may further comprise, as an option, a fifth code that directs processor **201** to scan the SMS text inbox of device **200** for dCVV2 fulfillment messages from provision entity **80**, and to delete each such message from the inbox except when it is the most recently received SMS text message in the inbox received from provision entity **80**. Such messages can be located by examining the protocol information of the message for the mobile number of entity **80**, and/or further by a particular sequence of text characters placed in a selected location of the message or message header. Processor **201** may be directed to check the SMS text inbox upon the starting of application **205** before the second code is executed, or periodically. For these tasks, the fourth code may comprise API function calls to the telecommunication services module of the operating system, memory access instructions, CPU logic instructions, and CPU control instructions. In view of this disclosure, the above codes may be implemented by one of ordinary skill in the software art without undue experimentation.

[0073] The above second through fifth codes may be executed upon application **205** being executed by the operating system, at which point application **205** may terminate. User **1** may then check the SMS text message inbox for a message from entity **80** that provides a datum indicative of the dCVV2 value. As another option, the exemplary embodiment of application **205** may further comprise a sixth code that directs processor **201** to scan the SMS text inbox of device **200** for the most recent dCVV2 fulfillment message from provision entity **80** received after the execution of the second code, to obtain the dCVV2 value from the message, and to display dCVV2 value on touch screen **207** of user interface **206** for the user. As an option, provision entity **80** may include a representation of the consumer account for which the dCVV2 value is being provided, and the sixth code may direct processor **201** to obtain this representation from the SMS text message, and to display it on touch screen **207** along with the dCVV2 value. The representation may comprise an incomplete account number or a code phrase. The sixth code can include instructions that perform simple

to very complex decoding of the dCVV2 datum to obtain the dCVV2 value, thereby enabling entity **80** to send dCVV2 values with a higher degree of security. These instructions can include decrypting instructions using a decryption key stored in computer-readable medium **202**. For the above tasks, the sixth code may comprise API function calls to the I/O communication module and telecommunication services module of the operating system, memory access instructions, CPU arithmetic instructions, CPU logic instructions, and CPU control instructions. In view of this disclosure, the above codes may be implemented by one of ordinary skill in the software art without undue experimentation.

[0074] In the above second set of embodiments, communications between provision entity **80** and personal communication devices **7** and **200** are performed with SMS messaging. In a third set of embodiments, some or all of this communication may be performed by simple packet messaging between entity **80** and devices **7**, **200** routed via communications network **31** (*e.g.*, using the Internet). For example, a modified version **205'** of application **205** may send a dCVV2 request to provision entity **80** in a network message sent from networking facility **210** that is addressed to a universal resource identifier (URID) for entity **80**. A uniform resource identifier (URID) may comprise a uniform resource locator (URL), an Internet-protocol address (IP-address), an e-mail address, or any other type of identifier or network address that can identify an entity on a communications network. The network message may be sent by any number of well-known messaging protocols, such as User Datagram Protocol (UDP), Datagram Congestion Control Protocol (DCCP), Stream Control Transmission Protocol (SCTP), Transmission Control Protocol (TCP). The network message can include one or more of the following: the mobile phone number of device **200**, an account number or incomplete account number for a consumer account of a portable consumer device **5**, a code phrase for a consumer account of a portable consumer device **5**, the user's unique identification code, each of which may be encoded or encrypted. The protocol used to send the network message includes a URID (*e.g.*, a network address) of device **200**, which may be used by provision entity **80** to access and obtain an account record for the user, as described above. Provision entity **80** may send back a dCVV2 datum to device **200** by way of an SMS message, as described above. Instead of, or in addition to, provision entity **80** may send back a dCVV2 datum by way of a network

message addressed to a URID (*e.g.*, a network address) of device **200**, with the message being routed via communications network **31** and received by networking facility **210** of device **200**.

[0075] To implement the third set of embodiments, device **200** may comprise a modified version **205'** of application **205**. Application **205'** may comprise the above-described first code of application **205** that directs processor **201** to present (GUI) button **208** on touch screen display **207** of user interface **206**. Application **205'** may comprise a modified version of the above described second code of application **205**. The modified second code may direct data processor **201** to send a network message to provision entity **80** to request a dCVV2 value. The URID for entity **80** may be embedded in the modified second code, or may be stored in a segment of computer-readable medium **202** and accessed by processor **201** under the direction of the modified second code. The modified second code may comprise one or more function calls to the API of the network services module to send a network message, wherein the network services module may include a URID (*e.g.*, the network address) of communications device **200** in the protocol of the network message. The modified second code may further direct data processor **201** to access one or more segments of computer-readable medium **202** for the mobile phone number and/or the unique identification code for user **1**, before sending the network message. The modified second code may further direct data processor **201** to access a segment of computer-readable medium **202** for stored code phrases and/or account numbers, or portions thereof, before sending the network message. If only one stored code phrase or account number is found, the modified second code may further direct data processor **201** to include the code phrase or account number (or portion thereof) in the network message that is sent to provision entity **80**. If two or more stored code phrases and/or account numbers are found, the modified second code may include instructions that direct data processor **201** to present the above-described selection screen to the user on touch screen **207** that displays representations of the stored consumer accounts along with corresponding selection buttons, and to obtain a selection of an consumer account from user **1**, as described above. For these tasks, the modified second code may comprise API function calls to the I/O communications module and network services module of the operating system, memory access instructions, CPU

logic instructions, and CPU control instructions. In view of this disclosure, the above codes may be implemented by one of ordinary skill in the art without undue experimentation.

[0076] The modified version **205'** of application **205** may comprise the third, forth, fifth, and sixth codes of application **205**, and may accordingly receive update messages and dCVV2 fulfillment messages in the form of SMS messages. In some implementations, the fifth code may be omitted in the modified version **205'**, and a modified version of the sixth code may be used. The modified sixth code directs processor **201** to receive a network message (*e.g.*, dCVV2 fulfillment message) from provision entity **80** after the execution of the modified second code, to obtain the dCVV2 value from the so-received message, and to display the dCVV2 value on touch screen **207** of user interface **206** for the user. The modified sixth code can include instructions that perform simple to very complex decoding of the dCVV2 datum to obtain the dCVV2 value, thereby enabling entity **80** to send dCVV2 values with a higher degree of security. These instructions can include decrypting instructions using a decryption key stored in computer-readable medium **202**. For the above tasks, the modified sixth code may comprise API function calls to the I/O communication module and network services module of the operating system, memory access instructions, CPU logic instructions, and CPU control instructions. In view of this disclosure, the above codes may be implemented by one of ordinary skill in the software art without undue experimentation.

[0077] In the above set of embodiments, provision entity **80** may be further configured to send a time datum with the dCVV2 datum, where the time datum provides an indication of how long a period of time the dCVV2 datum is valid. The time datum may provide this indication in the form of an absolute point in time that is to be detected using a clock of device **200**, with the presumption that the clocks of entity **80** and device **200** are sufficiently synchronized, or in the form of a relative period of time measured against the time that the fulfillment message is received in device **200**. The above described fourth code of provision entity **80** may be modified to include instructions to generate the time datum based on information in the account record for the user and the value of its clock **88**. The modifications to the code can be implemented with conventional I/O instructions, memory access instructions, CPU arithmetic instructions, CPU logic instructions, and CPU control instructions. In view of

this disclosure, the above modified codes may be implemented by one of ordinary skill in the software art without undue experimentation.

[0078] Each of applications **205** and **205'** may have their second codes modified to include instructions that first check computer-readable medium **202** for an indication of the last received dCVV2 value and the associated time datum to determine if a request to provision entity **80** needs to be sent. (The indication may comprise the last received text message from provision entity **80** in the user's text inbox.) If the time datum indicates that the last received dCVV2 datum is still good, as compared to the time indicated by clock **212**, applications **205** and **205'** may simply display the dCVV2 value indicated by the last received dCVV2 datum. For this, the additional instructions of the modified second code of each application may include: (1) memory access instructions that direct the data processor to retrieve from computer-readable memory **202** the indication of the last received dCVV2 datum, associated time datum, and optionally the receipt time; (2) I/O instructions that direct the data processor to obtain the current time and date from clock **212**; (3) CPU arithmetic and logic instructions that direct the data processor to determine if the last received dCVV2 datum is still good (valid) from the current time and date, the time datum, and optionally the receipt time of the last dCVV2 datum by device **200** (the receipt time may be used in some cases where the time period is measured from the receipt time); and (4) CPU control instructions that direct the data processor to proceed normally with the remainder of the second code (which sends the request to entity **80**) if the last dCVV2 datum is no longer valid, or to bypass the remainder of the second code and to jump to the above-described fifth or sixth codes (which display the dCVV2 value from the last received dCVV2 datum) if the last dCVV2 datum is valid. If the second code is executed to obtain a new dCVV2 datum and associated time datum, indications of these newly-obtained datum (and optionally time of receipt) are stored in computer-readable memory **202** for use the next time application **205** or **205'** is called. In view of this disclosure, the above instructions and modifications may be implemented by one of ordinary skill in the software art without undue experimentation.

[0079] As further variations of the above embodiments that use time datum, it may be appreciated that the time of receipt of a message from entity **80** having a dCVV2 datum can effectively serve as the time datum, and that entity **80** does not need to send the

time datum. In these embodiments, applications **205** and **205'** and entity **80** may have a shared understanding of how long a dCVV2 value is valid from the time of its receipt. The validity period for the dCVV2 value may be a given amount of time as measured from the receipt time (*e.g.*, relative time period), such as three days from the receipt time. The validity period may also be for certain days of the week as determined by the receipt time (*e.g.*, absolute time period). As an example of the latter, the days of the month may be divided into groups of five consecutive days, such as days 1-5, 6-10, 11-15, *etc.* A dCVV2 datum received during a particular group of days would be valid for the days of that group (for example, a dCVV2 value received on day 12 of a month would be valid for days 11-15). Provision entity **80** may send a message with a dCVV2 datum as described above, but without a time datum. The shared understanding may be embodied in a time-period algorithm that can be embodied in each of codes **85**, **205**, and **205'** as one or more instructions, embodied on a computer-readable medium, that direct a processor to determine if the validity period has expired from the current time and the receipt time.

[0080] For this embodiment, each of applications **205** and **205'** may have their second codes modified to include instructions that first check computer-readable medium **202** for an indication of the last received dCVV2 datum and the associated receipt time to determine if a request to provision entity **80** needs to be sent. (The indication may comprise the last received text message from provision entity **80** in the user's text inbox, which includes a receipt time.) If the receipt time indicates that the last received dCVV2 datum is still good, as determined by the time indicated by clock **212** and the time-period algorithm, applications **205** and **205'** may simply display the dCVV2 value indicated by the last received dCVV2 datum. For this, the additional instructions of the modified second code of each application may include: (1) memory access instructions that direct the data processor to retrieve from computer-readable memory **202** the indication of the last received dCVV2 datum and associated receipt time, (2) I/O instructions that direct the data processor to obtain the current time and date from clock **212**; (3) CPU arithmetic and logic instructions that implement the time-period algorithm and that direct the data processor to determine if the last received dCVV2 datum is still good (valid) from the following: the current time and date, the receipt time, and the time-period algorithm; and (4) CPU control instructions that direct the data

processor to proceed normally with the remainder of the second code (which sends the request to entity **80**) if the last dCVV2 datum is no longer valid, or to bypass the remainder of the second code and to jump to the above-described fifth or sixth codes (which display the dCVV2 value from the last received dCVV2 datum) if the last dCVV2 datum is valid. If the second code is executed to obtain a new dCVV2 datum, indications of newly-obtained dCVV2 datum and associated receipt time are stored in computer-readable memory **202** for use the next time application **205** or **205'** is called. In view of this disclosure, the above instructions and modifications may be implemented by one of ordinary skill in the software art without undue experimentation.

[0081] Each of the above-described embodiments for provision entity **80** may be modified so that it unilaterally sends a dCVV2 datum (and optionally a time datum) without receiving a request from device **200**. For example, provision entity **80** may periodically or intermittently send a dCVV2 datum and optionally a time datum to device **200**. The above-modified versions of Applications **200** and **205'** may be used in this implementation of entity **80** without further modification, or the applications may be further modified to omit the instructions pertaining to sending requests for dVCC2 datums. In this modified embodiment, provision entity **80** may comprise a first code that scans through the account records and generates dCVV2 datums and optionally associated time datums (using instructions described above) according to one or more selected time intervals, and a second code that sends the dCVV2 datums and optionally time datums to the personal communication devices **7** of the users (using instructions described above). As a further modification, provision entity **80** may send the dCVV2 datum (and optionally the time datum) along with a normal transaction notification message.

[0082] FIG. 5 illustrates a general exemplary embodiment **130** of a method of providing dCVV2 datums that may be implemented by provision entity **80**. Exemplary method **130** comprises a plurality of actions **131**-**133**. Action **131**, which is optional in some implementations, comprises receiving, at a server, a request for a device verification value for a portable consumer device **5** associated with a user **1**. Action **132** comprises obtaining, at the server, datum indicative of a device verification value (dCVV2 value) for the portable consumer device **5** associated with the user **1**. Various implementations of obtaining the datum have been described above. Action **133**

comprises sending, from the server, a datum indicative of the device verification value (dCVV2 value) to a personal communication device associated with the user. Various implementations of sending the datum have been described above. Action **133** may include sending a time datum that is indicative of a time period over which the dVCC2 value in the dVCC2 datum is valid. If action **131** is not employed, actions **132** and **133** may be performed unilaterally by the server, or in response to forwarding information about a transaction.

[0083] FIG. 6 illustrates a general exemplary embodiment **140** of a method of obtaining and using a dCVV2 datum. Exemplary method **140** comprises a plurality of actions **141-143**. Action **141** comprises transmitting, from a personal communication device of a user, a request for a device verification value for a portable consumer device associated with the user. Action **142** comprises obtaining, at a personal communication device, an indication of a device verification value for a portable consumer device. Action **143** comprises providing the device verification value as information in a financial transaction. In one implementation, action **141** may comprise sending, using a portable communication device, a message to a provision entity requesting a device verification value for a consumer account, the consumer account having an account number that identifies the consumer account within a payment processing network, the message comprising at least one of a code phrase or identification code that is different from said account number. The message may further comprise a phone number or network address of a personal communication device. The unique identification code may uniquely identify a user. Action **142** may comprise receiving, at the portable communication device, a device verification value for the consumer account. Action **143** may comprise providing information related to the consumer account to a merchant for a transaction with the merchant, the information including the received device verification value. In another implementation, action **141** may comprise sending, using a portable communication device, a message to a provision entity requesting a device verification value for a consumer account, the consumer account having an account number that identifies the consumer account within a payment processing network, the message comprising an incomplete part of said account number. The message may further comprise a phone number or network address of a personal communication device. The message may further comprise a unique identification code

that is different from the account number, and that uniquely identifies a user. Action **142** may comprise receiving, at the portable communication device, a device verification value for the consumer account. Action **143** may comprise providing information related to the consumer account to a merchant for a transaction with the merchant, the information including the received device verification value.

[0084] In each of the above embodiments, one or more portable consumer devices **5** may be combined and electronically integrated with personal communication device **7** and provided as a single physical unit.

[0085] **Alerts including data for use in completing transactions.** While the above embodiments have focused on device verification values for purchase transactions, the inventors have recognized that a verification value is one of several pieces of information that may be associated with a transaction, and that the above embodiments may be configured to process (*e.g.*, to obtain, receive, and send) other pieces of transaction-related information. For example, in some exemplary embodiments, a message may be sent from provision entity **80** to user **1** (FIG. 1) during a transaction in order to assist with the transaction. For example, user **1** may need to provide, to the merchant or other appropriate party, certain information in order to complete the transaction, such as a billing zip code, a PIN (personal identification number), an expiration date, a card security code (*e.g.* CVV, CVVC, etc), or other required information. During the transaction, user **1** may inadvertently omit or incorrectly enter some of the required information. In some exemplary embodiments, user **1** may receive a message (such as an SMS message or network message) with the omitted or corrected information to allow for completion of the transaction. For example, during a transaction using a credit card (such as at a gas station on a business trip), user **1** may be asked to provide the billing address of the credit card. The credit card may be associated with an employer of user **1**, such that user **1** may not know the correct billing address. Upon a certain trigger (*e.g.* inputting the wrong information during the transaction, user **1** requesting the information, *etc.*), a message may be sent to the personal communications device **7** of user **1** (*e.g.*, a wireless phone registered as belonging to user **1**). This message can contain the billing address for the credit card. User **1** can then supply the correct information, allowing the transaction to finish.

[0086] In certain embodiments, the message may only include a portion of the omitted or corrected information, or a hint regarding the omitted or corrected information, to prevent unauthorized transactions. For example, if user **1** provides the wrong information during a transaction, user **1** may receive a message (such as an SMS message) with a hint, such as "use your work address for the billing address." Another example of the hint may be "please enter your work zip code, not your current zip code." In certain embodiments, the message may include information for a future transaction. For example, once a first transaction has been completed, user **1** may receive a message containing a PIN code, a card security code, or other information that will be needed to complete a later, second transaction, such as the next transaction. This can prevent unauthorized transactions, as even if the portable consumer device **7** is compromised, the message containing the information can still be secure.

[0087] Referring to FIG. 1, omitted or incorrect information may be detected by payment processing network **70** when merchant **20** sends the transaction information to network **70** for authorization. Network **70** may determine which piece of information is omitted or incorrect, and may send a message to provision entity **80** instructing entity **80** to send a message to user **1** providing an indication of which piece of information was omitted or incorrect, and optionally providing the omitted or corrected piece of information or a hint thereto. The message sent from payment processing network **70** to provision entity **80** includes the account number of the portable consumer device **5** so that entity **80** may find the mobile phone number or URID (*e.g.*, the network address) of personal communication device **7** from one of its databases **86**. The message sent from network **70** to entity **80** may also include the text that is to be displayed to user **1** so that entity **80** may simply forward this text to user **1**. When the mobile phone number or URID (*e.g.*, the network address) is located from one of databases **86** by provision entity **80**, the entity can simply forward the text in a message to user **1**. At substantially the same time, network **70** may send a message to merchant **20** instructing the merchant to reacquire the payment information from user **1** and to retry the transaction with the reentered payment information. User **1** may then receive a message from entity **80** with text of what information was omitted or incorrect, which may contain an indication of how to correct the entry of the payment information. User **1** may then proceed with a complete and correct entry of the payment information with merchant **20**.

Merchant **20** may then resend the authorization request to payment processing network **70**.

[0088] To implement the above, computer-readable medium **82** of provision entity **80** may store an application **85'** having the following codes. A first code directs processor(s) **81** to receive a request message from payment processing network **70** and to place in temporary memory storage the following: a message datum from the request message indicating a piece of information for a portable consumer device, and an account number of the portable consumer device **7** associated with user **1**. The request message from payment processing network **70** may implicitly serve as a request to provision entity **80** to provide the message datum to user **1**, or the request message may contain an explicit direction to do so. The first code may comprise function calls to the network services module of the operating system of entity **80** and conventional I/O instructions to networking facility **84**, memory access instructions, CPU logic instructions, and CPU control instructions. A second code of application **85'** directs processor(s) **81** to access a record of user **1** based upon the account number provided in the request message, the record having at least one of a mobile phone number or a URID (*e.g.*, the network address) of the user's portable consumer device **7** that has been associated with the account number. The second code may comprise conventional I/O instructions or function calls to one of databases **86** (direct or via networking facility **84**), memory access instructions, and CPU control instructions. A third code of application **85'** directs processor(s) **81** to send an alert message to the mobile phone number or URID (*e.g.*, the network address) of personal communication device **7** in the form of a text message routed through SMS gateway **90** or a network message routed through first communications network **31**, with the alert message having the message datum indicative of the piece of information. The third code may comprise function calls to the network services module of the operating system and conventional I/O instructions to networking facility **84**, memory access instructions, CPU logic instructions, and CPU control instructions. The codes of this application for provision entity **80** may be implemented by one of ordinary skill in the software art without undue experimentation.

[0089] As another implementation approach, payment processing network **70** may be combined with provision entity **80**, in which case a formal message from network **70** to

entity **80** does not need to be sent. Computer-readable medium **82** of provision entity **80** may store an application **85"** having the following codes for the merged operation of network **70** and entity **80**. A first code directs processor(s) **81** to receive an authorization request message from a merchant **20** which includes payment information, and to store the payment information in temporary memory storage. The first code may comprise function calls to the network services module of the operating system of entity **80** and conventional I/O instructions to networking facility **84**, memory access instructions, CPU logic instructions, and CPU control instructions. A second code directs processor(s) **81** to access a record of payment information for the account number provided in the authorization request message, the record having at least one of a mobile phone number or the URID (*e.g.*, the network address) of the user's portable consumer device **7** that has been associated with the account number. The second code may comprise conventional I/O instructions or function calls to one of databases **86** (direct or via networking facility **84**), memory access instructions, and CPU control instructions. A third code directs processor(s) **81** to compare the received payment information with the payment information from the accessed record to identify omitted or incorrect payment information, and to generate a message datum indicative of the omitted or incorrect payment information. A portion of the message datum, or the entire message datum, may be copied and/or derived from a message field in the accessed record, the message field being associated with the record's data field that is related to the omitted or incorrect payment information. The third code may comprise memory access instructions (the accessed record may be stored in temporary memory), CPU logic instructions, and CPU control instructions. A fourth code directs processor(s) **81** to send an alert message to the mobile phone number or the URID (*e.g.*, the network address) of personal communication device **7** in the form of a text message routed through SMS gateway **90** or a network message routed through first communications network **31**, with the alert message having the message datum indicative of the omitted or incorrect piece of information. The code may comprise function calls to the network services module of the operating system and conventional I/O instructions to networking facility **84**, memory access instructions, CPU logic instructions, and CPU control instructions. The codes of application **85"** for provision

entity **80** may be implemented by one of ordinary skill in the software art without undue experimentation.

[0090] Embodiments of the invention are not limited to systems involving purchase transactions. The same approach could be applied for other financial systems. For example, embodiments could be used to authenticate a user using an online banking application. A cardholder may enter his user ID into a banking website. The cardholder can then use his or her personal communication device to obtain and use a dCVV2 value as a verification value. The banking website can validate the User ID and the verification value provided by the user by communicating with the provision entity.

[0091] Embodiments of the invention are not limited to the above-described embodiments. For example, although separate functional blocks are shown for an issuer, payment processing system, and acquirer, some entities perform all of these functions and may be included in embodiments of invention.

[0092] It should be understood that various embodiments of the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement embodiments of the present invention using hardware and a combination of hardware and software.

[0093] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, C, C#, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer-readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer-readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0094] The above description is illustrative and is not restrictive. Many variations of the invention and embodiments thereof will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0095] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0096] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0097] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

WHAT IS CLAIMED IS:

1. A method comprising:

(a) receiving, at a server, a request for a device verification value for a portable consumer device associated with a user, the request originating from a personal communication device associated with the user;

(b) obtaining, from the received request, a phone number or network address of the personal communication device from which the received request was originated;

(c) obtaining an account record that contains the obtained phone number or network address, the account record associating a consumer account of a portable consumer device with the obtained phone number or network address;

(d) obtaining a datum indicative of a device verification value for the consumer account of the obtained account record; and

(e) sending the obtained datum to at least one of a phone number or network address of a personal communication device associated with the consumer account of the obtained account record.

2. The method of Claim 1, wherein the obtained account record associates a plurality of consumer accounts of portable consumer devices with the obtained phone number or network address, and wherein the method further comprises selecting one of the consumer accounts from the obtained account record as the consumer account for which the datum is obtained.

3. The method of Claim 2, wherein the obtained account record stores one or more account numbers of one or more consumer accounts, each consumer account associated with a portable consumer device;

wherein the method further comprises obtaining an incomplete account number from the received request; and

wherein selecting a consumer account of the portable consumer device comprises comparing the obtained incomplete account number to the one or more account numbers stored in the obtained account record to find a match between the incomplete account number and a portion of one of the stored account numbers.

4. The method of Claim 2, wherein the obtained account record stores one or more code phrases of one or more consumer accounts, each consumer account corresponding to a portable consumer device;

wherein the method further comprises obtaining a code phrase from the received request; and

wherein selecting a consumer account of the portable consumer device comprises comparing the obtained code phrase to the one or more code phrases stored in the obtained account record to find a match between the obtained code phrase and a stored code phrase.

5. The method of Claim 1, further comprising sending a datum indicative of the device verification value for the consumer account and an indication of the consumer account to an entity different from the personal communication device associated with the consumer account.

6. The method of Claim 1, wherein the consumer account is provided by an issuing bank, and wherein the method further comprises sending a datum indicative of the device verification value for the consumer account and an indication of the consumer account to the issuing bank.

7. The method of Claim 1, wherein transmitting the datum indicative of the device verification value further comprises transmitting an indication of a time period in which the device verification value can be used for a transaction.

8. The method of Claim 1, wherein obtaining the datum indicative of a device verification value comprises generating the datum from an algorithm.

9. The method of Claim 1, wherein obtaining the datum indicative of the device verification value comprises obtaining the datum from a data storage device.

10. The method of Claim 1, wherein transmitting the datum indicative of the device verification value comprises transmitting said datum to a phone number of the personal communications device.

11. The method of Claim 1, wherein transmitting the datum indicative of the device verification value comprises transmitting said datum to a network address of the personal communications device via a communications facility of the server, the communications facility being coupled to a communications network.

12. The method of Claim 2 wherein obtaining a datum representative of a device verification value comprises: selecting a process of generating the device verification value based upon the selected consumer account.

13. The method of Claim 1, wherein the consumer account comprises an account number that identifies the consumer account within a payment processing network, wherein a unique identification code that is different from the account number is associated with the user, wherein the obtained account record stores the unique identification code, and wherein the method further comprises obtaining a identification code from the received request, and comparing the obtained identification code to the unique identification code stored in the obtained account record.

14. The method of Claim 1, wherein the obtained account record comprises a data field that indicates the route by which the datum indicative of a device verification value is to be sent, and wherein the method further comprises accessing the data field to determine the phone number or network address to which to send the datum.

15. The method of Claim 1, wherein the device verification value provided in the sent datum is intended for a financial transaction, and wherein the request for the device verification value is received prior to the financial transaction being initiated.

16. The method of Claim 1, further comprising comparing the obtained phone number or network address against a database that tracks mobile phone numbers and network addresses that have been used in fraudulent activities.

17. The method of Claim 1, further comprising comparing the consumer account against a database that tracks consumer accounts that have been used in fraudulent activities.

18. The method of Claim 1, further comprising sending an e-mail message to an e-mail address of the user notifying the user of one or more of the following occurrences: a request for a device verification value, a sending of a device verification value, a denial of a request for a device verification value.

19. A computer program product embodied on a computer-readable medium, the product comprising:

code that directs a data processor to receive a request for a device verification value for a portable consumer device associated with a user, the request originating from a personal communication device associated with the user;

code that directs the data processor to obtain, from the received request, a phone number or network address of the personal communication device from which the received request was originated;

code that directs the data processor to obtain an account record that contains the obtained phone number or network address, the account record associating a consumer account of a portable consumer device with the obtained phone number or network address;

code that directs the data processor to obtain a datum indicative of a device verification value for the consumer account of the obtained account record; and

code that directs the data processor to send the obtained datum to at least one of a phone number or network address of a personal communication device associated with the consumer account of the obtained account record.

20. The product of Claim 19, wherein the obtained account record associates a plurality of consumer accounts of portable consumer devices with the obtained phone number or network address, and wherein the product further comprises code that directs the data processor to select one of the consumer accounts from the obtained account record as the consumer account for which the datum is obtained.

21. The computer program product of Claim 20, wherein the obtained account record stores one or more account numbers of one or more consumer accounts, each consumer account associated with a portable consumer device;

wherein the computer program product further comprises code that directs the data processor to obtain an incomplete account number from the received request; and

wherein the code that directs the data processor to select a consumer account of the portable consumer device comprises code that directs the data processor to compare the obtained incomplete account number to the one or more account numbers stored in the obtained account record to find a match between the incomplete account number and a portion of one of the stored account numbers.

22. The computer program product of Claim 20, wherein the obtained account record stores one or more code phrases of one or more consumer accounts, each consumer account associated with a portable consumer device;

wherein the computer program product further comprises code that directs the data processor to obtain a code phrase from the received request; and

wherein the code that directs the data processor to select a consumer account of the portable consumer device comprises code that directs the data processor to compare the obtained code phrase to the one or more code phrases stored in the obtained account record to find a match between the obtained code phrase and a stored code phrase.

23. The computer program product of Claim 19, further comprising code that directs the data processor to send a datum indicative of the device verification value for the consumer account and an indication of the consumer account to an entity

different from the personal communication device associated with the consumer account.

24. The computer program product of Claim 19, wherein the consumer account is provided by an issuing bank, and wherein the computer program product further comprises code that directs the data processor to send a datum indicative of the device verification value for the consumer account and an indication of the consumer account to the issuing bank.

25. The computer program product of Claim 19, further comprising code that directs the data processor to send an indication of a time period in which the device verification value can be used for a transaction.

26. The computer program product of Claim 19, wherein the obtained account record stores one or more method data fields of one or more consumer accounts, each method data field indicating an algorithm to be used to generate a device verification value;

wherein the code that directs the data processor to obtain a datum indicative of a device verification value for the consumer account comprises code that directs the data processor to obtain an indication of an algorithm from a method data field of the obtained account record and to execute the algorithm for which the indication was obtained.

27. The computer program product of Claim 19, wherein the obtained account record stores one or more data fields of one or more consumer accounts, each data field holding at least one datum indicative of a device verification value;

wherein the code that directs the data processor to obtain a datum indicative of a device verification value for the consumer account comprises code that directs the data processor to obtain a datum indicative of a device verification value from a data field of the obtained account record.

28. The computer program product of Claim 19, wherein the code that directs the data processor to obtain a datum indicative of a device verification value for the consumer account comprises code that directs the data processor to determine the identity of the issuing bank from the consumer account, to send an electronic message to the issuing bank to request a datum indicative of a device verification value, and to receive a datum indicative of a device verification value from the issuing bank.

29. The computer program product of Claim 19, wherein the obtained account record stores at least one of a phone number or network address of a personal communication device associated with the consumer account; and

wherein the code that directs the data processor to send the obtained datum comprises code that directs the data processor to obtain the at least one of a phone number or network address from the obtained account record.

30. The computer program product of Claim 19, wherein the request is received in the form of a computer-readable data message sent from a short message server gateway, and wherein the computer program product further comprises code that directs the data processor to obtain the network address of the gateway from the received data message, to access a database that stores the network addresses of trusted short message server gateways to determine if the obtained network address is found in the accessed database.

31. The computer program product of Claim 19, wherein the consumer account comprises an account number that identifies the consumer account within a payment processing network, wherein a unique identification code that is different from the account number is associated with the user, wherein the obtained account record stores the unique identification code, and wherein the computer program product further comprises code that directs the data processor to obtain an identification code from the received request, and to compare the obtained identification code to the unique identification code stored in the obtained account record.

32. The computer program product of Claim 19, further comprising code that directs the data processor to compare the obtained phone number or network

address against a database that tracks mobile phone numbers and network addresses that have been used in fraudulent activities.

33. The computer program product of Claim 19, further comprising code that directs the data processor to compare the consumer account against a database that tracks consumer accounts that have been used in fraudulent activities.

34. The computer program product of Claim 19, further comprising code that directs the data processor to send an e-mail message to an e-mail address of the user notifying the user of one or more of the following occurrences: a request for a device verification value, a sending of a device verification value, a denial of a request for a device verification value.

35. A server incorporating the computer program product of Claim 11, the server comprising a data processor, a networking facility coupled to the processor, a computer-readable medium coupled to the processor, and the computer program product embodied on the computer-readable medium.

36. A method comprising:

(a) receiving, at a server, a request for a device verification value for a portable consumer device associated with a user;

(b) obtaining, from the received request, a unique identification code assigned to the user;

(c) obtaining an account record that contains the obtained unique identification code, the account record associating a consumer account of a portable consumer device with the obtained unique identification code, the consumer account having an account number associated with it that identifies the consumer account within a payment processing network, the obtained unique identification code being different from the account number of the consumer account of the obtained account record;

(d) obtaining a datum indicative of a device verification value for the consumer account of the obtained account record; and

(e) sending the obtained datum to at least one of a phone number or network address of a personal communication device associated with the consumer account of the obtained account record.

37. The method of Claim 36, wherein the obtained account record associates a plurality of consumer accounts of portable consumer devices with the obtained unique identification code, and wherein the method further comprises selecting one of the consumer accounts from the obtained account record as the consumer account for which the datum is obtained.

38. The method of Claim 37, wherein the obtained account record stores one or more account numbers of one or more consumer accounts, each consumer account associated with a portable consumer device;

wherein the method further comprises obtaining an incomplete account number from the received request; and

wherein selecting a consumer account of the portable consumer device comprises comparing the obtained incomplete account number to the one or more account numbers stored in the obtained account record to find a match between the incomplete account number and a portion of one of the stored account numbers.

39. The method of Claim 37, wherein the obtained account record stores one or more code phrases of one or more consumer accounts, each consumer account corresponding to a portable consumer device;

wherein the method further comprises obtaining a code phrase from the received request; and

wherein selecting a consumer account of the portable consumer device comprises comparing the obtained code phrase to the one or more code phrases stored in the obtained account record to find a match between the obtained code phrase and a stored code phrase.

40. The method of Claim 36, further comprising sending a datum indicative of the device verification value for the consumer account and an indication of

the consumer account to an entity different from the personal communication device associated with the consumer account.

41. The method of Claim 36, wherein the consumer account is provided by an issuing bank, and wherein the method further comprising sending a datum indicative of the device verification value for the consumer account and an indication of the consumer account to the issuing bank.

42. The method of Claim 36, wherein transmitting the datum indicative of the device verification value further comprises transmitting an indication of a time period in which the device verification value can be used for a transaction.

43. The method of Claim 36, wherein the obtained account record comprises a data field that indicates the route by which the datum indicative of a device verification value is to be sent, and wherein the method further comprises accessing the data field to determine the phone number or network address to which to send the datum.

44. The method of Claim 36, further comprising comparing the consumer account against a database that tracks consumer accounts that have been used in fraudulent activities.

45. The method of Claim 36, further comprising sending an e-mail message to an e-mail address of the user notifying the user of one or more of the following occurrences: a request for a device verification value, a sending of a device verification value, a denial of a request for a device verification value.

46. A computer program product embodied on a computer-readable medium, the product comprising:

code that directs a data processor to receive a request for a device verification value for a portable consumer device associated with a user;

code that directs the data processor to obtain, from the received request, a unique identification code assigned to the user;

code that directs the data processor to obtain an account record that contains the obtained unique identification code, the account record associating a consumer account of a portable consumer device with the obtained unique identification code, the consumer account having an account number associated with it that identifies the consumer account within a payment processing network, the obtained unique identification code being different from the account number of the consumer account of the obtained account record;

code that directs the data processor to obtain a datum indicative of a device verification value for the consumer account of the obtained record; and

code that directs the data processor to send the obtained datum to at least one of a phone number or network address of a personal communication device associated with the consumer account of the obtained account record.

47. The product of Claim 46, wherein the obtained account record associates a plurality of consumer accounts of portable consumer devices with the obtained unique identification code, and wherein the product further comprises code that directs the data processor to select one of the consumer accounts from the obtained account record as the consumer account for which the datum is obtained.

48. The computer program product of Claim 47, wherein the obtained account record stores one or more account numbers of one or more consumer accounts, each consumer account associated with a portable consumer device;

wherein the computer program product further comprises code that directs the data processor to obtain an incomplete account number from the received request; and

wherein the code that directs the data processor to select a consumer account of the portable consumer device comprises code that directs the data processor to compare the obtained incomplete account number to the one or more account numbers stored in the obtained account record to find a match between the incomplete account number and a portion of one of the stored account numbers.

49. The computer program product of Claim 47, wherein the obtained account record stores one or more code phrases of one or more consumer accounts, each consumer account associated with a portable consumer device;

wherein the computer program product further comprises code that directs the data processor to obtain a code phrase from the received request; and

wherein the code that directs the data processor to select a consumer account of the portable consumer device comprises code that directs the data processor to compare the obtained code phrase to the one or more code phrases stored in the obtained account record to find a match between the obtained code phrase and a stored code phrase.

50. The computer program product of Claim 46, further comprising code that directs the data processor to send a datum indicative of the device verification value for the consumer account and an indication of the consumer account to an entity different from the personal communication device associated with the consumer account.

51. The computer program product of Claim 46, wherein the consumer account is provided by an issuing bank, and wherein the computer program product further comprises code that directs the data processor to send a datum indicative of the device verification value for the consumer account and an indication of the consumer account to the issuing bank.

52. The computer program product of Claim 46, further comprising code that directs the data processor to send an indication of a time period in which the device verification value can be used for a transaction.

53. The computer program product of Claim 46, wherein the obtained account record stores one or more method data fields of one or more consumer accounts, each method data field indicating an algorithm to be used to generate a device verification value;

wherein the code that directs the data processor to obtain a datum indicative of a device verification value for the consumer account comprises code that directs the data processor to obtain an indication of an algorithm from a method data field of the obtained account record and to execute the algorithm for which the indication was obtained.

54. The computer program product of Claim 46, wherein the obtained account record stores one or more data fields of one or more consumer accounts, each data field holding at least one datum indicative of a device verification value;

wherein the code that directs the data processor to obtain a datum indicative of a device verification value for the consumer account comprises code that directs the data processor to obtain a datum indicative of a device verification value from a data field of the obtained account record.

55. The computer program product of Claim 46, wherein the code that directs the data processor to obtain a datum indicative of a device verification value for the consumer account comprises code that directs the data processor to determine the identity of the issuing bank from the consumer account, to send an electronic message to the issuing bank to request a datum indicative of a device verification value, and to receive a datum indicative of a device verification value from the issuing bank.

56. The computer program product of Claim 46, wherein the obtained account record stores at least one of a phone number or network address of a personal communication device associated with the consumer account; and

wherein the code that directs the data processor to send the obtained datum comprises code that directs the data processor to obtain the at least one of a phone number or network address from the obtained account record.

57. The computer program product of Claim 46, wherein the request is received in the form of a computer-readable data message sent from a short message server gateway, and wherein the computer program product further comprises code that directs the data processor to obtain the network address of the gateway from the

received data message, to access a database that stores the network addresses of trusted short message server gateways to determine if the obtained network address is found in the accessed database.

58. The computer program product of Claim 46, further comprising code that directs the data processor to compare the consumer account against a database that tracks consumer accounts that have been used in fraudulent activities.

59. The computer program product of Claim 46, further comprising code that directs the data processor to send an e-mail message to an e-mail address of the user notifying the user of one or more of the following occurrences: a request for a device verification value, a sending of a device verification value, a denial of a request for a device verification value.

60. A server incorporating the computer program product of Claim 46, the server comprising a data processor, a networking facility coupled to the processor, a computer-readable medium coupled to the processor, and the computer program product embodied on the computer-readable medium.

61. A method comprising:

sending, using a portable communication device, a message to a provision entity requesting a device verification value for a consumer account, the consumer account having an account number that identifies the consumer account within a payment processing network, the message comprising at least one of a code phrase or identification code that is different from said account number;

receiving, at the portable communication device, a device verification value for the consumer account; and

providing information related to the consumer account to a merchant for a transaction with the merchant, the information including the received device verification value.

62. The method of Claim 61, wherein the message further comprises a phone number or network address of a personal communication device.

63. The method of Claim 61, wherein the identification code is uniquely assigned to a user.

64. A method comprising:

sending, using a portable communication device, a message to a provision entity requesting a device verification value for a consumer account, the consumer account having an account number that identifies the consumer account within a payment processing network, the message comprising an incomplete part of said account number;

receiving, at the portable communication device, a device verification value for the consumer account; and

providing information related to the consumer account to a merchant for a transaction with the merchant, the information including the received device verification value.

65. The method of Claim 64, wherein the message further comprises a phone number or network address of a personal communication device.

66. The method of Claim 64, wherein the message further comprises a unique identification code that is different from the account number.

67. A computer program product embodied on computer-readable medium to be run by a data processor that is electrically coupled to a computer-readable medium, a touch screen display, and a networking facility, the product comprising:

a first code that directs the data processor to present a graphical-user interface button on the touch screen display; and

a second code that directs the data processor to sense an activation of the graphical-user interface button and, in response thereto, to direct the networking facility to send a message to a provision entity requesting a device verification value for a

consumer account, the consumer account having an account number that identifies the consumer account within a payment processing network, and the message including at least one of an incomplete account number, a code phrase different from the account number of the consumer account, or a unique identification code that is different from the account number of the consumer account.

68. The computer program product of Claim 67, wherein the second code further directs the data processor to access the computer-readable medium, prior to sending the request message, to obtain at least one item, the at least one item being a code phrase, incomplete account number of the consumer account, or unique identification code, and to include the at least one obtained item in the request message.

69. The computer program product of Claim 67, wherein the second code further directs the data processor to determine when there is more than one instance of a code phrase or incomplete account number stored in the accessed computer-readable medium, and in response, to present a selection screen on the touch screen display that displays representations of two or more of said instances, to obtain a selection from the touch display screen of one of said instances, and to include an indication of the selected instance in the message to the provision entity.

70. The computer program product of Claim 67, wherein the second code further directs the data processor to include in the request message at least one of a phone number or network address assigned to the networking facility.

71. The computer program product of Claim 67, wherein the second code further directs the data processor to include the unique identification code and at least one of the incomplete account number or code phrase in the request message.

72. The computer program product of Claim 67, further comprising code that directs the processor to scan a data structure of messages stored in the computer

readable medium for messages from the provision entity, and to delete such messages that have been stored in the data structure for more than a selected period of time.

73. The computer program product of Claim 67, further comprising code that directs the processor to scan a data structure of messages stored in the computer readable medium for messages from the provision entity, to identify the latest message from the provision entity, and to delete at least one message from the provision entity that is older than the latest message.

74. The computer program product of Claim 67, further comprising code that directs the processor to scan a data structure of messages stored in the computer readable medium for messages from the provision entity, to identify the latest message from the provision entity, to obtain a device verification value from the latest message, and to display the device verification value on the touch screen display.

75. The computer program product of Claim 67, further comprising code that directs the processor to scan a data structure of messages stored in the computer readable medium for messages from the provision entity, to identify the latest message from the provision entity, to obtain a datum indicative of a device verification value from the latest message, to decode or decrypt the datum to obtain a device verification value, and to display the device verification value on the touch screen display.

76. A personal communication device incorporating the computer program product of Claim 67, the personal communication device comprising a data processor, a networking facility coupled to the processor, a computer-readable medium coupled to the processor, and the computer program product embodied on the computer-readable medium.

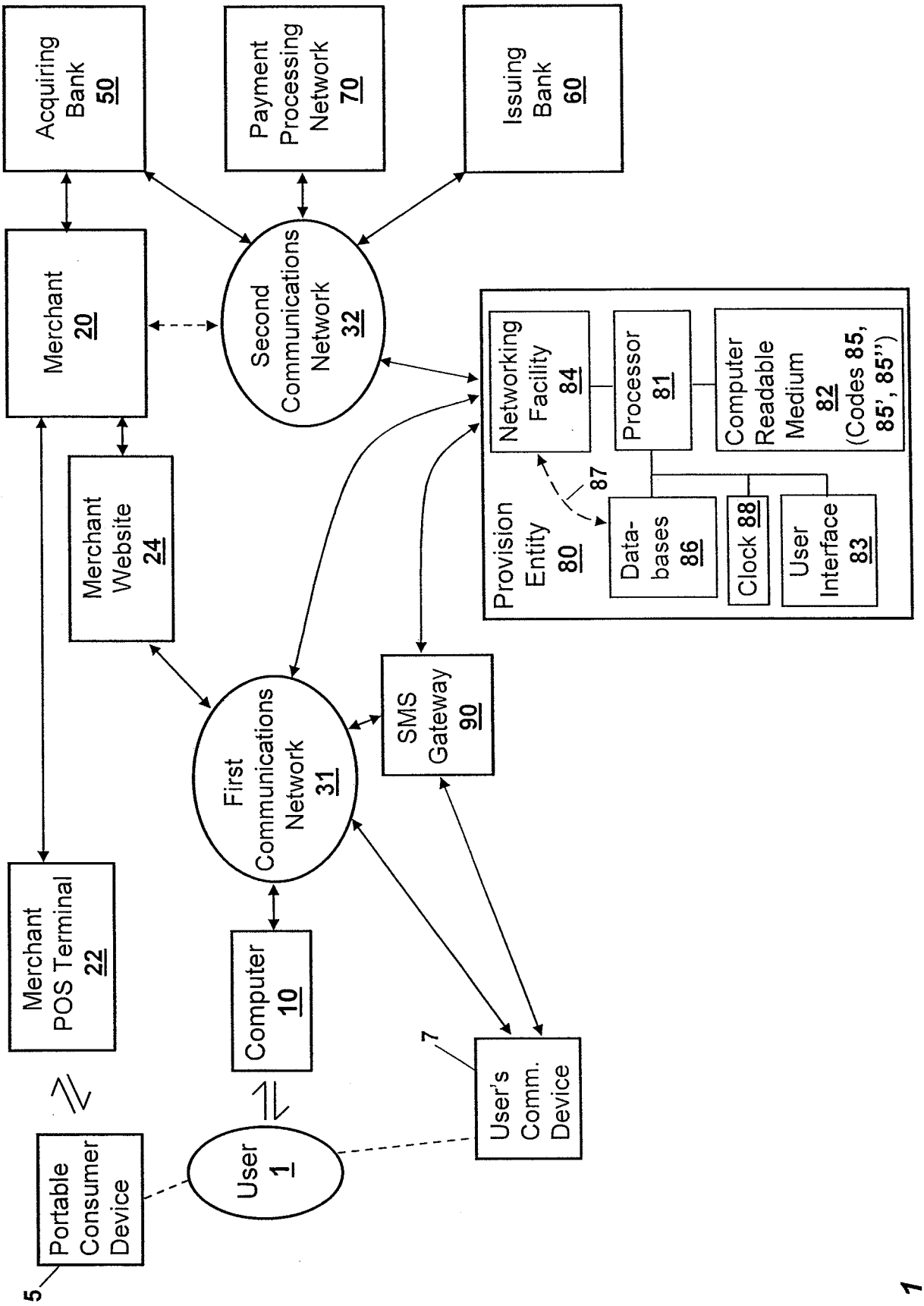

Acquiring Bank 50
Payment Processing Network 70
Issuing Bank 60
Merchant 20
Second Communications Network 32
Networking Facility 84
Processor 81
Computer Readable Medium 82 (Codes 85, 85', 85'')
Provision Entity 80
87
Data-bases 86
Clock 88
User Interface 83
Merchant Website 24
First Communications Network 31
SMS Gateway 90
Merchant POS Terminal 22
Computer 10
User's Comm. Device
7
Portable Consumer Device
User 1
5

FIG. 1

Mobile Phone Number	Network Address	User's Unique ID code			
Consumer Account A	Account Number for Account A	Code Phrase for Account A	Reply Route for Account A	dCVV2 Method for Account A	Parameters for Account A
Consumer Account B	Account Number for Account B	Code Phrase for Account B	Reply Route for Account B	dCVV2 Method for Account B	Parameters for Account B
Consumer Account C	Account Number for Account C	Code Phrase for Account C	Reply Route for Account C	dCVV2 Method for Account C	Parameters for Account C

FIG. 2

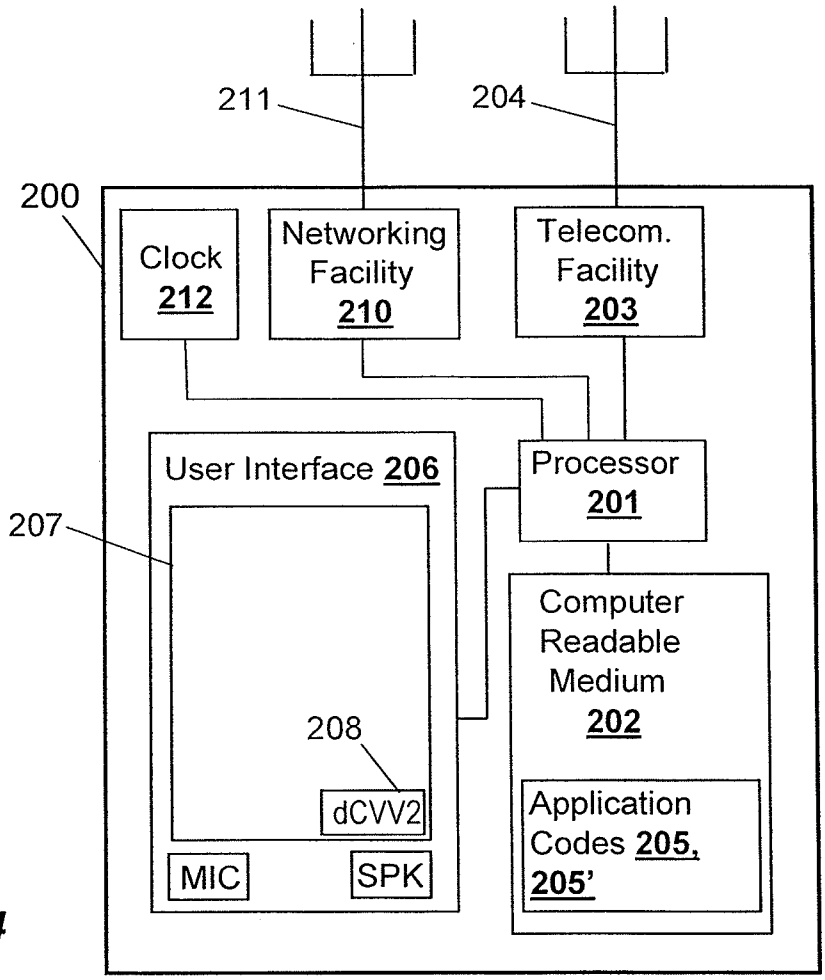


FIG. 4

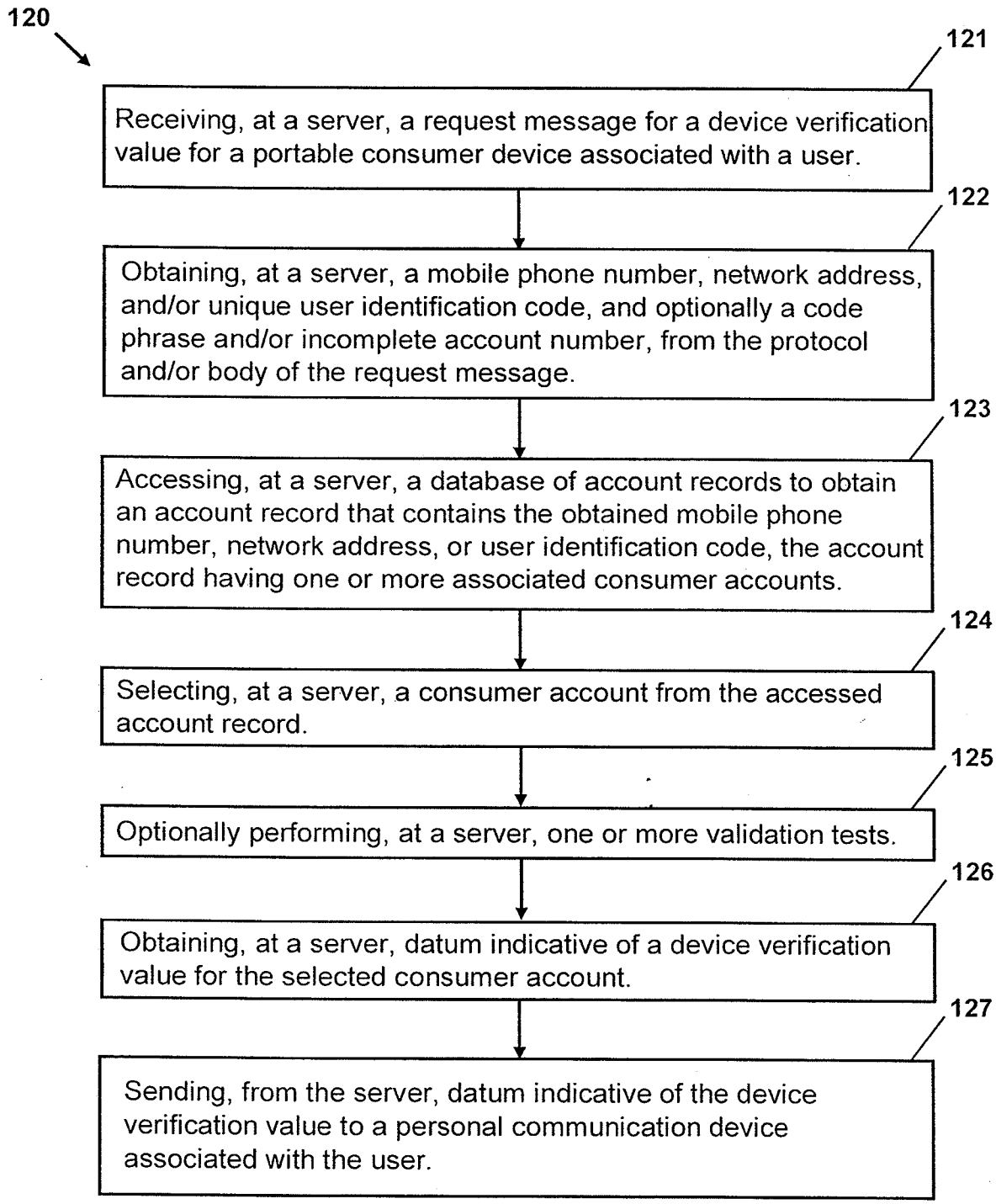

120
121
Receiving, at a server, a request message for a device verification value for a portable consumer device associated with a user.
122
Obtaining, at a server, a mobile phone number, network address, and/or unique user identification code, and optionally a code phrase and/or incomplete account number, from the protocol and/or body of the request message.
123
Accessing, at a server, a database of account records to obtain an account record that contains the obtained mobile phone number, network address, or user identification code, the account record having one or more associated consumer accounts.
124
Selecting, at a server, a consumer account from the accessed account record.
125
Optionally performing, at a server, one or more validation tests.
126
Obtaining, at a server, datum indicative of a device verification value for the selected consumer account.
127
Sending, from the server, datum indicative of the device verification value to a personal communication device associated with the user.

FIG. 3

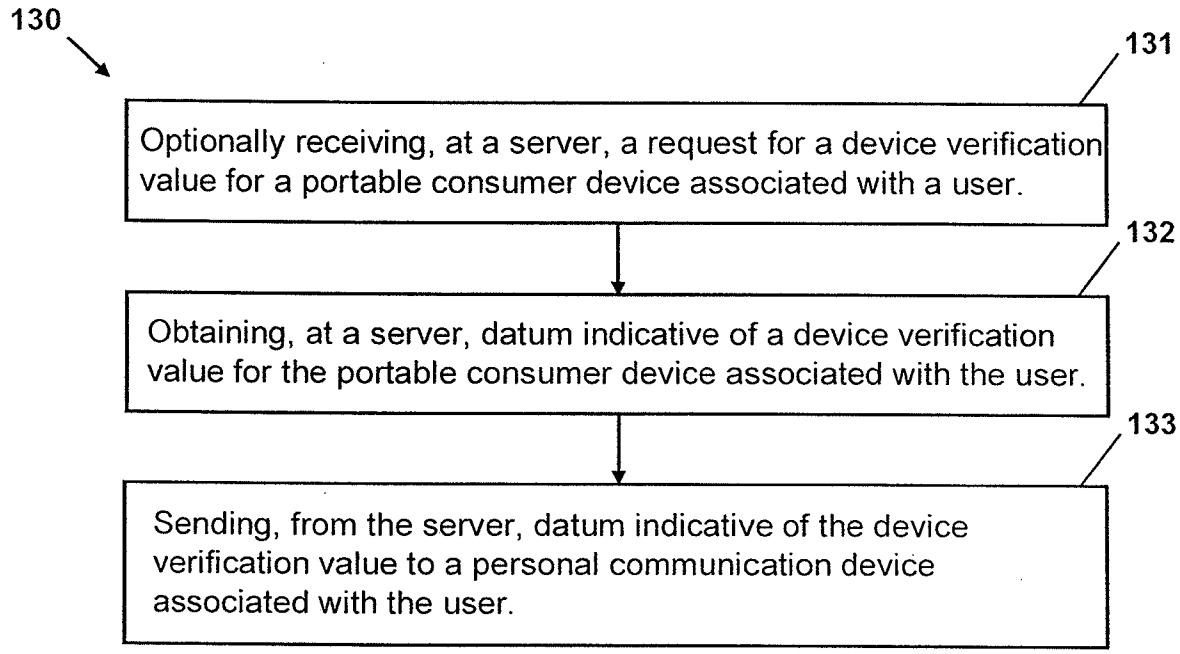

130
131
Optionally receiving, at a server, a request for a device verification value for a portable consumer device associated with a user.
132
Obtaining, at a server, datum indicative of a device verification value for the portable consumer device associated with the user.
133
Sending, from the server, datum indicative of the device verification value to a personal communication device associated with the user.

FIG. 5

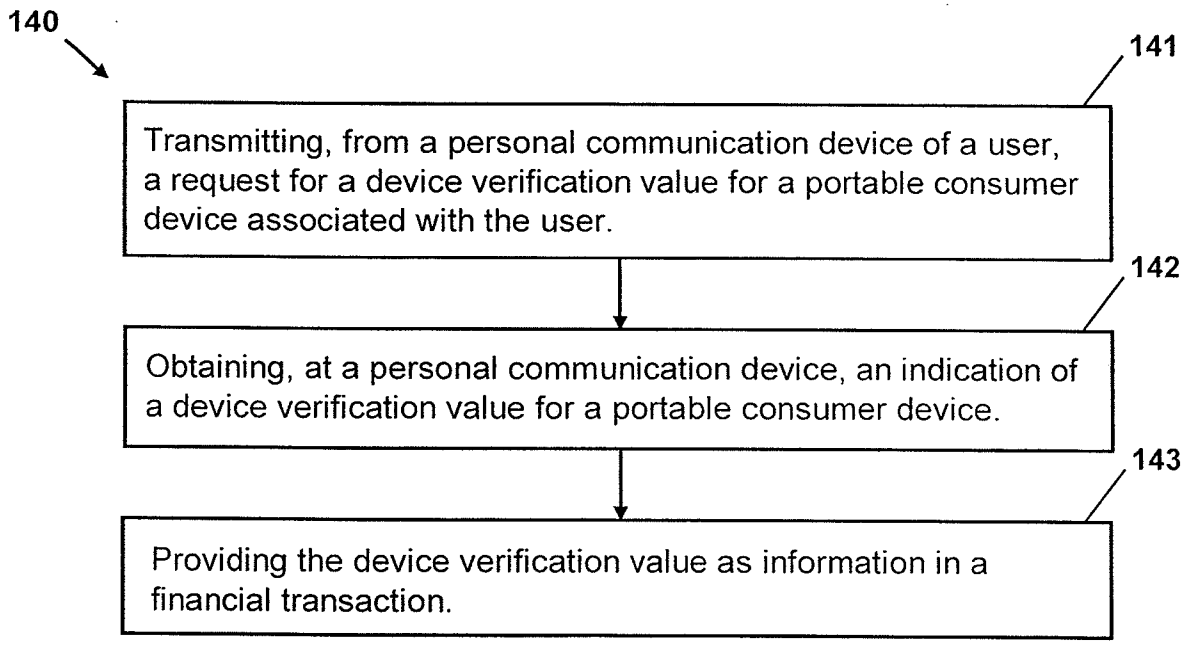

140
141
Transmitting, from a personal communication device of a user, a request for a device verification value for a portable consumer device associated with the user.
142
Obtaining, at a personal communication device, an indication of a device verification value for a portable consumer device.
143
Providing the device verification value as information in a financial transaction.

FIG. 6