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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 May 2008 (29.05.2008)

PCT

(10) International Publication Number
WO 2008/064013 A2

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

(21) **International Application Number:**
PCT/US2007/084565

(22) International Filing Date:
13 November 2007 (13.11.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/866,191 16 November 2006 (16.11.2006) US
11/935,740 6 November 2007 (06.11.2007) US

(71) **Applicants** *(for all designated States except US):* **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US). **VISA U.S.A. INC.** [US/US]; P. O. Box 8999, San Francisco, California 94128-8999 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only):* **STEELE, Kim** [US/US]; 24129 Heather Hill Place, Aldie, Virginia 20105 (US). **YAKEL, Mike** [US/US]; 8913 Newgard Court, Charlotte, North Carolina 28269 (US). **WELLER, Kevin** [US/US]; 63 Fernwood Drive, San Anselmo, California 94960 (US). **FAITH, Patrick** [US/US]; 2810 Jones Gate Court, Pleasanton, California 94566 (US). **VAN DELOO, Lori D.** [US/US]; 361 Hawthorne Avenue, Los Altos, California 94022 (US).

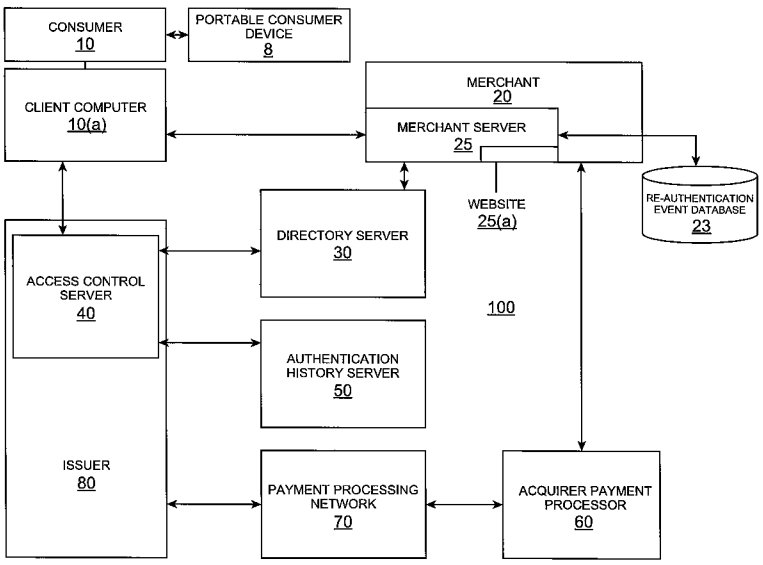
(74) Agents: PACHECO, Raquel et al; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available):* ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: ADAPTIVE AUTHENTICATION OPTIONS



(57) Abstract: A method for authenticating a consumer for a portable consumer device is disclosed. One embodiment of the invention includes receiving a transaction message relating to a request by a consumer to conduct a transaction using a portable consumer device, wherein the consumer was previously enrolled in an authentication program and the consumer was previously authenticated, analyzing the transaction message to determine if a re-authentication event has taken place, causing a re-authentication message to be sent to the consumer before initiating an authorization request message to the issuer if the re-authentication event has taken place, and initiating the authorization request message to the issuer without sending the re-authentication message to the consumer if the re-authentication event has not taken place.

WO 2008/064013 A2

European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

ADAPTIVE AUTHENTICATION OPTIONS

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This patent application is a non-provisional of and claims priority to U.S. provisional patent application no. 60/866,191 , filed on November 16, 2006, which is herein incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] In a typical purchase transaction, a consumer may use a portable consumer device to pay for goods or services from a merchant. It is important to ensure that the consumer is the authorized user of the portable consumer device that is used to make the purchase. Otherwise, the issuers of such portable consumer devices, merchants, consumers, etc. are at risk of losing money. Further, if consumers perceive that buying goods and services using such portable consumer devices is not safe and secure, they may be inhibited from using them. Ensuring that a consumer is an authorized user of a portable consumer device becomes especially important in situations where the consumer is not making the purchase in person, but rather is making the purchase online, through the mail, or over the phone.

[0003] To address the issue of unauthorized use or fraudulent purchases, many solutions have been developed. One example is the Verified by Visa™ service that enables an issuer to verify ownership of a portable consumer device during an online purchase. Once activated, a consumer can shop online at any participating online merchant using that portable consumer device and a password. Each time the consumer shops online at the participating merchant, he will see a Verified by Visa™ window. This window is used to allow the consumer to enter information that is authenticated by the issuer of the personal consumer device. After verifying the consumer's identity, the issuer creates and sends an authentication response to the merchant, who can thereafter decide to proceed or not proceed with the transaction.

[0004] These types of solutions help give consumers more confidence to make purchases over the Internet and also allow issuers, acquirers, and merchants to enjoy increased online transaction volumes and reduced exposure to fraud.

[0005] However, there are many business models that have emerged that are not conducive to prompting the consumer for a password each time the consumer makes a purchase online. For example, a consumer may have set up a recurring payment for a particular good or service so that the bills for these goods or services can be paid automatically each month, a consumer may regularly make small purchases (e.g., a micro-payment) such as buying songs online, or a merchant may have set up a one-step online payment so a regular consumer can simply click one button to make a purchase, instead of re-entering his billing information every time. These business models were designed specifically to save time and effort for the consumer, allowing the consumer to make a purchase in as few steps as possible. Merchants using these business models have been reluctant to adopt an authentication solution where they will be obligated to prompt the consumer for a password or other form of identification every time a purchase is made. Thus, a different solution is needed to authenticate consumers under these business models to ensure authentication and lower the risk of unauthorized use and fraud, but still allow for an easy and quick process for a consumer making a payment transaction.

[0006] Embodiments of the invention address these and other problems individually and collectively.

SUMMARY

[0007] Embodiments of the invention are directed to methods, systems, and computer readable media for allowing financial transactions to be conducted in a secure manner.

[0008] One embodiment of the invention is directed to a method comprising receiving a transaction message (e.g., a purchase message) relating to a request by a consumer to conduct a transaction (such as a purchase transaction) using a portable consumer device, wherein the consumer was previously enrolled in an authentication program and the consumer was previously authenticated, analyzing the transaction message to determine if a re-authentication event has taken place, causing a re-authentication message to be sent to the consumer before initiating an authorization request message to the issuer if the re-authentication event has taken place, and initiating the authorization request message to the issuer without sending

the re-authentication message to the consumer if the re-authentication event has not taken place.

[0009] Another embodiment of the invention is directed to a method comprising receiving a transaction message relating to a request by a consumer to conduct a transaction using a portable consumer device, analyzing the transaction message to determine if a re-authentication event has taken place, causing an authentication message to be sent to the consumer before initiating an authorization request message if the re-authentication event has taken place, and initiating the authorization request message without sending the authentication message to the consumer if the re-authentication event has not taken place, wherein the transaction uses a recurring payment, a micro-payment, or a one-step online payment.

[0010] Another embodiment of the invention is directed to a method comprising sending a transaction message to a website by a consumer using a portable consumer device, wherein the consumer was previously enrolled in an authentication program, receiving a re-authentication request for re-authentication information only if a re-authentication event has taken place, and sending re-authentication information in response to the re-authentication request.

[001 1] Other embodiments of the invention are directed to computer readable media comprising code for performing the above-described methods as well as systems, apparatuses and devices that perform the methods and/or that use the computer readable media.

[0012] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. 1(a) shows a block diagram of a system according to an embodiment of the invention.

[0014] FIG. 1(b) shows a block diagram of a computational apparatus that can be used in embodiments of the invention.

[0015] FIG. 2 shows a flowchart illustrating steps in a method according to an embodiment of the invention.

[0016] FIG. 3 shows an exemplary information request that prompts a consumer for credit card information.

[0017] FIG. 4 shows an exemplary information request that prompts a consumer for credit card and personal information.

[0018] FIG. 5 shows an exemplary information request that prompts a consumer to create a password.

[0019] FIG. 6 shows an exemplary information request that prompts a consumer for a password.

[0020] FIG. 7 shows an exemplary screen that informs a consumer that authentication failed.

DETAILED DESCRIPTION

[0021] Embodiments of the invention allow entities such as merchants, issuers, payment processing organizations, and/or third parties to re-authenticate a consumer after a consumer has attempted to conduct a transaction and after the consumer has enrolled in an authentication program. The transaction may be a type of transaction that would not normally require the consumer to be authenticated by providing a password or the like, because the type of transaction should either occur very quickly (as intended by a merchant), or because the transaction may occur without the user's active involvement (e.g., as in a recurring bill payment process).

[0022] Embodiments of the invention can allow a merchant, an issuer, a payment processing organization, a third party, or any combination of such entities to receive a purchase message relating to a request by a consumer to conduct a purchase transaction using a portable consumer device. The consumer may have been previously enrolled in an authentication program. The authentication program may be one in which the consumer is asked to re-authenticate himself (e.g., with a password) before conducting online transactions during normal transactions.

[0023] If a specialized transaction is conducted, then the consumer would be re-authenticated only if a re-authentication event has occurred. Specialized transactions include transactions that involve small payment amounts, recurring payments, and payments made in one-step transactions. Re-authentication in such situations may be inconvenient to consumers and/or may slow down the purchasing process.

[0024] After the purchase message is received, the purchase message is analyzed to determine if a re-authentication event has taken place. An example of a re-authentication event can be a change in home address. A re-authentication message is then sent to the consumer before initiating an authorization request message to the issuer if the re-authentication event has taken place.

[0025] If the re-authentication event has not taken place, then the process for sending the authorization request message to the issuer can be initiated.

[0026] Additional details regarding embodiments of the invention are described below.

[0027] FIG. 1(a) shows a system that can be used for conducting a payment transaction. For simplicity of illustration, one merchant, one issuer, one acquirer, one portable consumer device, and one consumer are shown. It is understood, however, that embodiments of the invention may include multiple merchants, acquirers, portable consumer devices, and/or consumers. In addition, some embodiments of the invention may include fewer than all of the components shown in FIG. 1(a). Also, the components in FIG. 1(a) may communicate via any suitable communication medium (including the Internet), using any suitable communication protocol.

[0028] The system 100 includes a merchant 20 and an acquirer payment processor 60 associated with the merchant 20. In a typical payment transaction, a consumer 10 may purchase goods or services at the merchant 20 using a portable consumer device 8. The acquirer payment processor 60 may be in operative communication with an issuer 80 of the portable consumer device 8 via a payment processing network 70. The merchant 20 can be in operative communication with an access control server 40 that is associated with (e.g., at or operated by) an issuer 80 via a

directory server 30. An authentication history server 50 may also be in operative communication with the access control server 40 at the issuer 80.

[0029] The acquirer payment processor 60 is typically a bank that has a merchant account. The issuer 80 may also be a bank, but could also be a business entity such as a retail store. Some entities are both acquirers and issuers, and embodiments of the invention include such entities.

[0030] The consumer 10 may be an individual, or an organization such as a business that is capable of purchasing goods or services. The consumer 10 may operate a client computer 10(a). The client computer 10(a) can be a desktop computer, a laptop computer, a wireless phone, a personal digital assistant (PDA), etc. It may operate using any suitable operating system including a Windows™ based operating system. Basic components of the client computer 10(a) are shown in FIG. 1(b).

[0031] The client computer 10(a) may utilize any suitable number of subsystems. Examples of such subsystems or components are shown in FIG. 1(b). The subsystems shown in FIG. 1(b) are interconnected via a system bus 775. Additional subsystems such as a printer 774, keyboard 778, fixed disk 779, monitor 776, which is coupled to display adapter 782, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 771 , can be connected to the computer system by any number of means known in the art, such as serial port 777. For example, serial port 777 or external interface 781 can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus 775 allows the central processor 773 to communicate with each subsystem and to control the execution of instructions from system memory 772 or the fixed disk 779, as well as the exchange of information between subsystems. The system memory 772 and/or the fixed disk 779 may embody a computer readable medium.

[0032] The portable consumer device 8 may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially

available form Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular phones, PDAs, pagers, payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be debit services (e.g., a debit card), credit devices (e.g., a credit card), or stored value devices (e.g., a stored value card).

[0033] The payment processing network 70 is located between (in an operational sense) the acquirer payment processor 60 and the issuer 80. It may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services. The payment processing network 70 may use any suitable wired or wireless network, including the Internet.

[0034] The merchant 20 may be associated with (e.g., may have or may operate) a merchant server computer 25 operating a website 25(a). A "server computer" as used herein, is typically a powerful computer or cluster of components. For example, the server computer 25, or any other server computer shown in FIG. 1 or elsewhere can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server.

[0035] The merchant 20 may have one or more additional access devices (not shown). Suitable access devices include interfaces and may include point of sale (POS) devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers (ECR), automated teller machines (ATM), virtual cash registers (VCR), kiosks, security systems, access systems, and the like. They can interact with portable consumer devices. For example, a consumer 10 using a credit card to purchase a good or service can swipe it through an appropriate slot in the POS terminal. Alternatively the POS terminal may be a contactless reader, and the portable consumer device 8

may be a contactless device such as a contactless card. As another alternative, a consumer 10 may purchase a good or service via a merchant's website where the consumer enters the credit card information into the client computer 10(a) and clicks on a button to complete the purchase. The client computer 10(a) may be considered an access device.

[0036] The website 25(a) may allow the consumer 10 to purchase goods or services offered by the merchant 20. The website 25(a) may include any suitable features. For example, it may be configured to provide for one-step online payment processing. An example of a one-step online payment process is the "one click" shopping process offered by Amazon.com. In another example, the website 25(a) may allow the consumer 10 to make recurring payments such as monthly payments for monthly invoices (e.g., utility invoices). In yet another example, the website 25(a) may allow for the purchase of items (e.g., songs) which may have low value (e.g., less than $5). An example of a suitable website 25(a) may be a website that allows for the purchase of music. This may be referred to as a micro-payment in some instances.

[0037] The merchant server 25 may also comprise a program such as a plug in. The plug in may be software which allows the server computer 25 to perform such functions as determining if the consumer's portable consumer device 8 is enrolled in an authentication program (e.g., by querying a directory server). The software may also allow the server computer 25 to determine if the current transaction is a specialized transaction (e.g., a one-step online payment transaction, a recurring payment transaction, or a transaction involving a micro-payment) or if it is a normal transaction. If the consumer 10 is not enrolled in the authentication program, then the transaction would proceed as it normally would in a conventional purchase transaction. If the consumer 10 is enrolled, but the transaction is not a specialized transaction, then the consumer 10 may be asked to re-authenticate himself via the consumer's client computer 10(a) whether or not a re-authentication event has occurred. If the consumer 10 is enrolled, but the transaction is a specialized transaction, then the consumer 10 may be asked to re-authenticate himself only if a re-authentication event has occurred. If the transaction is a specialized one and a re-authentication event has not occurred, then the consumer 10 would not be asked to re-authenticate himself. The merchant server 25 may comprise a computer

readable medium comprising computer code for performing any suitable permutation of these functions.

[0038] The merchant 20 may also be associated with a re-authentication event database 23, if the merchant 20 checks to see if re-authentication of the consumer 10 is needed. In the alternative embodiment, the re-authentication event database can reside at or otherwise be associated with the issuer 80, if the issuer 80 or some other entity (e.g., a third party) checks to see if re-authentication of the consumer 10 is needed.

[0039] FIG. 2 shows a flowchart including a general method according to an embodiment of the invention. The method can be described with reference to the block diagram in FIG. 1(a).

[0040] First, the consumer 10 enrolls in an authentication program. The authentication program may be run by any suitable entity including a payment processing organization, an issuer, a third party processor, etc.

[0041] The consumer 10 may want to enroll in the authentication program so that greater security is provided for the consumer 10 when the consumer 10 buys goods or services via the Internet. By enrolling in the authentication program, the consumer 10 will be prompted to re-authenticate himself before purchases can be made via the Internet. An exception to this would be if a specialized transaction (e.g., a one-step purchase process) is being conducted.

[0042] The consumer 10 may enroll in the authentication program before conducting a purchase transaction or during the purchase transaction using the client computer **10(a).** During the enrollment process, the consumer 10 may be asked to verify the consumer's identity, create a password, and enter an account number or other identifier associated with the portable consumer device 8. This information may then be stored in the directory server 30, or some other location.

[0043] Screenshots that the consumer 10 might see on the client computer **10(a)** during enrollment are shown in FIG. 3-5.

[0044] FIG. 3 shows a screenshot including data fields for the consumer to enter his or her name, address, type of portable consumer device, and account number.

[0045] FIG. 4 shows a screenshot including data fields for the consumer to enter the signature panel code associated with the consumer's portable consumer device, the last four digits of the consumer's social security number, the consumer's date of birth, and consumer's e-mail address. "Activate" and "Do Not Activate Now" buttons are shown. If the latter is selected, the entered data may be temporarily stored for later retrieval.

[0046] FIG. 5 shows a screenshot where the consumer can create a password. The consumer may be prompted to enter this password before proceeding with future transactions that are normal. As explained below, the consumer would not be prompted for the password if the transaction is a specialized one and no re-authentication event has occurred. If a re-authentication event has occurred, then the consumer would be prompted to re-authenticate himself by entering a password.

[0047] After the consumer is enrolled in the authentication program, the consumer 10 purchases a good or service from the merchant 20 using a portable consumer device 8 such as a credit card and a client computer 10(a) (step 800). The consumer 10 can interact with the merchant 20 and merchant server 25 through a website 25(a). For example, the website 25(a) can sell downloadable songs. The consumer 10 can select songs to purchase and may be prompted be asked if the consumer 10 wants to purchase selected songs for a fee (e.g., $1.00 per song).

[0048] Regardless of what type of purchase is being conducted, a purchase message is sent from client computer 10(a) operated by the consumer 10, to the merchant website 25(a) and consequently the merchant 20. The purchase message may include any suitable information that might be sent to a merchant during a typical Internet purchase transaction. For example, the purchase message may include information relating to the amount of the purchase, the item being purchased, and identifying information such as the consumer's account number (e.g., credit card number), an IP address of the client computer 10(a) being used by the consumer 10, etc.

[0049] Upon receiving the purchase message from a consumer 10, the merchant 20 identifies the identifying information for the portable consumer device 8 in the purchase message, such as a credit card account number (step 805). Other types of information identifying the portable consumer device 8 could be used in other

embodiments of the invention. For example, the identifying information could additionally or alternatively include the consumer's name, the expiration date of the portable consumer device 8, a verification value such as a card verification value, etc.

[0050] After the merchant server computer 25 receives and identifies the identifying information for the portable consumer device 8, it analyzes the identifying information. As described below, the merchant server computer **25** may then cause, either directly or indirectly, a re-authentication message to be sent to the consumer 10 if the purchase transaction is a specialized one, and if a re-authentication event has occurred. It may then initiate (either directly or indirectly) the sending of an authorization request message to the issuer **80.**

[0051] In one embodiment, if the merchant's website **25(a)** conducts both specialized transactions (e.g., a one-step online payment transaction, a recurring payment transaction, or a transaction involving a micro-payment) or normal transactions, the merchant 20 may then determine if the current transaction is a specialized transaction (e.g., a one-step online payment transaction, a recurring payment transaction, or a transaction involving a micro-payment) or if it is a normal transaction. If it is a normal transaction, then the consumer 10 would be asked to re-authenticate himself as he would in a conventional re-authentication program. If it is a specialized transaction, then the purchase transaction may continue to proceed as shown in FIG. 2. Note that if the website **25(a)** only conducts specialized transactions (e.g., a website that sells music and only conducts micro-payments), then the method does not need to determine of the transaction is a normal one or a specialized one.

[0052] If the transaction is a specialized transaction and the consumer 10 is enrolled in the authentication program, then the merchant server 25 determines if a re-authentication event has occurred by analyzing the purchase message against the re-authentication events in a re-authentication event database 23 (step **810).** "Re-authentication events" may include an event that can indicate the potential for fraudulent activity such as a new consumer completing her first purchase, significant account changes, and orders that are perceived to be a higher-risk. For example, a re-authentication event can include a change in the consumer's home address,

shipping address, billing address, email address, name, account number, payment method, portable consumer device expiration date, or password. Other examples of re-authentication events include: different or new IP addresses, out of pattern activities (e.g., jewelry purchases where the consumer does not normally buy jewelry), order amounts above a specified dollar amount (e.g., greater than $1000.00), a long period of inactivity in the account (e.g., at least one month, or twelve months), orders for particular types of goods (e.g., furniture, clothing, jewelry, or consumer electronics such as laptop computers, big screen TVs, etc.), authentication failures or attempts (e.g., a consumer fails to provide a password or other identifier in a prior transaction), changes in payment terms, instances where authentication attempts have failed more than a pre-determined number of times in the past, or where authentication occurred more than a pre-set amount of time in the past. A list of such events may be stored in the re-authentication database 23.

[0053] If a re-authentication event has occurred, the merchant 20, using the merchant server 25, sends the identifying information and optionally other information to the directory server 30. The directory server 30 may determine which issuer issued the portable consumer device 8. After the directory server 30 determines the issuer, the directory server 30 determines if the identified issuer participates in the authentication program. If the issuer does participate, the directory server 30 determines whether or not the consumer 10 and the portable consumer device 8 are enrolled in the authentication program (step 815). For example, if the issuer 80 of the portable consumer device 8 participates in the authentication program, then the directory server 30 sends a request to the access control server 40 of the issuer 80 to determine whether or not the portable consumer device 8 is enrolled in the authentication program.

[0054] The consumer 10 may be asked if he wants to enroll in the authentication program during the transaction (step 820). If the portable consumer device 8 and/or the consumer 10 are not enrolled, the merchant server 25 receives a message from the access control server 40 via the directory server 30 that the portable consumer device 8 and/or the consumer 10 are not enrolled or that authentication is not available. The merchant server 25 then proceeds with a standard transaction processing (steps 845, 850, 855, described below). If the portable consumer device

8 is enrolled in the authentication program, the access control server 40 returns a response to the directory server 30 indicating this.

[0055] The directory server 30 then forwards the response to the merchant server 25. After the merchant server 25 receives the response, the merchant server 25 sends an authentication request message to the to the client computer 10(a) for routing to the access control server 40. Alternatively, the authentication request message may be sent directly to the access control server 40 or the authentication request message may be sent to the directory server 30 for routing to the access control server 40.

[0056] The access control server 40 then authenticates the consumer 10 by sending a re-authentication request message to the client computer 10(a) operated by the consumer 10. After the re-authentication request message is received by the client computer 10(a), the client computer 10(a) displays information about the particular purchase to be authenticated and prompts the consumer 10 to enter his re-authentication information (step 825). Re-authentication information may be any identifying information such as a password, a card verification value, a full or partial social security number, the consumer's date of birth, and/or the consumer's email address. An exemplary screenshot of what the consumer 10 might see on the client computer 10(a) is shown in FIG. 6. After seeing a screenshot like the one shown in FIG. 6 on the client computer 10(a), the consumer 10 enters his password (or other identifier) into the client computer 10(a). The client computer 10(a) then sends the password to the access control server 40. The password is received by the access control server 40 and it verifies the password. The access control server 40 creates, digitally signs, and sends an authentication response to the merchant server 25. The access control server 40 also sends a transaction record to the authentication history server 50 for storage.

[0057] If the consumer 10 is unable to correctly enter the correct password, the consumer 10 is notified that he cannot be authenticated (step 830). A message indicating this may be sent from the access control server 40 to the client computer 10(a). An exemplary screen shot that a consumer might see is shown in FIG. 7.

[0058] An authentication response message indicating that the consumer 10 failed authentication may then be sent from the access control server 40, to the client

computer 10(a), and then to the merchant server 25. Alternatively, the authentication response message indicating that the consumer 10 failed authentication may be sent from the access control server 40, to the directory server 30, and then to the merchant server 25. If the merchant 20 receives a "Failed" authentication response from the access control server 40, the merchant 20 can proceed with the purchase, request another form of payment from the consumer 10 or decline the transaction (step 865). This supplemental payment request may be sent from the merchant server 25 to the client computer 10(a).

[0059] If the consumer 10 successfully re-authenticates himself by entering the correct password into the client computer 10(a), the access control server 40 may send an authentication response message back to the merchant server 25 via the client computer 10(a) or via the directory server 30 after receiving the correct password. The merchant server 25 then verifies that the digital signature is from a valid participating issuer 80 (step 840). If the digital signature is verified and the issuer's authentication response contains a message indicating successful authentication (e.g., an "Approved" message), then the merchant server 25 sends an authorization request message which includes a request to authorize the purchase transaction, to the acquirer payment processor 60. The authorization request message may include information including the amount of the purchase, the expiration date of the portable consumer device 8, the PAN (personal account number), and other information. It may also include information about the issuer's authentication response.

[0060] The acquirer payment processor 60 receives the authorization request from the merchant 20 and sends an authorization request to the payment processing network 70 (step 845). The payment processing network 70 then transmits the authorization request received from the acquirer payment processor 60 to the issuer 80 (step 850). The issuer 80 receives the authorization request containing additional authentication information and processes the transaction (step 855). The issuer 80 may choose to decline the authorization request for reasons unrelated to the authentication (e.g., insufficient funds or insufficient credit available to make the requested purchase).

[0061] An authorization response is returned to the acquirer payment processor 60 through the payment processing network 70 by the issuer 80. The acquirer payment processor 60 then returns the authorization response to the merchant 20. If the payment transaction is not authorized, the merchant 20 declines the transaction or requests another form of payment from the consumer 10 (step 865). If the payment transaction is authorized, the merchant 20 notifies the consumer 10 that the transaction is complete (step 860).

[0062] In an alternative embodiment, a re-authentication event database 23 can reside at the issuer 80. In this example, upon receiving a purchase message from the consumer 10, the merchant 20 analyzes the payment message against the re-authentication events in a re-authentication event database (not shown) at the issuer 80 via a directory server 30 (step 810). The steps outlined in FIG. 2 from this point forward are the same as described above.

[0063] Embodiments of the invention have a number of advantages. For example, embodiments of the invention can allow specialized payment transactions such as micro-payments, recurring payments, and payments made according to one-step processing to occur without re-authentication of the consumer. This makes it easier for the consumer to conduct such specialized payment transactions, and this increases transaction volume for the merchant. If, however, a re-authentication event that may indicate potential fraud occurs, the consumer can be asked to re-authenticate himself before the transaction can proceed. Thus, embodiments of the invention advantageously provide security for online transactions in appropriate situations, without impeding the progress of transactions where re-authentication may slow down a transaction or may be inconvenient to a consumer.

[0064] Although the examples described above specifically relate to embodiments where transactions occur online, it is understood that embodiments of the invention could also use other modes of communication including the mail and telephones (e.g., as in telephone orders using interactive voice response units) and in a physical store (e.g., at the physical point of sale). In addition, although purchase transaction are described in detail, embodiments of the invention may also be used for transactions such as money transfer transactions (e.g., between individuals and businesses).

[0065] It should be understood that 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 the present invention using hardware and a combination of hardware and software.

[0066] 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, 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.

[0067] The above description is illustrative and is not restrictive. Many variations of the invention 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.

[0068] 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.

[0069] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving a transaction message relating to a request by a consumer to conduct a transaction using a portable consumer device, wherein the consumer was previously enrolled in an authentication program and the consumer was previously authenticated;

analyzing the transaction message to determine if a re-authentication event has taken place;

causing a re-authentication message to be sent to the consumer before initiating an authorization request message to the issuer if the re-authentication event has taken place; and

initiating the authorization request message to the issuer without sending the re-authentication message to the consumer if the re-authentication event has not taken place.

2. The method of claim 1, wherein the transaction is a purchase transaction.

3. The method of claim 1, wherein the re-authentication event is a change in the consumer's home address, shipping address, billing address, email address, name, account number, payment method, portable consumer device expiration date, or password, and wherein the consumer was previously authenticated to an issuer of the portable consumer device.

4. The method of claim 1, wherein the re-authentication event is a new or different IP address, an out of pattern activity, an order amount above a specified dollar amount, or a long period of inactivity in the account.

5. The method of claim 1, wherein the re-authentication event is where a previous transaction was an authentication failure or attempt.

6. The method of claim 1, wherein the re-authentication event is a change in payment terms.

7. The method of claim 1, wherein the re-authentication event is where authentication occurred more than a pre-set amount of times in the past and have failed.

8. The method of claim 1 wherein the transaction is a purchase transaction and involves a recurring payment, a micro-payment, or a one-step online payment.

9. The method of claim 1 further comprising:

sending an authentication message to a merchant, wherein the merchant thereafter sends an authorization request message to the issuer and the issuer thereafter returns an authorization response message back to the merchant.

10. The method of claim 1 wherein the portable consumer device is in the form of a card.

11. A method comprising:

sending a transaction message to a website by a consumer using a portable consumer device, wherein the consumer was previously enrolled in an authentication program;

receiving a re-authentication request for re-authentication information only if a re-authentication event has taken place; and

sending re-authentication information in response to the re-authentication request.

12. The method of claim 11, wherein the re-authentication information is selected from the group consisting of a password, a card verification value, a social security number, the consumer's date of birth, and the consumer's email address.

13. A computer readable medium comprising:

code for sending a transaction message to a website by a consumer using a portable consumer device, wherein the consumer was previously enrolled in an authentication program;

code for receiving a re-authentication request for re-authentication information only if a re-authentication event has taken place; and

code for sending re-authentication information in response to the re-authentication request.

14. A client terminal comprising the computer readable medium of claim 13.

15. A computer readable medium comprising:

code for receiving a transaction message relating to a request by a consumer to conduct a transaction using a portable consumer device, wherein the consumer was previously enrolled in an authentication program and the consumer was previously authenticated;

code for analyzing the transaction message to determine if a re-authentication event has taken place;

code for causing a re-authentication message to be sent to the consumer before initiating an authorization request message to the issuer if the re-authentication event has taken place; and

code for initiating the authorization request message to the issuer without sending the re-authentication message to the consumer if the re-authentication event has not taken place.

16. A server computer comprising the computer readable medium of claim 15.

17. A computer readable medium comprising:

code for receiving a transaction message relating to a request by a consumer to conduct a transaction using a portable consumer device;

code for analyzing the transaction message to determine if a re-authentication event has taken place;

code for causing an authentication message to be sent to the consumer before initiating an authorization request message if the re-authentication event has taken place; and

code for initiating the authorization request message without sending the authentication message to the consumer if the re-authentication event has not taken place, wherein the transaction is one of a recurring payment, a micro-payment, or a one-step online payment.

18. A server computer comprising the computer readable medium of claim 17.

19. A method comprising:

receiving a transaction message relating to a request by a consumer to conduct a transaction using a portable consumer device;

analyzing the transaction message to determine if a re-authentication event has taken place;

causing an authentication message to be sent to the consumer before initiating an authorization request message if the re-authentication event has taken place; and

initiating the authorization request message without sending the authentication message to the consumer if the re-authentication event has not taken place, wherein the transaction uses at least one of a recurring payment, a micro-payment, or a one-step online payment.

20. A computer readable medium comprising code for performing the method of claim 19.

21. A server computer comprising the computer readable medium of claim 20.

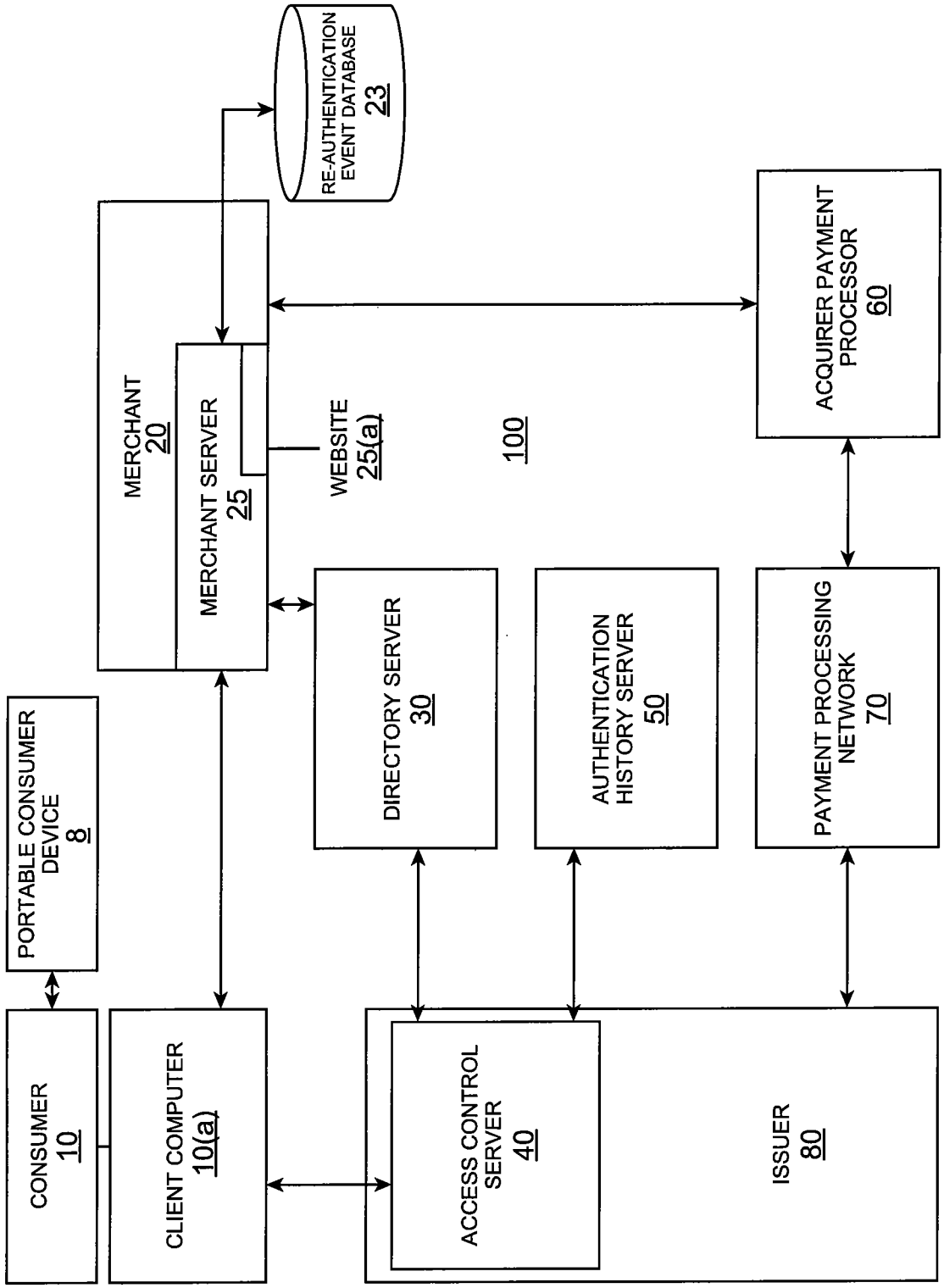

RE-AUTHENTICATION EVENT DATABASE 23
MERCHANT 20
MERCHANT SERVER 25
WEBSITE 25(a)
100
ACQUIRER PAYMENT PROCESSOR 60
PORTABLE CONSUMER DEVICE 8
DIRECTORY SERVER 30
AUTHENTICATION HISTORY SERVER 50
PAYMENT PROCESSING NETWORK 70
CONSUMER 10
CLIENT COMPUTER 10(a)
ACCESS CONTROL SERVER 40
ISSUER 80

FIG. 1(a)

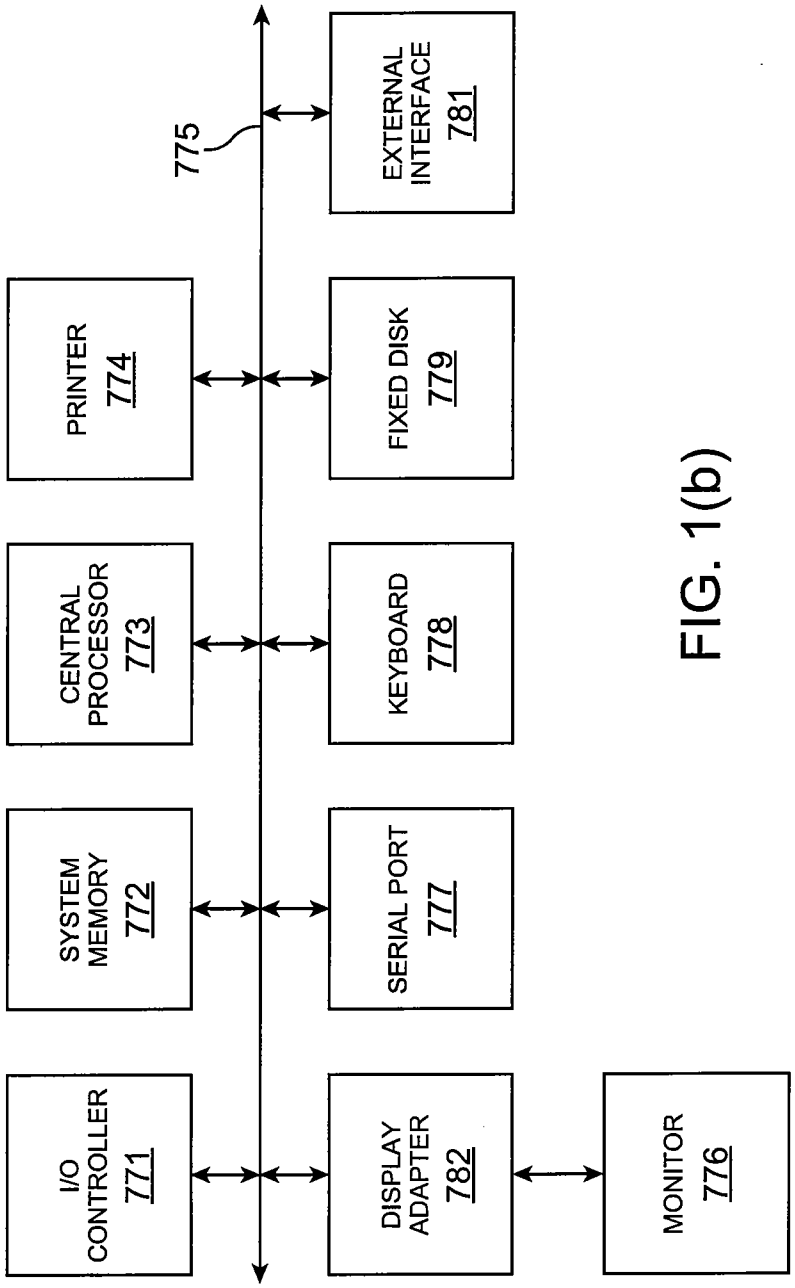

I/O CONTROLLER 771
SYSTEM MEMORY 772
CENTRAL PROCESSOR 773
PRINTER 774
775
DISPLAY ADAPTER 782
SERIAL PORT 777
KEYBOARD 778
FIXED DISK 779
MONITOR 776
EXTERNAL INTERFACE 781

FIG. 1(b)

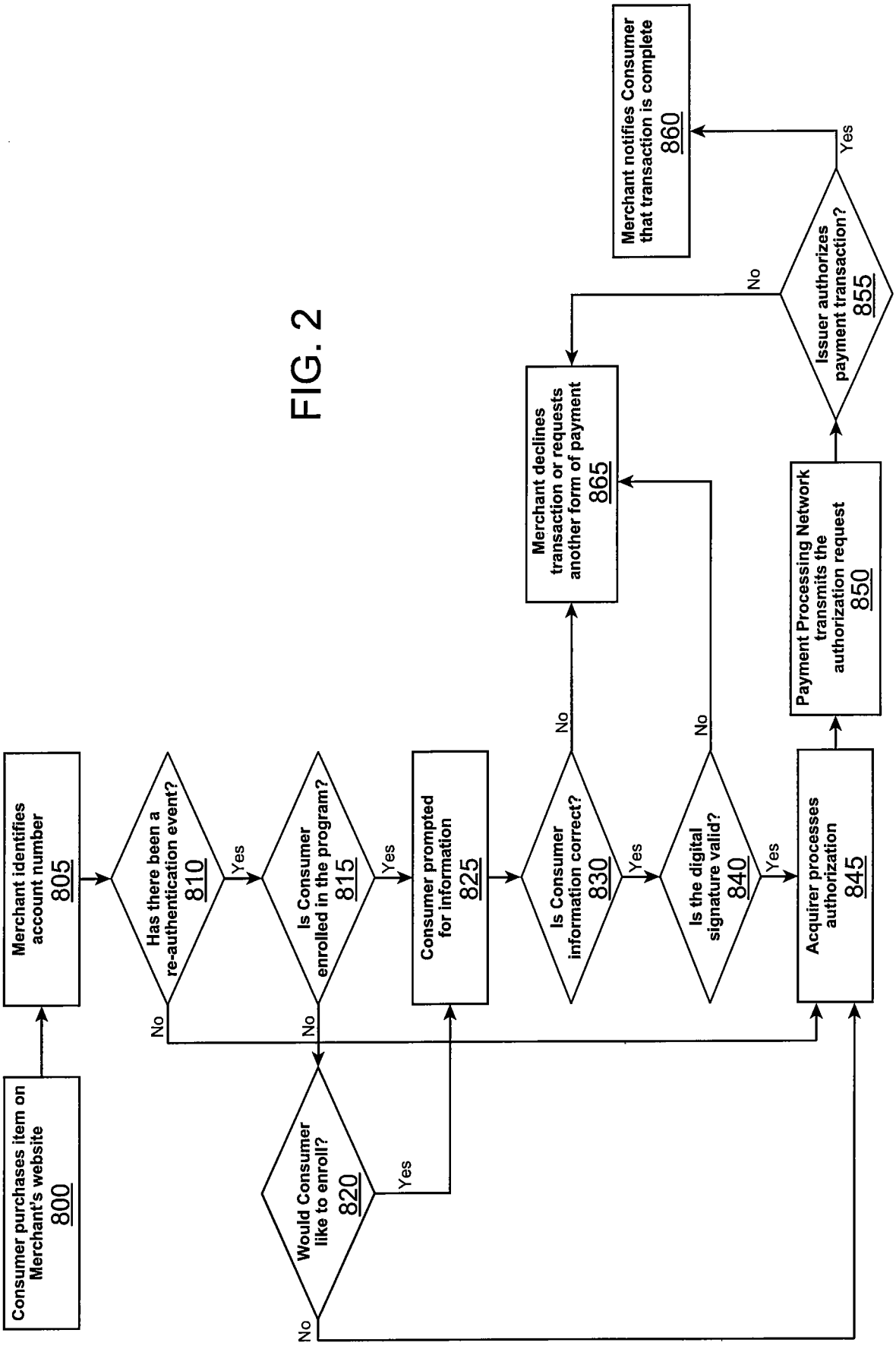

Consumer purchases item on Merchant's website 800
Merchant identifies account number 805
Has there been a re-authentication event? 810
Is Consumer enrolled in the program? 815
Would Consumer like to enroll? 820
Consumer prompted for information 825
Is Consumer information correct? 830
Is the digital signature valid? 840
Acquirer processes authorization 845
Payment Processing Network transmits the authorization request 850
Issuer authorizes payment transaction? 855
Merchant notifies Consumer that transaction is complete 860
Merchant declines transaction or requests another form of payment 865
Yes
No

FIG. 2

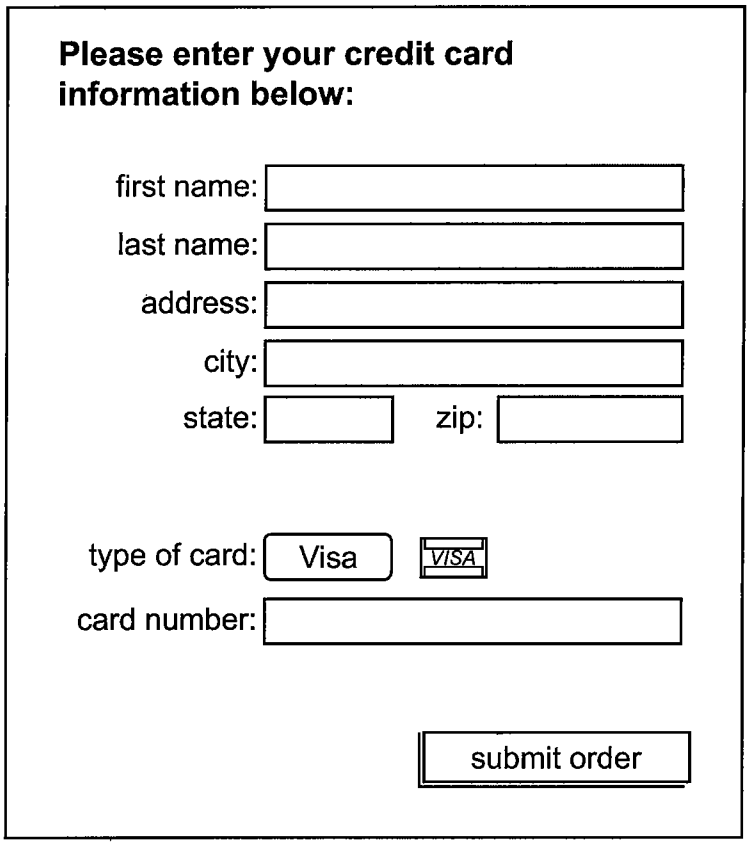

Please enter your credit card information below:
first name:
last name:
address:
city:
state:
zip:
type of card:
Visa
VISA
card number:
submit order

FIG. 3

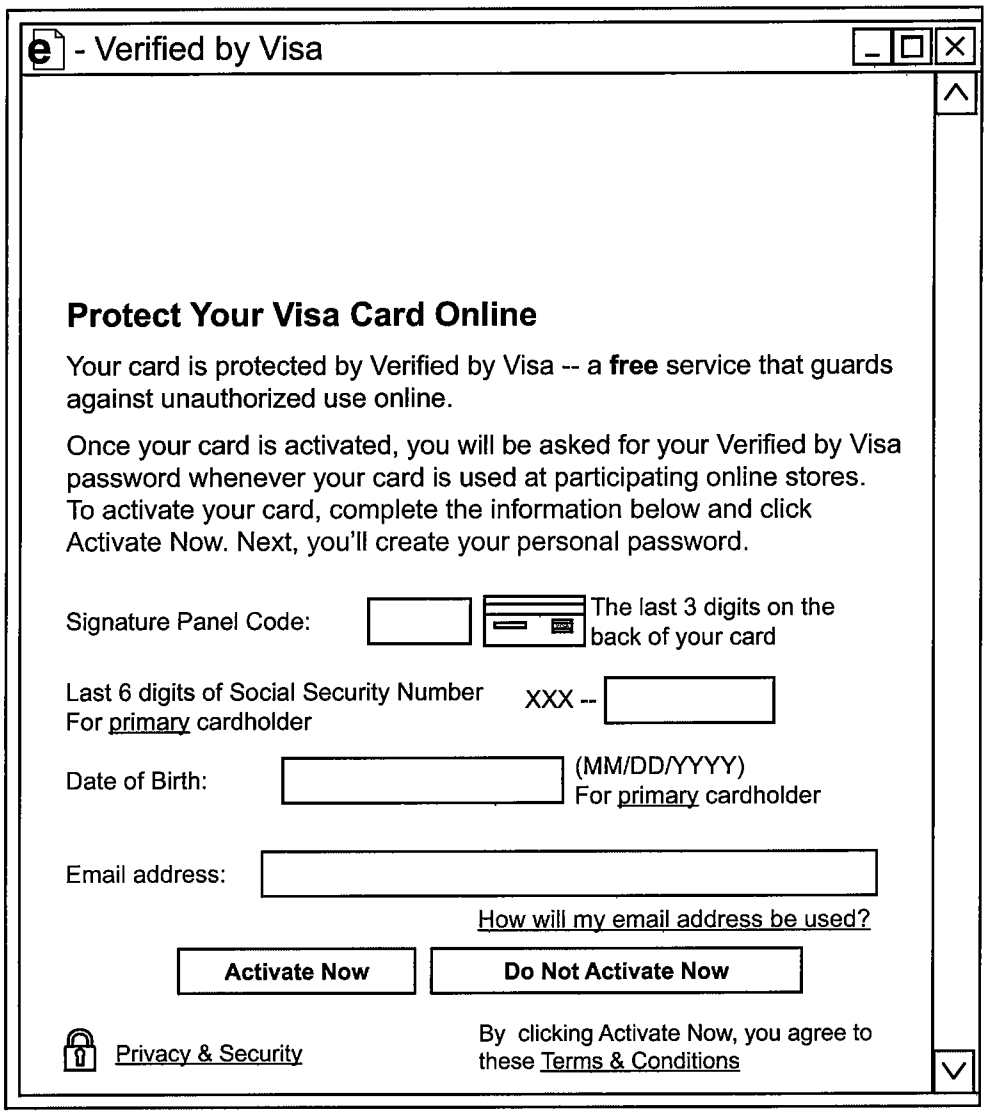

- Verified by Visa
Protect Your Visa Card Online
Your card is protected by Verified by Visa -- a free service that guards against unauthorized use online.
Once your card is activated, you will be asked for your Verified by Visa password whenever your card is used at participating online stores. To activate your card, complete the information below and click Activate Now. Next, you'll create your personal password.
Signature Panel Code:
The last 3 digits on the back of your card
Last 6 digits of Social Security Number For primary cardholder
XXX --
Date of Birth:
(MM/DD/YYYY) For primary cardholder
Email address:
How will my email address be used?
Activate Now
Do Not Activate Now
Privacy & Security
By clicking Activate Now, you agree to these Terms & Conditions

FIG. 4

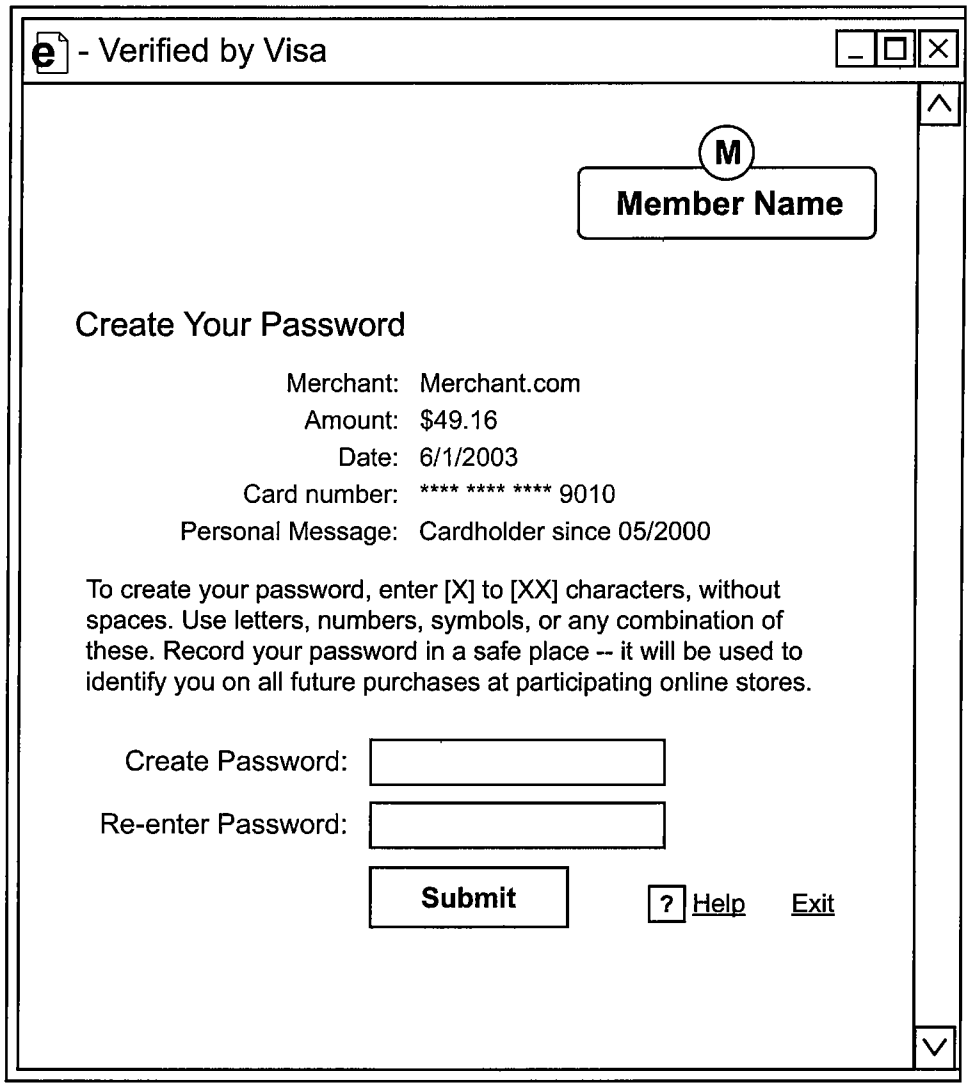

- Verified by Visa
M
Member Name
Create Your Password
Merchant: Merchant.com
Amount: $49.16
Date: 6/1/2003
Card number: **** **** **** 9010
Personal Message: Cardholder since 05/2000
To create your password, enter [X] to [XX] characters, without spaces. Use letters, numbers, symbols, or any combination of these. Record your password in a safe place -- it will be used to identify you on all future purchases at participating online stores.
Create Password:
Re-enter Password:
Submit
? Help
Exit

FIG. 5

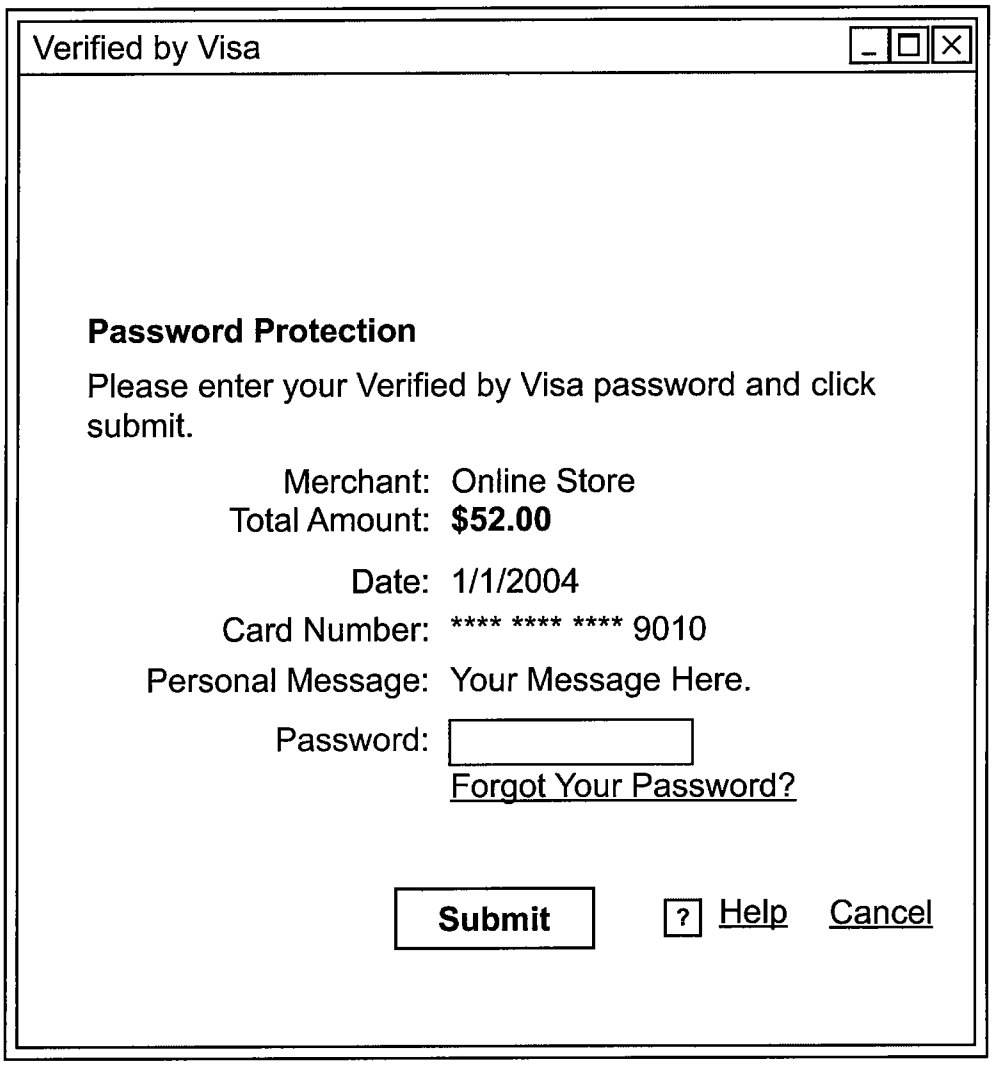

Verified by Visa
Password Protection
Please enter your Verified by Visa password and click submit.
Merchant: Online Store
Total Amount: $52.00
Date: 1/1/2004
Card Number: **** **** **** 9010
Personal Message: Your Message Here.
Password:
Forgot Your Password?
Submit
Help
Cancel

FIG. 6

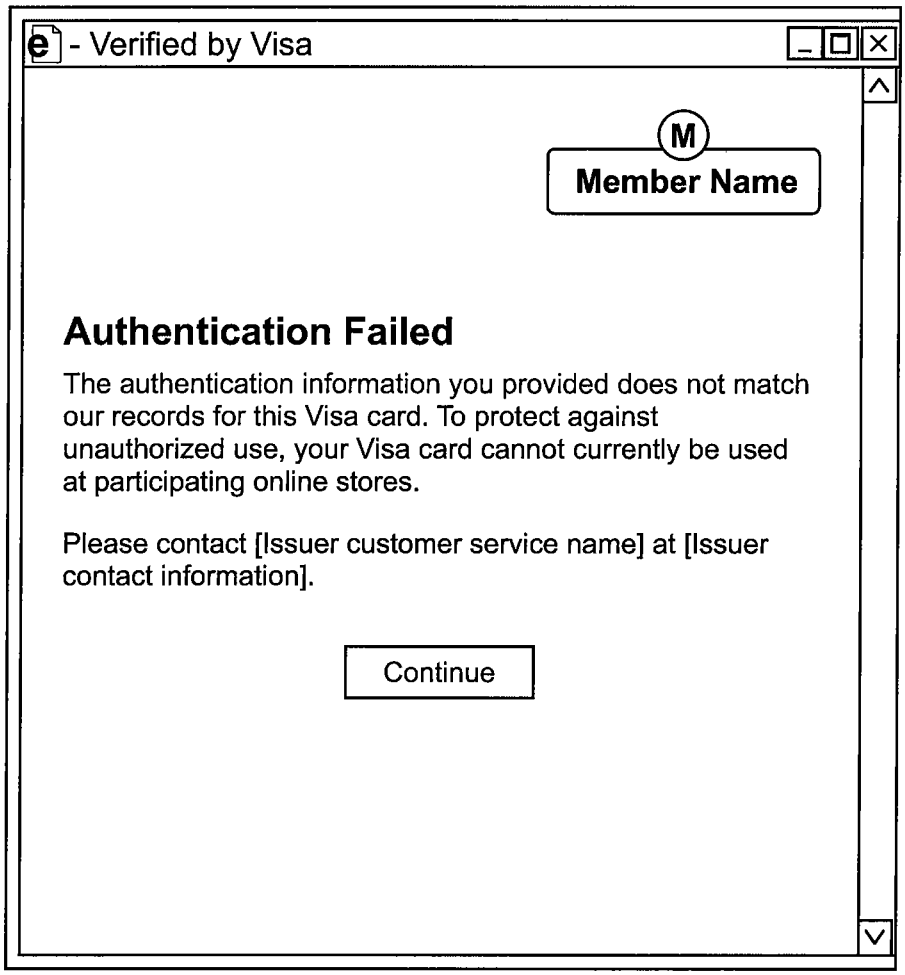

- Verified by Visa
M
Member Name
Authentication Failed
The authentication information you provided does not match our records for this Visa card. To protect against unauthorized use, your Visa card cannot currently be used at participating online stores.
Please contact [Issuer customer service name] at [Issuer contact information].
Continue

FIG. 7