



- (51) **International Patent Classification:**
G06Q 20/40 (2012.01) *G06Q 20/12* (2012.01)
- (21) **International Application Number:**
PCT/US2012/048406
- (22) **International Filing Date:**
26 July 2012 (26.07.2012)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/513,337 29 July 2011 (29.07.2011) US
13/559,250 26 July 2012 (26.07.2012) US
- (71) **Applicant (for all designated States except US):** VISA INTERNATIONAL SERVICE ASSOCIATION [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).
- (72) **Inventors; and**
- (75) **Inventors/Applicants (for US only):** McCULLAGH, Ni-all [IE/GB]; 19 Fairview Road, Plumbridge Omagh, Co. Tyrone BT79 8DY (GB). CUSHLEY, Seamus [IE/GB]; 55A Broagh Road, Castledawson Derry, Co. Londonderry, BT45 8ER (GB).
- (74) **Agents:** ANNIS, David et al.; Kilpatrick Townsend & Stockton 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, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, 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, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, 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:** PASSING PAYMENT TOKENS THROUGH AN HOP/SOP

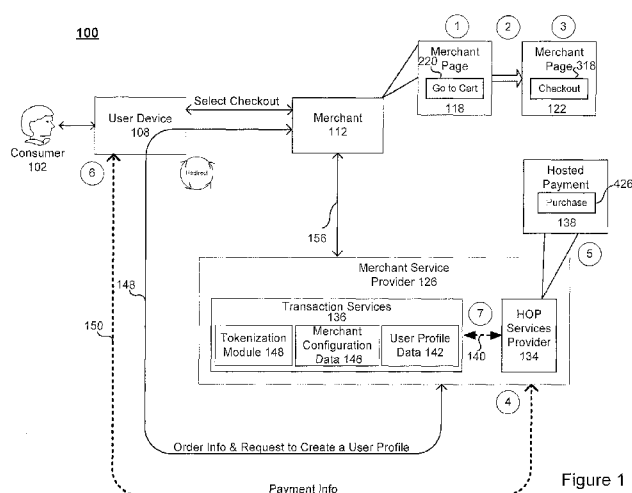


Figure 1

(57) **Abstract:** Embodiments of the invention are directed to methods, a computer-readable medium, servers and systems for enabling merchants to pass payment tokens, instead of actual payment information, to third party HOPs and SOPs. This, for example, enables a merchant to charge a consumer, such as on a recurring basis or for a one-off purchase, without having the consumer enter payment information each time and without the merchant actually having to handle payment information. As such, merchants can avoid costs and responsibilities associated with handling and storing consumer payment data, while at the same time it also gives merchants the benefit of engaging in purchase transactions with consumers without requiring that the consumers reenter payment data each time they want to make a purchase.

PASSING PAYMENT TOKENS THROUGH AN HOP / SOP

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application is a continuation of and claims the benefit of U.S. Application No. 13/559,250, filed July 26, 2012, which claims the benefit of U.S. Provisional Application No. 61/513,337, filed July 29, 2011. The above applications are hereby incorporated by reference in their entireties for all purposes.

BACKGROUND

[0002] 1. Field of the Art

[0003] Generally, payment processing for online retail businesses is described. Specifically, third party-assisted tokenization and payment processing are described.

[0004] 2. Discussion of the Related Art

[0005] A “hosted order page” (HOP) is a third-party hosted webpage that accepts payment information from customers on behalf of merchants. A merchant website typically redirects a customer to an HOP on the third-party’s domain/server when the customer selects a ‘Buy’ or ‘Checkout’ button from an online shopping cart. Once at the HOP, the customer inputs payment information, such as credit card information. The third-party, which is neither the merchant nor the customer, uses the payment information entered by the customer to process the purchase transaction for the merchant so that the merchant can avoid handling the customer’s payment information, and thereby avoid the cost and effort of complying with the Payment Card Industry Data Security Standard (PCI DSS) and government regulations regarding storing sensitive payment information.

[0006] A “silent order post” (SOP) is akin to an HOP but with only the sensitive textboxes and other input controls being hosted by the third party. That is, the merchant hosts the order page but the sensitive fields, such as the credit card number and expiration date entry textboxes, are posted only to the third party’s servers.

[0007] Oftentimes, online merchants enable consumers to create an account/profile on the merchant’s webserver and store their payment information (e.g., credit-card

information) in the account/profile. This way, instead of the consumers having to enter payment information each time they want to make a purchase from the merchant's website, the merchant can use the stored payment information to process the transaction. Also, for example, merchants use stored payment information to charge consumers on a recurring basis. For example, an online newspaper publisher may charge its subscribers once per month.

[0008] Merchants that utilize an HOP / SOP and therefore do not store or have access to consumers' payment information cannot charge consumers, either for one-time or recurring payments, without instructing the consumers to input their payment information each time. Requesting consumers to input their payment information each time the consumer wants to make a purchase or each time a recurring payment needs to be made can be burdensome to consumers and could result in missed sales opportunities and consumers delaying or missing payments.

BRIEF SUMMARY

[0009] Embodiments of the invention are directed to methods, a computer-readable medium, servers and systems for enabling merchants to pass payment tokens, instead of actual payment information, to third party HOPs and SOPs. This, for example, enables merchants to charge consumers, such as on a recurring basis or for a one-off purchase, without having the consumer enter payment information each time and without the merchant actually having to handle payment information and therefore incur costs associated with PCI compliance.

[0010] An example will now be provided for the purpose of illustrating embodiments of the invention. This example will be provided in the context of a consumer purchasing an item from a merchant website. The example generally begins with the consumer identifying an item of interest on the merchant's website. Upon identifying the item of interest, the consumer clicks on a link associated with the item and thereby navigates to a page on the merchant website that provides details about the item, along with an "Add to Cart" button. The user selects the "Add to Cart" button and causes the merchant to add the item to a virtual cart. The user then selects a "Go to Cart" button and thereby navigates to the virtual cart. The virtual cart displays order information, which includes a summary description of the item as well as line item data, such as quantity, price, taxes, shipping costs, etc. The virtual cart also prompts the consumer to create an account with the merchant. For example, the

virtual cart may have a checkbox that the consumer can select to indicate that the consumer would like to create an account and/or the virtual cart may prompt the user to provide his name, email address and/or userID, and a password for the purpose of creating new account.

[0011] After checking the box and/or providing account information, the user selects a "Checkout" or "Submit" button. In response, the merchant redirects the consumer to an HOP that is provided by a merchant service provider for payment authorization. In doing so, the merchant sends the authorization request and order information along with a request to create an account for the consumer to the merchant service provider. The request for the merchant service provider to create an account for the consumer is sometimes referred to herein as a subscription request. The order information, the authorization request, and the request to create an account may be sent to the merchant service provider in the form of an HTML post, for example. The HOP, which is provided by the merchant service provider, displays a payment page to the consumer. The payment page renders the order information and prompts the consumer to input his payment information, such as credit card or e-check information. The merchant service provider then creates an account for the consumer on the merchant service provider's database, stores the payment information in the user account, tokenizes the payment information, stores a payment token that results from the tokenization in the user account, and then sends a copy of the payment token back to the merchant.

[0012] The merchant stores the copy of the payment token on the merchant's database. For example, the merchant creates an account for the user on the merchant's database and stores the payment token in the user's account. In future transactions with the consumer, the merchant can pass the payment token through the HOP to the merchant service provider. This enables the merchant to avoid requesting the consumer to input payment information. After the merchant passes the payment token through the HOP to the merchant service provider, the merchant service provider accesses the consumer's account on the merchant service provider's database and verifies the payment token received from the merchant against the payment token stored in the merchant service provider's database. If the payment token is verified, the merchant service provider uses the payment information stored on the merchant service provider's database to process the purchase transaction on behalf of the merchant.

[0013] For example, if the consumer signs up for a subscription (e.g., online newspaper subscription) with the merchant that involves recurring payment, the merchant can simply pass the payment token associated with the consumer to the HOP each time a payment is due, and thereby cause the merchant service provider to process the payment. Also for example, when the consumer visits the merchant website in the future to purchase one or more items, the merchant can pass the consumer's payment token to the merchant service provider and avoid prompting the consumer to enter his payment information. Embodiments of this invention provide the advantage of, for example, being able to utilize an HOP and avoid having to store or have access to consumers' payment information, while at the same time avoid the need for consumers to input their payment information each time a payment needs to be processed.

[0014] An embodiment relates to a method comprising receiving order information and a request to create an account from a merchant, the order information associated with a purchase transaction between a user and the merchant, the account being for the purpose of storing payment information of the user at the merchant service provider, rendering a hosted payment page on behalf of the merchant, the hosted payment page presenting to the user at least a portion of the order information and at least an input field into which the user may input the payment information, receiving the payment information from the user, processing the purchase transaction between the user and the merchant using the payment information, creating an account for the user if the user does not already have an account, tokenizing the payment information so as to create a payment token, storing the payment information and the payment token in the account, and sending a copy of the payment token to the merchant, the merchant being able to submit the payment token in future purchase transactions between the merchant and the user, thereby eliminating the need for the user to resubmit the payment information in future purchase transactions between the merchant and the user.

[0015] Another embodiment relates to a method comprising receiving, at a merchant service provider, order information and a request to create an account from a merchant server of a merchant, the order information associated with a purchase transaction between a user and the merchant, the account being for the purpose of storing payment information of the user at the merchant service provider, receiving, at the merchant service provider, payment information from the user who

is engaging in the purchase transaction with the merchant, wherein the payment information is sent to the merchant service provider from a device associated with the user and wherein the payment information bypasses the merchant server, creating, at the merchant service provider, an account for the user, storing, at the merchant service provider, the payment information of the user in the account of the user, tokenizing, at the merchant service provider, the payment information in the account of the user so as to create a payment token that represents the payment information of the user, and transmitting, from the merchant service provider, a copy of the payment token to the merchant server.

[0016] Another embodiment relates to a system comprising a processor, a memory device including instructions that, when executed by the processor, cause the processor to: receive from a merchant server of a merchant order information and a request to create an account, the order information associated with a purchase transaction between a user and the merchant, the account being for the purpose of storing payment information of the user at the merchant service provider; receive payment information from the user who is engaging in the purchase transaction with the merchant, wherein the payment information is sent to the merchant service provider from a device associated with the user and wherein the payment information bypasses the merchant server; create an account for the user; store the payment information of the user in the account of the user; tokenize the payment information in the account of the user so as to create a payment token that represents the payment information of the user; and transmit a copy of the payment token to the merchant server.

[0017] 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.

[0018] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] Figure 1 provides a block diagram of an example operating environment in which embodiments of the invention can be implemented.

[0020] Figure 2 provides an illustration of an example merchant webpage, according to an embodiment.

[0021] Figure 3 provides an illustration of an example merchant webpage, according to an embodiment.

[0022] Figure 4 provides an illustration of an example hosted order webpage, according to an embodiment.

[0023] Figure 5 provides a flow diagram of an example process for enabling a merchant to send order information along with a request to create an account for a user to a merchant service provider, according to an embodiment.

[0024] Figure 6 provides a flow diagram of an example process for enabling a merchant service provider to obtain payment information from a user, according to an embodiment.

[0025] Figure 7 provides a flow diagram of an example process for enabling a merchant service provider to create an account for a user, save the user's payment information in the account, and tokenize the user's payment information, according to an embodiment.

[0026] Figure 8 provides a flow diagram of an example process for enabling a merchant to pass payment tokens – instead of actual payment information – to an HOP / SOP provided by a merchant service provider, according to an embodiment.

[0027] Figure 9 provides a block diagram of an example operating environment in which embodiments of the invention can be implemented.

[0028] Figure 10 provides an illustration of an example webpage having hosted input fields, according to an embodiment.

[0029] Figure 11 provides a block diagram of a transaction processing system that may be used with some embodiments of the present invention.

[0030] Figure 12 provides a block diagram of an exemplary computer system in which various embodiments can be implemented.

DETAILED DESCRIPTION

[0031] Embodiments of the invention are directed to methods, a computer-readable medium, servers and systems for enabling merchants to pass tokenized payment

information, e.g., payment tokens, instead of actual payment information, to HOPs and SOPs that are provided by third-party merchant service providers. The example methods, a computer-readable medium, servers and systems provide the advantage of enabling merchants to charge consumers without having to handle actual payment information. This enables merchants to avoid the costs associated with PCI compliance and other disadvantages that go along with handling consumer payment information. Further advantages include merchants being able to submit a purchase transaction to an HOP / SOP without the relevant consumer having to provide payment information at the time of the transaction. Thus, the consumer does not have to participate in the purchase transaction. For example, the consumer may provide payment information to the HOP / SOP during an initial account setup, the HOP / SOP can tokenize the payment information and pass a payment token to the merchant, and the merchant can thereafter submit the payment token in subsequent purchase transactions without the consumer's involvement. For example, when the consumer attempts to make a future purchase from the merchant (e.g., the consumer makes a subsequent purchase from the merchant's website), the merchant can pass the payment token to the HOP / SOP instead of the user having to reenter payment information. This streamlines the payment process for consumers and merchants. This also enables merchants to bill consumers on a recurring basis by simply passing payment tokens through the HOP / SOP.

[0032] A "purchase transaction" can be an electronic transaction involving a user, such as a consumer, and a merchant, where the user purchases an item or service from the merchant. An example includes a consumer making an online credit-card purchase on a merchant website.

[0033] "Order information" may include information about an electronic transaction, such as information about the item(s) to be purchased, payment amounts, sales tax, shipping address, shipping type (e.g., overnight, one-day, standard), carrier, shipping & handling costs, special requests (e.g., gift wrapping), etc. It may also include information about the consumer making the transactions, such as name, address, email address, purchase history, profile information, and any other information that may be used to measure the level of risk associated with the electronic transaction.

[0034] "Payment information" may include information associated with financial accounts, such credit-card accounts, debit-card accounts, demand accounts (e.g., checking accounts, money market accounts), prepaid accounts, eWallet accounts,

etc. Examples of such information include payment account numbers ("PANs"), expiration dates, bank routing numbers, checking account numbers, etc.

[0035] A "merchant service provider" can be any entity that provides services in support of electronic transactions. Examples of such services include using HOPs and/or SOPs to collect payment information and/or order information and using that information to process purchase transactions and/or evaluate fraud risk in purchase transactions. A merchant service provider may include both a payment service and a fraud detection service.

[0036] Figure 1 is a block diagram of an example of an operating system 100 in which embodiments of the invention can be implemented.

[0037] Figure 1 depicts a consumer 102, a user device 108 associated with the consumer 102, a merchant 112 and associated merchant pages 118 and 122, and a merchant service provider 126 ("service provider"), communicatively connected. The service provider 126 includes transaction services 136 and HOP services provider 134, which provides a hosted payment page 138. The transaction services 136 includes user profile/account data 142 and merchant configuration data 146 as well as a tokenization module 148. The system 100 illustrated in Figure 1 is referred to as a hosted service system 100, wherein the service provider 126, acting as a "host", hosts services for clients, such as the merchant 112. According to the illustrated embodiment, the merchant 112 and the consumer 102 can transmit information associated with electronic transactions to the service provider 126. According to some embodiments, the merchant 112 may transmit information, such as order information, or a request to create an account and to tokenize payment information, to the service provider 126, which performs one or more services based at least on the transaction information received from the merchant 112.

[0038] The consumer 102 is, generally, any entity that is a purchaser of products or services via an electronic transaction. Non-limiting examples include a person or business entity that purchases or licenses goods and services from merchants via the public Internet or at a retail store using a credit card, debit card, e-check, etc. The merchant 112 is, generally, any entity that offers goods or services in exchange for value.

[0039] The service provider 126 may be a third party other than the consumer and merchant, that provides services in support of electronic transactions. Non-limiting

examples of such services include services related to payment acceptance processing (e.g., HOP and SOP), credit card authorization, payment information tokenization, risk evaluation and management, fraud screening, tax calculation, export compliance verification, delivery address verification, Internet and/or e-mail address verification, payment crediting, billing, and the like. Service providers 126 may invoke service features of other service providers in support of their service offerings.

[0040] The consumer 102 and the merchant 112 may communicate through a network, such as with Internet-originated transactions. As part of a purchasing process, certain information is collected from the consumer 102 by the merchant 112. Non-limiting examples of information collected from the consumer 102 include information about the item to be purchased, payment information, shipping address, and whether the consumer wants to create an account with the merchant. However, as discussed above, some merchants may opt to not collect payment information, such as credit or bank card payment account numbers. For example, some merchants opt not to collect payment information because merchants want to avoid the costs associated with PCI compliance.

[0041] Once various transaction and customer-related information is collected by the merchant 112, the merchant transmits at least a portion of the information to the service provider 126. Additional information may be transmitted along with the information described. For example, the merchant 112 may transmit customized data or a specification of service provider 126 services to apply, or to ignore, in the electronic transaction processing that is provided by the service provider 126. Furthermore, according to embodiments described herein, customer-specified service strategies and schedules (e.g. schedules for recurring payments) may also be transmitted from the merchant 112 to the service provider 126. Any or all of the information referenced above, which is transmitted from the merchant 112 to the service provider 126, may be transmitted through a network in any suitable protocol. An example of a suitable protocol is Secure Sockets Layer (SSL). The service provider 126 then performs one or more services in relation to the electronic commercial transaction associated with transmitted transaction information.

[0042] An example will now be provided with reference to the encircled reference numerals 1-7 provided in Figure 1. It should be appreciated that the encircled reference numerals are provided for illustrative convenience and are not intended to

limit ways in which data may flow or the order in which steps may be executed in the system 100. For example, data may flow to and from any component of the system 100 in any order. This example will be discussed with reference to Figures 1-4.

[0043] Referring to encircled reference numeral 1 of Figure 1, this example begins with the consumer 102 visiting the merchant page 118 (see Figure 2), which is provided by a merchant web server 204. While visiting the merchant page 118, the consumer 102 can view details for a particular item. For example, as illustrated in Figure 2, the consumer 102 may view details of the item, which is a notebook computer. Further, while visiting the merchant page 118, the consumer 102 may select the “Add to Cart” button 210 to add the item to his or her electronic shopping cart. The consumer 102 may then select the “Go to Cart” button 220 to navigate to a webpage that displays order information for the item(s) that is in the consumer’s electronic shopping cart.

[0044] Referring now to encircled reference numeral 2, when the consumer selects the “Go to Cart” button 220, the merchant server 204 obtains the order information for the item(s) in the shopping cart and creates a one-way hash of the order information. Here, for example, at least some of the order information is form-filled data that is hidden from the consumer 102. According to an embodiment, script provided to the merchant 112 by the service provider 126 resides on the merchant server 204 and generates the one-way hash. Then, as indicated at encircled reference number 3, the merchant server 204 provides the one-hash and order information when generating the merchant page 122, an example of which is illustrated in Figure 3.

[0045] As illustrated in Figure 3, the merchant page 122 may be a shopping cart page that provides a summary of order information 312, which, beyond what is illustrated in Figure 3, may include, for example, an order number, customer information, item information (e.g., SKU data), etc. The merchant page 122 may provide the user with the option of creating an account with the merchant 112, if the user does not already have an account. For example, the merchant page 122 may display a “Create An Account” check box 320 and/or the merchant page 122 may display a “Create Account” section 324. To create an account, the consumer 102 may check the check box 320 and/or the consumer 102 may provide the information (e.g., name, email address or userID, and password) requested in the “Create Account” section 324.

[0046] As indicated at encircled reference numeral 4 of Figure 1, when the consumer 102 presses the "Checkout" button 318 on the merchant page 122, the merchant server 204 sends the order information 312, the one-way hash, and the request to create an account to the HOP services provider 134 of the service provider 126. For example, the "Checkout" button 318 may include a URL that redirects the user device 108 to a location at the HOP services provider 134. When the redirect occurs, the order information, the one-way hash, and the request to create an account are transmitted via the SSL pipe 148 from the merchant server 204 of the merchant 112 to the HOP services provider 134 by way of the redirect through the user device 108. In this example, the one-way hash, the order information, and the request to create an account are provided to the HOP services provider 134 in an HTML post. It should be appreciated that the merchant server 204 may send the order information, the one-way hash, the request to create an account, and any other desired information to the services provider 134 in any way known to those having ordinary skill in the art, such as via a direct connection between the merchant and the services provider.

[0047] Referring to encircled reference number 5, the HOP services provider 134 verifies the one-way hash provided by the merchant by applying its own copy of the hashing script to the order information to generate its own one-way hash of the order information and then comparing the hash it generates to the hash provided by the merchant. If the one-way hash is verified and thereby confirms that the order information was not tampered with during transmission from the merchant 112, then the HOP services provider 134 provides the hosted payment page 138 to the consumer 102. An example of the hosted payment page 138 is provided in Figure 4. For example, the hosted payment page 138 may include a summary of the order information 412, input fields 418 into which users may input their credit card information, e.g., credit card type, number, expiration data, etc., and input fields 422 into which user may input billing address information for the credit card, and a "Purchase" button 426 that user may select to submit their order. Referring to encircled reference number 6, the consumer 102, via the user device 108, inputs the payment information. For example, the consumer 102 inputs his or her credit card information into input fields 418 and his or her billing address information into input fields 422 and then presses the "Purchase" button 426.

[0048] It should be noted that, in the illustrated example, the payment information is transmitted via SSL pipe 150 from the user device 108 to the HOP services provider 134 and bypasses the merchant 112 altogether. Thus, the merchant 112 does not handle the payment information and therefore does not have to be PCI compliant.

[0049] Referring to encircled reference number 7, when the consumer 102 presses the "Purchase" button 426 and sends the payment information to the HOP services provider 134, the HOP services provider 134 forwards the payment information received from the consumer 102 as well as the order information received from the merchant 112 to the transaction services 136 via link 140.

[0050] The transaction services 136 accesses the user profile data 142 to determine whether the consumer already has an account/profile stored at the merchant service provider 126. If the consumer 102 already has a profile, then the transaction services 136 updates the payment information and the billing information in the consumer's account/profile with the payment information and the billing information that the consumer inputted into input fields 418 and 422 of the hosted payment page 138. If the consumer 102 does not already have a profile, then the transaction services 136 creates an account/profile for the user in the user profile data 142 and stores in the newly created account/profile the payment information and the billing information that the consumer inputted into input fields 418 and 422 of the hosted payment page 138. Further, the merchant service provider 126 instructs the tokenization module 148 to tokenize the payment information inputted by the user and thereby create a payment token for the payment information. It should be appreciated that the tokenization module 148 may create a unique payment token for each payment account (e.g., for each credit card) stored in the consumer's profile. The merchant service provider 126 then sends a copy of the payment token(s) to the merchant 112, which stores the payment token(s) on its database. The payment token(s) may be sent from the services provider 126 to the merchant 112 according to any means known to those having ordinary skill in the art. For example, the token(s) may be redirected to the merchant via the user device or the tokens may be sent directly to the merchant via connection 156. The merchant 112 may also create an account/profile for the consumer on its database and stores the payment token(s) in the consumer's account/profile.

[0051] An example process 500 is provided in Figure 5 whereby the process enables a merchant to securely send order information along with a request to create

an account for a consumer to a merchant service provider, according to an embodiment. According to embodiments, a merchant 112 presents item information about a particular item to a consumer 102 via an item detail page (504), such as the merchant page 118 of Figure 2. In the illustrated embodiment, the merchant web server 204 generates the merchant page 118 and the consumer 102 can view the page 118 via the user device 108. Next, the consumer 102 adds the item to the consumer's shopping cart (508). For example, as illustrated in Figure 2, the consumer 102 presses the "Add to Cart" button 210. After the consumer 102 adds the item to the shopping cart, the consumer 102 navigates to the shopping cart for the purpose of checking out and buying the item and, if applicable, indicating whether the consumer would like to create a new account (512). For example, as illustrated in Figures 2 and 3, the consumer 102 presses the "Go to Cart" button 220 of the merchant page 118 and thereby causes the web server 204 to take the consumer 102 to the merchant page 122 (e.g., the shopping cart page) of Figure 3, where the consumer 102 can review the order information 312 and create a new account, if applicable.

[0052] In operation, according to some embodiments, upon the consumer 102 pressing the "Go to Cart" button 220, the merchant web server 204 obtains the order information for the items to be displayed in the shopping cart and applies a hashing script/program to the order information to generate a one-way hash of the order information. The merchant web server 204 then provides the hash and the order information to the shopping cart page 122. For example, the hash and order information are provided to the shopping card page 122 in an HTML post.

[0053] At merchant page 122, the consumer may indicate that the consumer would like to create an account with the merchant. For example, the consumer may check the "Create An Account" check box 320 and/or input the appropriate information (e.g., name, email address or userID, and password) into the input fields of the "Create Account" section 324. If the consumer 102 intends to purchase the items presented on the shopping cart page, then the consumer 102 presses the "Checkout" button 318 (518) and thereby causes the merchant web server 204 to send the order information, the one-way hash of the order information, and the new account request to the HOP services provider 134 (524). For example, the merchant web server 204 sends the order information, the hash, and the new account request

to the HOP services provider 134 of the services provider 126 via the consumer device 108 in the form of a HTML post.

[0054] An example process 600 is provided in Figure 6 whereby the process enables a merchant service provider to obtain payment information from a consumer, according to an embodiment. According to embodiments, the HOP services provider 134 receives the order information, the hash of the order information, and the request to create an account from the merchant web server 204 (604), and the HOP services provider 134 verifies the hash provided by the merchant (608). For example, the HOP services provider applies its own copy of the hashing script to the order information to generate its own hash of the order information and then compares the hash it generated to the hash provided by the merchant. If the hash is verified, then the HOP services provider 134 searches the merchant configuration data 146 to obtain the merchant's 112 configurations regarding rendering the hosted payment page to the customer on behalf of the merchant (612). For example, the merchant 112 may specify that the hosted payment page (e.g., page 138 of Figure 4) only provide input fields for collecting payment information or that it provide input fields for collecting payment information as well as the relevant order summary information.

[0055] The HOP services provider 134 renders the payment page according to the merchant's configurations (618), and the consumer 102 may input and submit payment information (622). For example, the HOP services provider 134 may render a hosted webpage such as the hosted payment page 138 illustrated in Figure 4. Upon viewing the hosted payment page via the user device 108, the consumer 102 may use the consumer device 108 to review the order information 412, input credit card information into the payment input fields 418, and input billing address information into the billing address information fields 422. After reviewing and inputting information, the consumer 102 may submit the payment information to the HOP services provider 134 by selecting the "Place Order" or "Purchase" button 426. As discussed, in the illustrated example, the payment information is transmitted from the user device 108 to the HOP services provider 134 via the SSL pipe 148 and bypasses the merchant 112. Thus, the merchant does not handle the payment information and therefore does not have to be PCI compliant. The HOP services provider 134 creates a transaction request that includes the payment information received from the consumer 102 as well as the order information and the request to

create an account received from the merchant 112 (626) and sends the transaction request to transaction services 136 (630).

[0056] An example process 700 is provided in Figure 7 whereby the process enables a merchant service provider to create an account for a user, save the user's payment information in the account, and tokenize the user's payment information, according to an embodiment. According to embodiments, the transaction services 136 receives the transaction request from the HOP service provider 134 (720). The transaction services 136 accesses the user profile data 142 to determine whether the consumer already has an account stored on the service provider's 126 databases (724). For example, if the consumer 102 already has an account that includes payment information, the process 700 involves updating the consumer's account to include the most recent payment information provided by the consumer to the HOP services (728).

[0057] On the other hand, if the services provider 126 does not have an account for the consumer, then the transaction services 136 creates an account for the consumer 102 in the user profile data 142 and saves the consumer's payment information in the account (730). The transaction services 136 then instructs the tokenization module 148 to tokenize the payment information in the consumer's account so as to create a payment token (734) for each payment account and then pass the payment token(s) back to the merchant 112 (738). It should be appreciated that the payment token(s) may be sent to the merchant 112 via connection 156 or via a redirect through the user device 108 using the SSL pipe 148. The merchant then saves the payment token(s) in the consumer's account on the merchant's databases.

[0058] An example process 800 is provided in Figure 8 whereby the process enables a merchant to pass payment tokens – instead of actual payment information – to an HOP provided by a merchant service provider, according to an embodiment. According to embodiments, the merchant and a consumer initiate a purchase transaction (804), where the consumer has already created an account with the merchant and the consumer's profile, which includes at least a payment token, is stored on the merchant's database and in the user profile data 142 of the merchant service provider 126. For example, the consumer may navigate to the merchant's ecommerce website, select an item, and attempt to purchase the item. Also for example, the consumer may have previously signed up for a recurring billing arrangement with the merchant. For example, the merchant may be an online

newspaper publisher and the consumer may have purchased a subscription for the newspaper, where the consumer agreed to have his credit card charged on a monthly, recurring basis.

[0059] Upon initiation of the purchase transaction, the merchant locates the consumer's profile on the merchant's database (812) and obtains the payment token (816) associated with the consumer's payment information. The merchant then creates an authorization call, which includes the order information and the payment token (820). The merchant then sends the authorization call to the merchant service provider 126 (822). The merchant service provider 126, upon receiving the payment token, locates the payment token stored in the consumer's account in the user account data 146 that matches the payment token that was included in the authorization call (826). The merchant then obtains the payment information that is associated with the payment token (830) and uses that payment information to process the purchase transaction (834).

[0060] According to an embodiment, a the authorization call from the merchant may be a subscription request that includes order information and the payment token, where the order information provides details regarding the subscription. Such subscription details may include payment frequency (e.g., monthly, annually, etc.), duration (e.g., six months, one year, two years, etc.), and payment amount. In this case, the merchant service provider uses the subscription details information provided in the subscription request to process subscription payments on behalf of the merchant without the merchant having to prompt the merchant service provider each time a payment is to be processed. For example, an online newspaper publisher may enter a subscription agreement with a consumer whereby the consumer agrees to pay twenty dollars per month for one year, the payment to be made on the first day of each month. In this example, the online newspaper publisher would send the merchant service provider a subscription request that instructs that the merchant service provider to process a payment on the first day of each month for one year. This way, the online newspaper publisher does not have to submit an authorization call to the merchant service provider each time a payment is due under the subscription.

[0061] Figure 9 is a block diagram of an example of an operating system 900 in which embodiments of the invention can be implemented.

[0062] The system 900 of Figure 9 includes similar components as the system 100 of Figure 1 except, for example, instead of having an HOP services provider 134, the system 900 includes an SOP services provider 934. Operation of the system 900 is similar to the operation of system 100 in some regards except, for example, instead of relying on the HOP services provider 134 to host the payment page (e.g., hosted payment page 138 of Figure 4), the merchant 112 of Figure 9 hosts its own payment page 1022, an example of which is provided in Figure 10, and the SOP services provider 934 is used to provide the merchant 112 with a SOP.

[0063] Exemplary operation of the system 900 will now be described with reference to the encircled reference numerals 1-7 provided in Figure 9. It should be appreciated that the encircled reference numerals are provided for illustrative convenience and are not intended to limit ways in which data may flow or the order in which steps may be executed in the system 900. For example, data may flow to and from any component of the system 900 in any order. This example will be discussed with reference to Figures 2, 3, and 10.

[0064] Referring to encircled reference numeral 1, this example begins with the consumer 102 visiting the merchant page 118 (see Figure 2), which is provided by a merchant web server 204. While visiting the merchant page 118, the consumer 102 can view details for a particular item and the consumer 102 may select the "Add to Cart" button 210 to add one or more items to his or her electronic shopping cart. Further, as indicated at encircled reference numeral 2, the consumer 102 may select the "Go to Cart" button 220 to navigate to a webpage that displays order information for the items that are in the consumer's electronic shopping cart. The merchant page 122 is an example of such a page and is illustrated in Figure 3. For example, as illustrated in Figure 3, the merchant page 122 may provide a summary of the order information 312, which, beyond what is illustrated in Figure 3, may include, for example, an order number, customer information, item information (e.g., SKU data), etc.

[0065] The merchant page 122 may further provide the user with the option of creating an account with the merchant 112, if the user does not already have an account. For example, the merchant page 122 may display a "Create An Account" check box 320 and/or the merchant page 122 may display a "Create Account" section 324. To create an account, the consumer 102 may check the check box 320

and/or the consumer 102 may provide the information (e.g., name, email address or userID, and password) requested in the "Create Account" section 324.

[0066] As indicated at encircled reference numeral 3 of Figure 9, when the consumer 102 presses the "Checkout" button 318 of Figure 3, the merchant server 204 provides a payment page, an example of which is provided in Figure 10. For example, the payment page 1022 may include a summary of the order information 1012, input fields 1018 into which users may input their credit card information, e.g., credit card type, number, expiration data, etc., and input fields 1022 into which users may input billing address information for the credit card. The consumer 102, via the user device 108, inputs his or her credit card information into input fields 1018 and his or her billing address information into input fields 1022 and then presses the "Purchase" button 1026.

[0067] As indicated at encircled reference numeral 4 in Figure 9, after the user inputs his or her payment information into payment page 1022, the merchant 112 transmits the payment information, the order information, and a request to create an account/profile to the SOP services provider 934. It should be noted that, in the illustrated example, the merchant 112 does not store the payment information, but instead transmits the payment information to the SOP services provider 934. Thus, because the merchant 112 does not store payment information, the merchant 112 does not have to be PCI compliant. Referring to encircled reference numeral 5, the SOP services provider 934 sends the payment information, the order information, and the request to create an account/profile received from the merchant 112 to the transaction services 136.

[0068] Referring to encircled reference numeral 6, the transaction services 136 accesses the user profile data 142 to determine whether the consumer already has an account stored at the merchant service provider 126. If the consumer 102 already has an account, then the transaction services 136 updates the payment information and the billing information in the consumer's account with the payment information and the billing information that the consumer inputted into input fields 1018 and 1022 of the payment page 1022 hosted by the merchant's servers. If the consumer 102 does not already have an account, then the transaction services 136 creates a profile for the user in the user profile data 142 and stores in the newly created profile the payment information and the billing information that the consumer inputted into input fields 1018 and 1022 of the payment page 1022.

[0069] Further, the merchant service provider 126 instructs the tokenization module 148 to tokenize the payment information inputted by the user and thereby create a payment token for the payment information. It should be appreciated that the tokenization module 148 may create a unique payment token for each payment account (e.g., for each credit card) stored in the consumer's profile. Then, as indicated at encircled reference numeral 7, the merchant service provider 126 sends a copy of the payment token(s) to the merchant 112, which stores the payment token(s) on its database. It should be appreciated that the merchant service provider 126 may send the payment token(s) via connection 1050 to the user device 108, which sends the copy of the payment token(s) to the merchant 112, and/or the merchant service provider 126 may send the payment token(s) via connection 1056 to the merchant 112 and thereby bypass the user device 108. According to an embodiment, the merchant 112 also creates an account for the consumer on its database and stores the payment token(s) in the consumer's account.

[0070] Figure 11 is a block diagram illustrating a transaction processing system 10 that may be used with some embodiments of the present invention.

[0071] Figure 11 illustrates the primary functional elements that are typically involved in processing a purchase transaction and in the authorization process for such a transaction. As shown in Figure 11, in a typical purchase transaction, a consumer wishing to purchase a good or service from a merchant uses a payment device 20 to provide purchase transaction data that may be used as part of a consumer authentication or transaction authorization process. Payment device 20 may be a debit card, credit card, smart card, mobile device containing a contactless chip, computer, or other suitable form of device.

[0072] The portable payment device is presented to a mobile payment acceptance device 22 of a merchant 24. For example, the acceptance device 22 could be a device reader or point of sale (POS) terminal 22 which is able to access data stored on or within the payment device. In embodiments, the portable payment device communicates account/payment information to the merchant 24 via a "card not present" transaction over a communications network, such as a cellular network, the Internet, etc. The account data (as well as any required consumer data) is communicated to the merchant 24 and ultimately to a merchant service provider 26 (such as AUTHORIZE.NET). As part of the authentication or authorization process performed by the service provider, the service provider 26 may access database 28,

which typically stores data regarding the customer/consumer/user (as the result of a registration process with the merchant, for example), the consumer's payment device, and the consumer's transaction history with the merchant. The database 28 may also include information about the merchant 24, such as a list of the merchant's approved payment acceptance devices 22. For example, upon receiving information about the payment device 20 from the merchant's mobile payment acceptance device 22, the service provider 26 may extract information that identifies the mobile payment acceptance device 22 and validate that information against a list of approved mobile payment acceptance devices. The service provider 26 typically communicates with acquirer 30 (which manages the merchant's accounts) as part of the overall authentication or authorization process. The service provider 26 and/or acquirer 30 provide data to payment processing network 34, which, among other functions, participates in the clearance and settlement processes that are part of the overall transaction processing.

[0073] Communication and data transfer between service provider 26 and payment processing network 34 are typically by means of an intermediary, such as acquirer 30. As part of the consumer authentication or transaction authorization process, payment processing network 34 may access account database 36, which typically contains information regarding the consumer's account payment history, chargeback or transaction dispute history, credit worthiness, etc. Payment processing network 34 communicates with issuer 38 as part of the authentication or authorization process, where issuer 38 is the entity that issued the payment device to the consumer and manages the consumer's account. Customer or consumer account data is typically stored in customer/consumer database 40 which may be accessed by issuer 38 as part of the authentication, authorization or account management processes. Note that instead of, or in addition to, being stored in account database 36, consumer account data may be included in, or otherwise part of, customer/consumer database 40.

[0074] According to an embodiment, in standard operation, an authorization request message is created by the mobile payment acceptance device 22 during a consumer purchase of a good or service using a portable payment device. In some embodiments, the mobile payment acceptance device 22 of the merchant 24 may be a wireless phone or personal digital assistant that incorporates a contactless card or chip or payment acceptance application. The authorization request message is

typically sent from the payment application of the mobile payment acceptance device 22 to the service provider 26, and then to the merchant's acquirer 30, to a payment processing network 34, and then to an issuer 38. An authorization request message can include a request for authorization to conduct an electronic purchase transaction and data relevant to determining if the request should be granted as well as device identification information related to the mobile payment acceptance device 22, which the service provider 26 validates against the list of approved mobile payment acceptance devices 22. For example, it may include one or more of an account holder's payment account number, currency code, sale amount, merchant transaction stamp, acceptor city, acceptor state/country, etc. An authorization request message may be protected using a secure encryption method (e.g., 128-bit SSL or equivalent) in order to prevent unauthorized access to account or transaction data.

[0075] After the issuer receives the authorization request message, the issuer determines if the transaction should be authorized and sends an authorization response message back to the payment processing network to indicate whether or not the current transaction is authorized. The payment processing system then forwards the authorization response message to the acquirer. The acquirer then sends the response message to the service provider 26, which then sends the response message to the merchant's mobile payment acceptance device 22. The merchant is thus made aware of whether the issuer has authorized the transaction, and hence whether the transaction can be completed.

[0076] At a later time, a clearance and settlement process may be conducted by elements of the payment/transaction processing system depicted in Figure 2. A clearance process involves exchanging financial details between an acquirer and an issuer to facilitate posting a transaction to a consumer's account and reconciling the consumer's settlement position. Clearance and settlement can occur simultaneously or as separate processes.

[0077] Payment processing network 34 may include a server computer. A server computer is typically a powerful computer or cluster of computers. For example, the server computer 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. Payment processing network 34 may use any suitable combination of wired or wireless networks, including the Internet, to

permit communication and data transfer between network elements. Among other functions, payment processing network 34 may be responsible for ensuring that a consumer is authorized to conduct a transaction (via an authentication process), confirm the identity of a party to a transaction (e.g., via receipt of a personal identification number), confirm a sufficient balance or credit line to permit a purchase, or reconcile the amount of a purchase with the consumer's account (via entering a record of the transaction amount, date, etc.).

[0078] The payment device 20 may take one of many suitable forms. As mentioned above, the portable payment device can be a mobile device that incorporates a contactless element such as a chip for storing payment information (e.g., a BIN number, account number, etc.) and a near field communications (NFC) data transfer element such as an antenna, a light emitting diode, a laser, etc. The portable payment device may also include a keychain device (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. The device containing the contactless card or chip, or other data storage element may be a cellular (mobile) phone, personal digital assistant (PDA), pager, transponder, or the like. The portable payment device may also incorporate the ability to perform debit functions (e.g., a debit card), credit functions (e.g., a credit card), or stored value functions (e.g., a stored value or prepaid card).

[0079] Figure 12 shows a block diagram of an exemplary computer apparatus that can be used in some embodiments of the invention (e.g., in any of the components shown in the prior Figures).

[0080] The subsystems shown in Figure 12 are interconnected via a system bus 1205. Additional subsystems such as a printer 1210, keyboard 1220, fixed disk 1230 (or other memory comprising computer-readable media), monitor 1240, which is coupled to display adapter 1250, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 1260, can be connected to the computer system by any number of means known in the art, such as through serial port 1270. For example, serial port 1270 or external interface 1280 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 1205 allows the central processor 1290 to communicate with each subsystem and to control the execution of instructions from system memory 1295 or the fixed disk

1230, as well as the exchange of information between subsystems. The system memory 1295 and/or the fixed disk 1230 may embody a computer-readable medium.

[0081] The previous description of the embodiments is provided to enable any person skilled in the art to practice the invention. The various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without the use of inventive faculty. Thus, the present invention is not intended to be limited to the embodiments shown herein, but is to be accorded the widest scope consistent with the principles and novel features disclosed herein. For example, although some specific embodiments describe the use of a message conversion process with typical brick and mortar type merchants, embodiments of the invention can also be used in on-line e-commerce type transactions.

[0082] 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.

[0083] Further, additional embodiments of the invention may be directed to methods and systems involving merchants, and their access devices, as well as issues. For example, other embodiments may include the following additional embodiments.

[0084] 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 can know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0085] 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 CDROM. 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.

[0086] 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.

[0087] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary. A recitation of "she" is meant to be gender neutral, and may be read as "he" or "she", unless specifically indicated to the contrary.

[0088] 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:

receiving order information and a request to create an account from a merchant, the order information associated with a purchase transaction between a user and the merchant, the account being for the purpose of storing payment information of the user at the merchant service provider;

rendering a hosted payment page on behalf of the merchant, the hosted payment page presenting to the user at least a portion of the order information and at least an input field into which the user may input the payment information;

receiving the payment information from the user;

processing the purchase transaction between the user and the merchant using the payment information;

creating an account for the user if the user does not already have an account;

tokenizing the payment information so as to create a payment token;

storing the payment information and the payment token in the account;

and

sending a copy of the payment token to the merchant, the merchant being able to submit the payment token in future purchase transactions between the merchant and the user, thereby eliminating the need for the user to resubmit the payment information in future purchase transactions between the merchant and the user.

2. The method of claim 1 further comprising:

receiving from the merchant the copy of the payment token and a request to process a purchase transaction involving the user;

accessing the account of the user to obtain the payment token;

verifying that the copy of the payment token matches the payment token in the account of the user; and

using the payment information associated with the payment token in the account of the user to process the purchase transaction.

3. The method of claim 1 wherein a server of the merchant generates a hash of the order information and transmits the hash along with the order information.
4. The method of claim 3 further comprising:
verifying the hash to ensure that the order information was not tampered with during transmission from the server of the merchant.
5. The method of claim 1 wherein creating an account for the user, if the user does not already have an account, comprises:
determining whether the user already has an account.
6. The method of claim 5 further comprising:
if it is determined that the user already has an account, updating the account with the payment information received from the user.
7. The method of claim 1 further comprising:
obtaining hosted-payment-page configurations designated by the merchant, wherein the hosted payment page is rendered in accordance with the hosted-payment page configurations.
8. A method, comprising:
receiving, at a merchant service provider, order information and a request to create an account from a merchant server of a merchant, the order information associated with a purchase transaction between a user and the merchant, the account being for the purpose of storing payment information of the user at the merchant service provider;
receiving, at the merchant service provider, payment information from the user who is engaging in the purchase transaction with the merchant, wherein the payment information is sent to the merchant service provider from a device associated with the user and wherein the payment information bypasses the merchant server;
creating, at the merchant service provider, an account for the user;
storing, at the merchant service provider, the payment information of the user in the account of the user;

tokenizing, at the merchant service provider, the payment information in the account of the user so as to create a payment token that represents the payment information of the user; and

transmitting, from the merchant service provider, a copy of the payment token to the merchant server.

9. The method of claim 8 further comprising:

receiving, at the merchant service provider, from the merchant, the copy of the payment token and a request to process a purchase transaction involving the user;

accessing the account of the user to obtain the payment token;

verifying the copy of the payment token matches the payment token;

and

using the payment information associated with the payment token in the account of the user to process the purchase transaction.

10. The method of claim 8 wherein the merchant service provider is a hosted order page (HOP) service provider.

11. The method of claim 10 further comprising:

rendering, at the HOP service provider, a hosted payment page on behalf of the merchant, the hosted payment page displaying at least a portion of the order information, the hosted payment page comprising a payment information entry section for collecting payment information from the user.

12. The method of claim 11 further comprising:

obtaining, at the HOP service provider, hosted-payment-page configurations designated by the merchant, wherein the hosted payment page is rendered in accordance with the hosted-payment page configurations.

13. The method of claim 11 wherein the payment information is received from the user via the payment information entry section of the hosted payment page.

14. The method of claim 8 wherein the merchant server generates a hash of the order information and transmits the hash to the merchant service provider along with the order information.

15. The method of claim 14 further comprising:

verifying, at the merchant service provider, the hash to ensure that the order information was not tampered with during transmission between the merchant server and the merchant service provider.

16. A system, comprising:

a processor;

a memory device including instructions that, when executed by the processor, cause the processor to:

receive from a merchant server of a merchant order information and a request to create an account, the order information associated with a purchase transaction between a user and the merchant, the account being for the purpose of storing payment information of the user at the merchant service provider;

receive payment information from the user who is engaging in the purchase transaction with the merchant, wherein the payment information is sent to the merchant service provider from a device associated with the user and wherein the payment information bypasses the merchant server;

create an account for the user;

store the payment information of the user in the account of the user;

tokenize the payment information in the account of the user so as to create a payment token that represents the payment information of the user; and transmit a copy of the payment token to the merchant server.

17. The system of claim 16 wherein the instructions, when executed by the processor, further cause the processor to:

receive from the merchant the copy of the payment token and a request to process a purchase transaction involving the user;

access the account of the user to obtain the payment token;

verify the copy of the payment token matches the payment token; and

use the payment information associated with the payment token in the account of the user to process the purchase transaction.

18. The system of claim 16 wherein the instructions, when executed by the processor, further cause the processor to:

render a hosted payment page on behalf of the merchant, the hosted payment page displaying at least a portion of the order information, the hosted

payment page comprising a payment information entry section for collecting payment information from the user.

19. The system of claim 18 wherein the instructions, when executed by the processor, further cause the processor to:

obtain hosted-payment-page configurations designated by the merchant, wherein the hosted payment page is rendered in accordance with the hosted-payment page configurations.

20. The method of claim 18 wherein the payment information is received from the user via the payment information entry section of the hosted payment page.

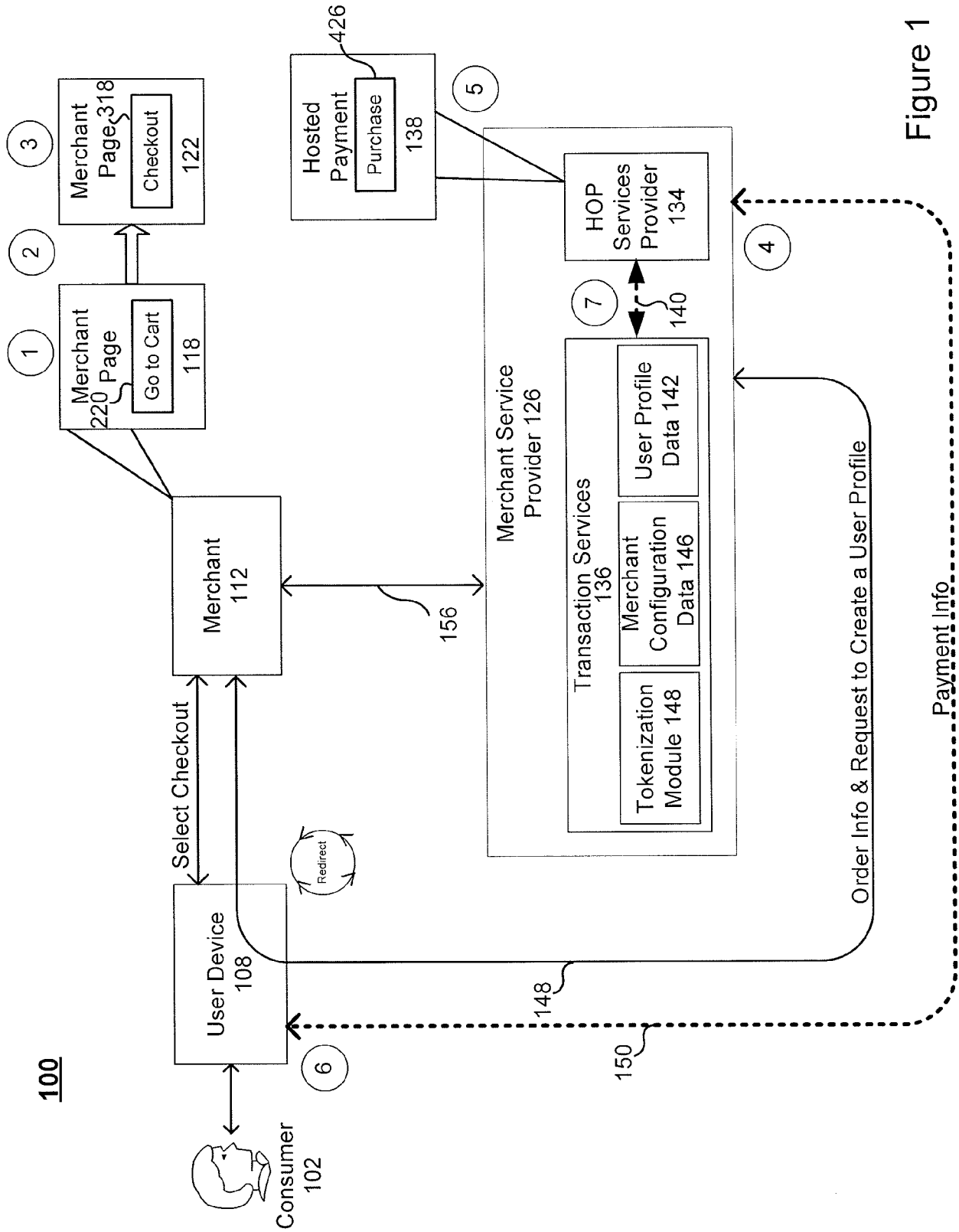


Figure 1

2/12

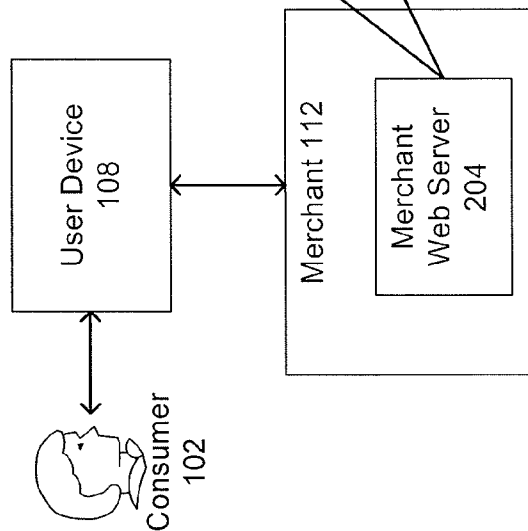
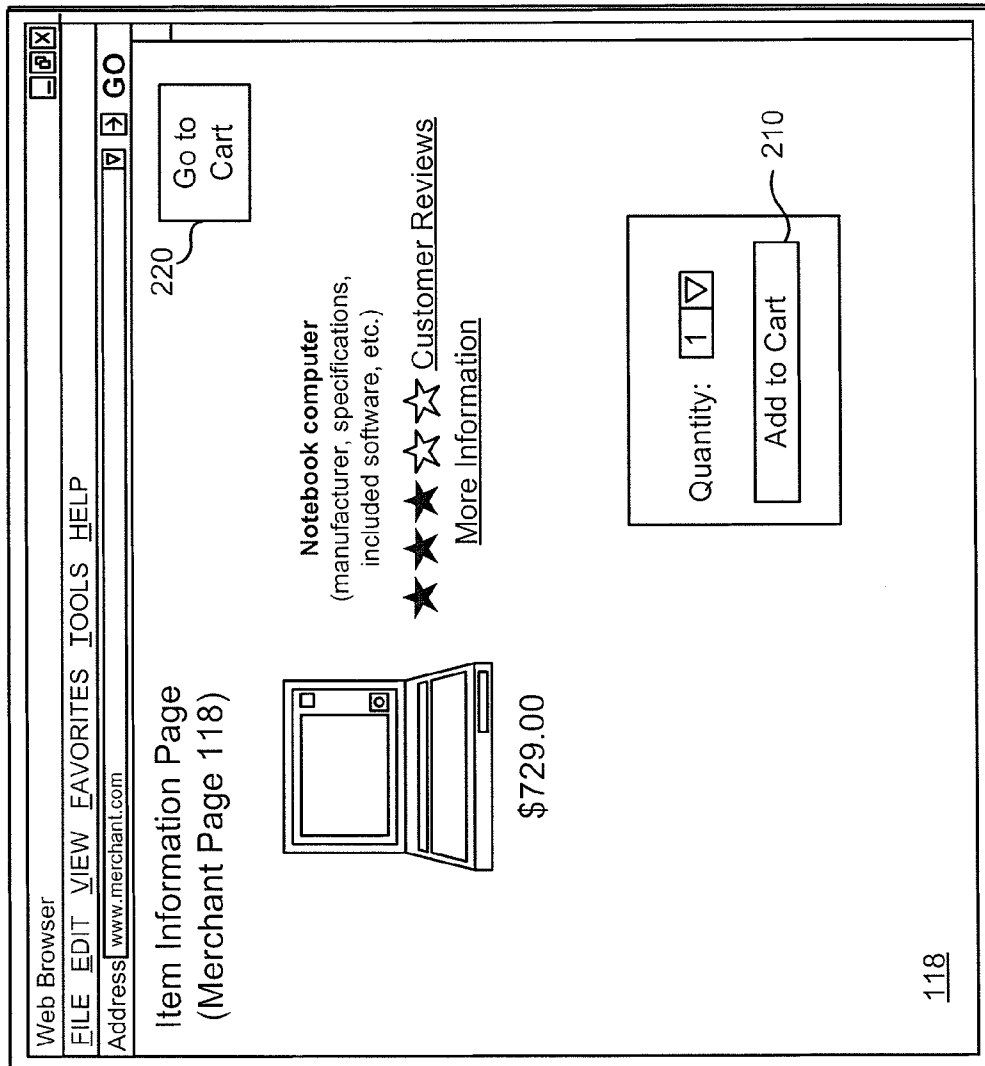


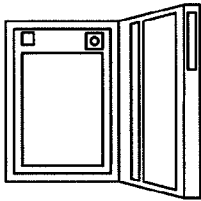
Figure 2

3/12

Web Browser
FILE EDIT VIEW FAVORITES TOOLS HELP
Address GO

Shopping Cart

(Merchant Page 122)



Notebook computer
(manufacturer, specifications, included software, etc.)

Order Summary

Item: Notebook computer ³¹²
Qty: 1
Price: \$729.00
Tax: \$67.00
Shipping: \$12.00
Total: \$808.00 ³²⁰

Create an Account? ☐ ³²⁴

[Create Account](#)

Name
Email Address
Password

³¹⁸

122

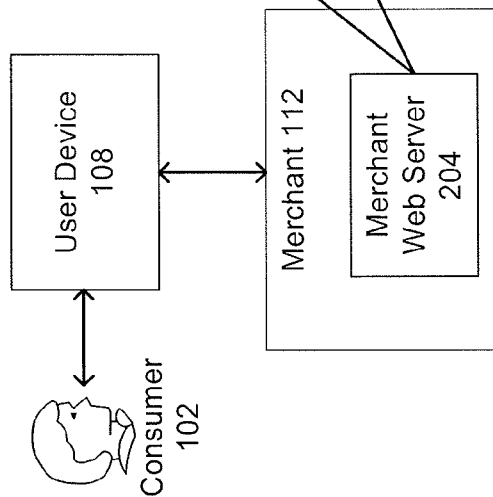


Figure 3

4/12

Web Browser
FILE EDIT VIEW FAVORITES TOOLS HELP
Address

Payment Page (Hosted Payment Page 138)

Order Summary

Qty: 1

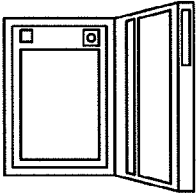
Price: \$729.00

Tax: \$67.00

Shipping: \$12.00

Total: \$808.00

Notebook Computer



Payment Information

Card Type

Number

Exp. Date

Cardholder Name

Billing Information

Street

City

State

Zip Code

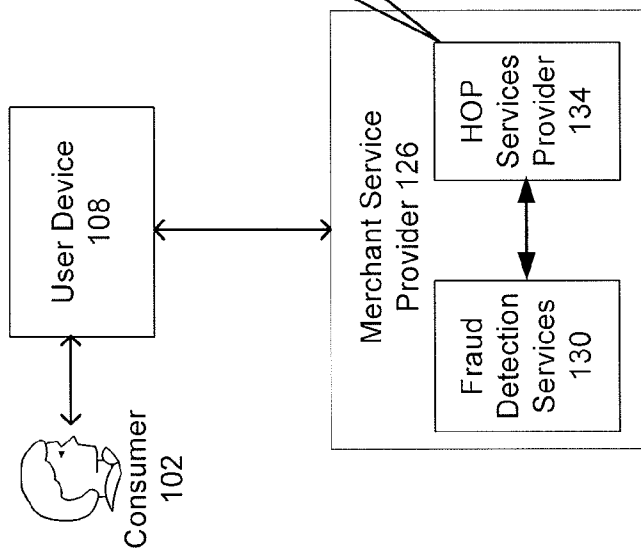


Figure 4

5/12

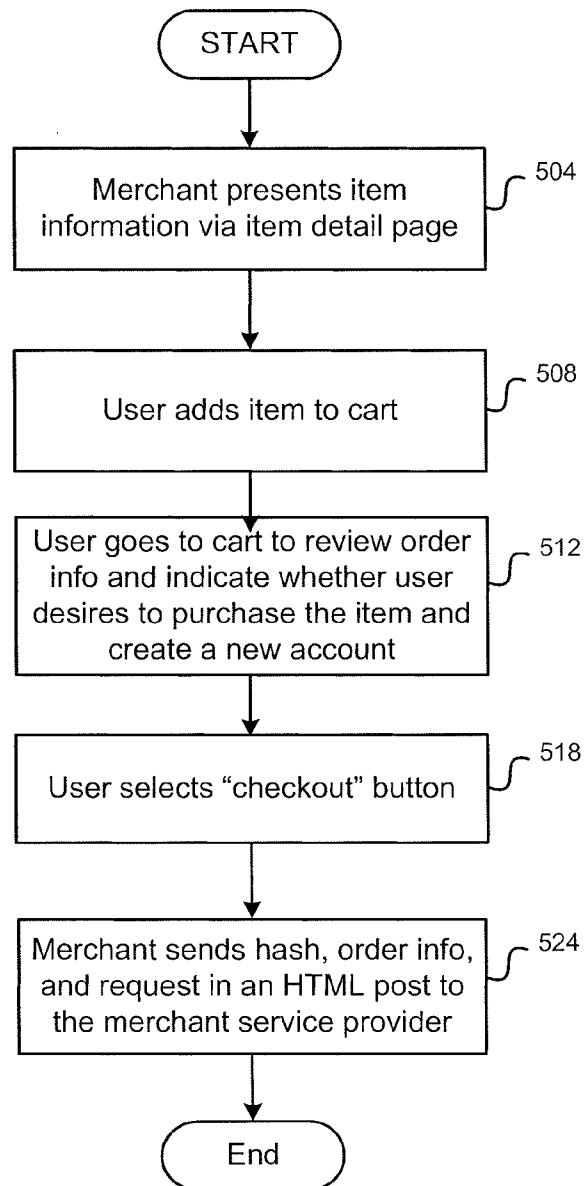
500

Figure 5

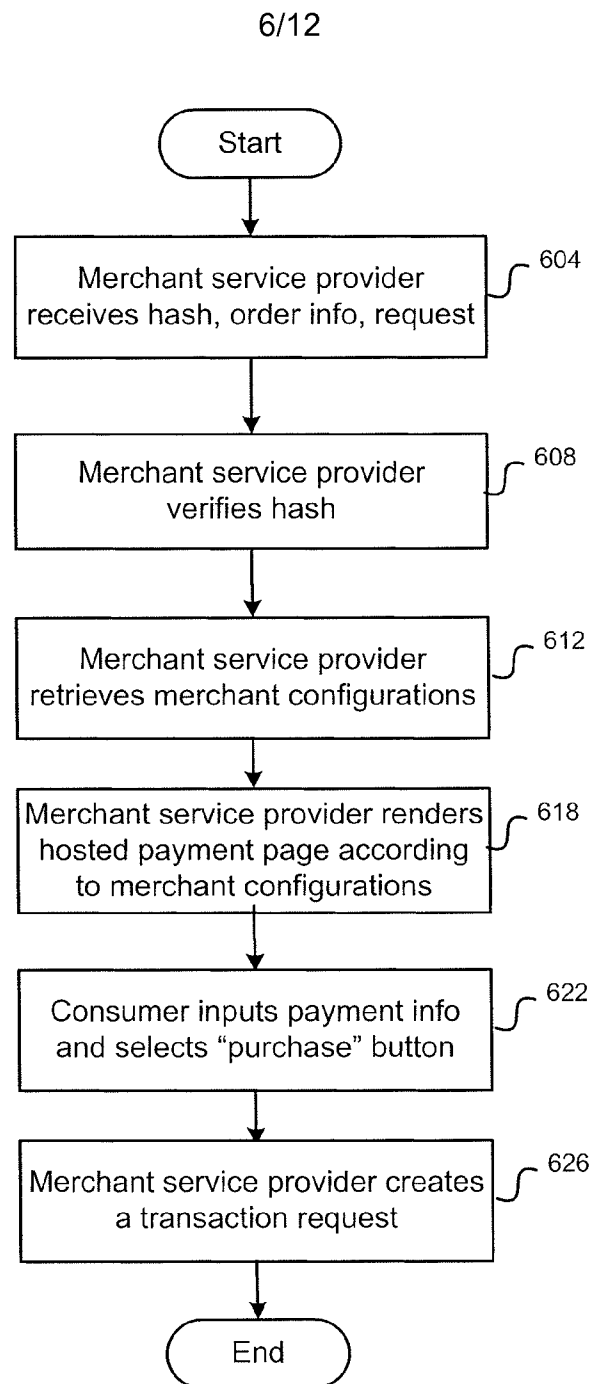


Figure 6

7/12

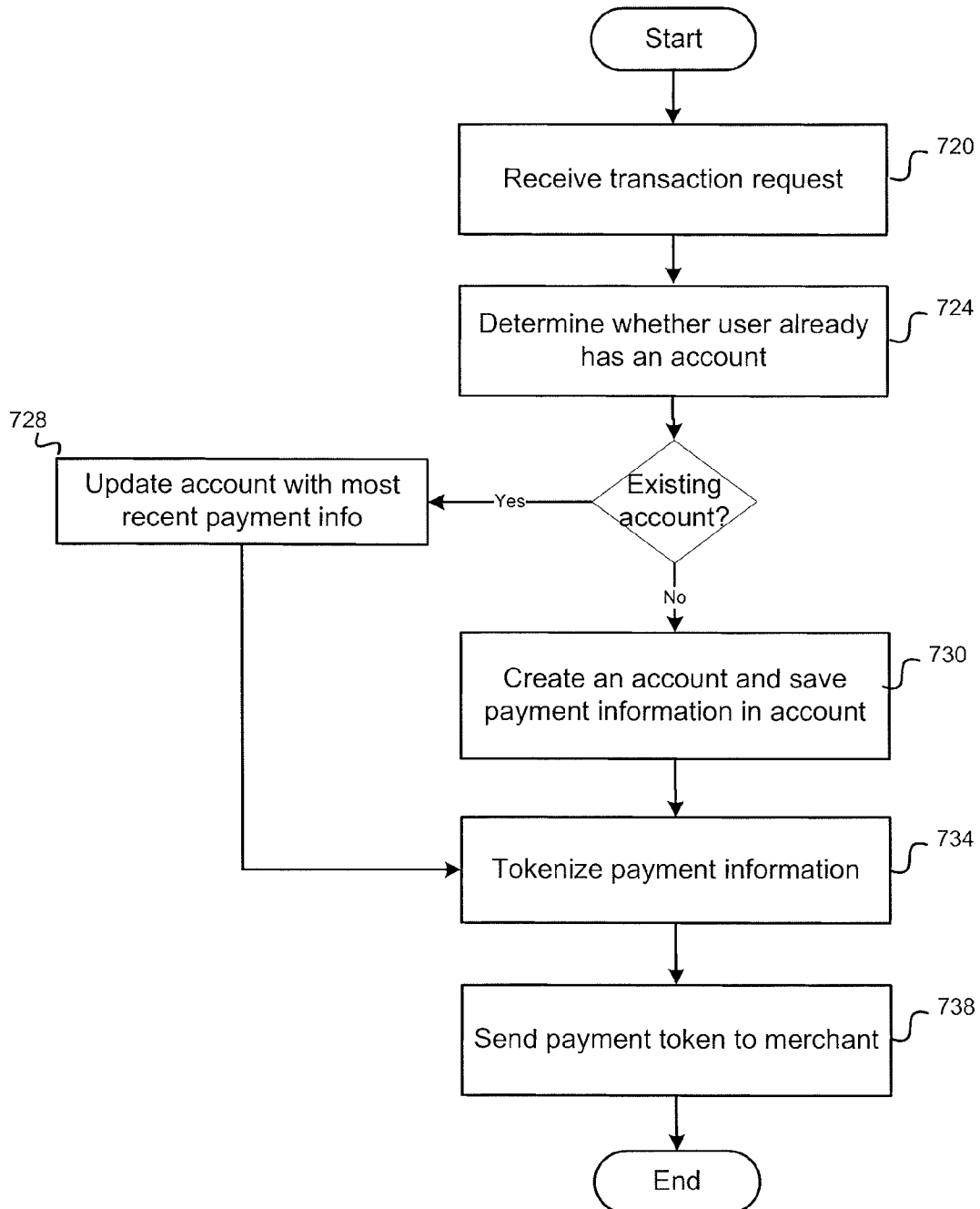
700

Figure 7

8/12

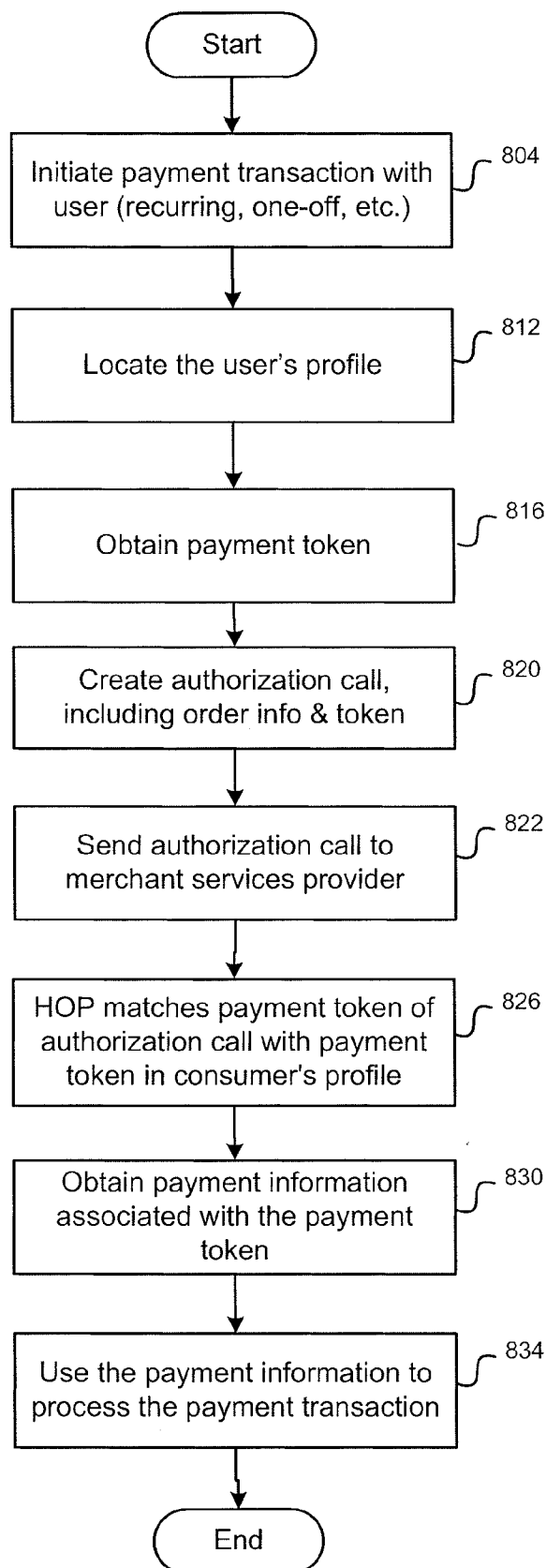
800

Figure 8

9/12

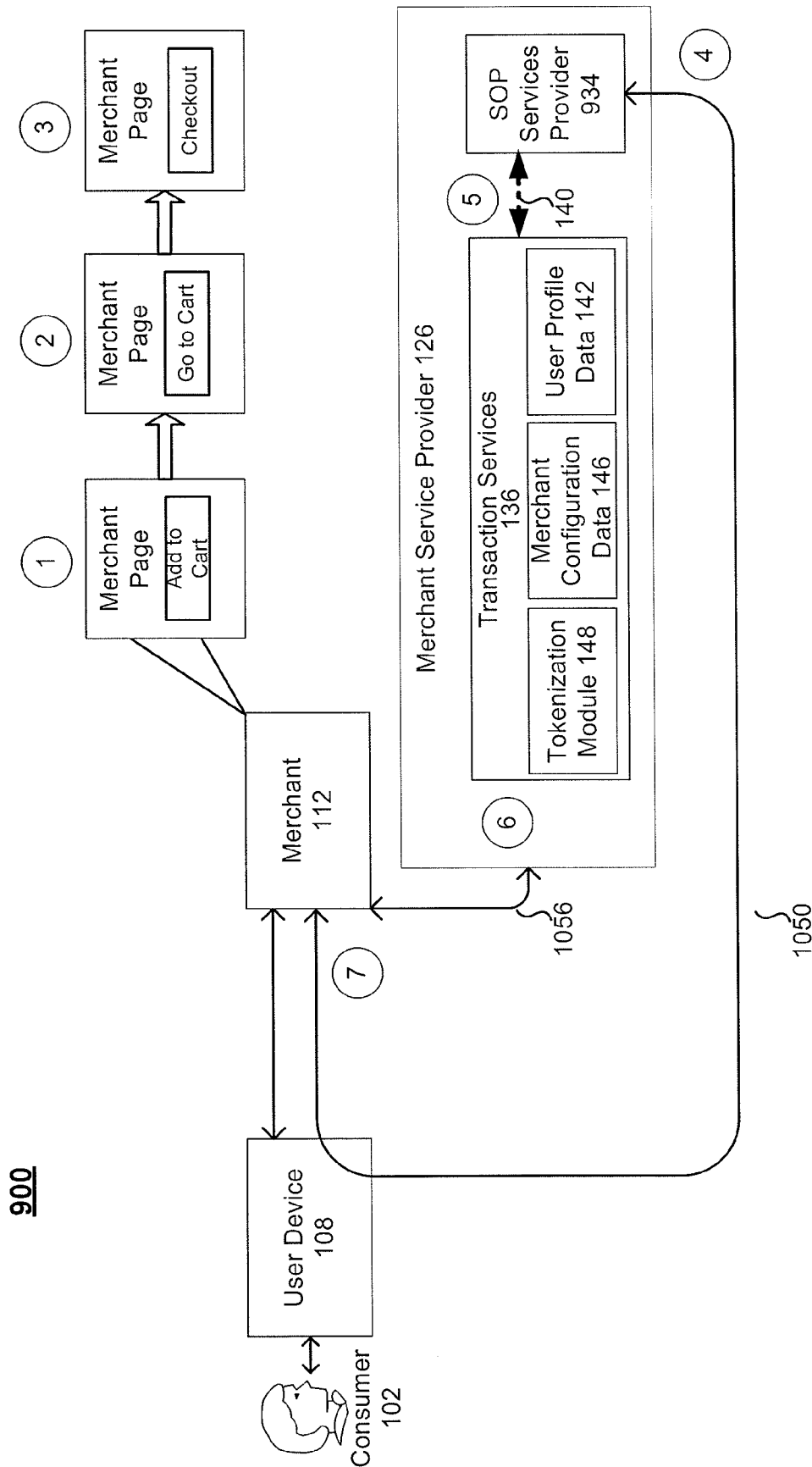


Figure 9

10/12

Web Browser

FILE EDIT VIEW FAVORITES TOOLS HELP

Address www.merchant.com

1012

Order Summary

Qty: 1

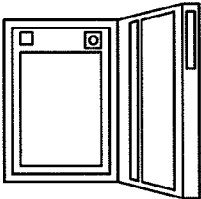
Price: \$729.00

Tax: \$67.00

Shipping: \$12.00

Total: \$808.00

Notebook Computer



Credit Card Information

1018

Card Type

1018

Visa

Number

5555-5555-5555

Exp. Date

07/2020

Cardholder Name

John Doe

Billing Information

1022

Street

1701 North Avenue

City

Asheville

State

North Carolina

Zip Code

28202

1026

Purchase

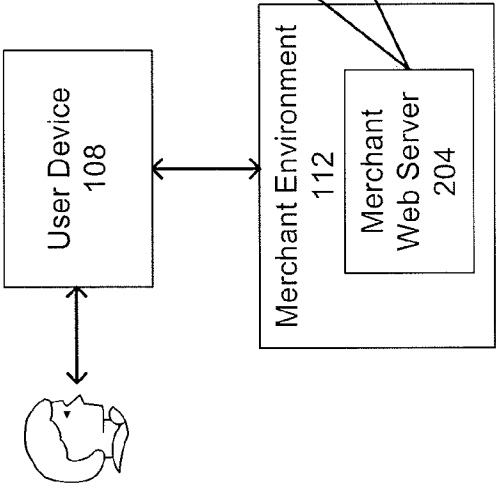
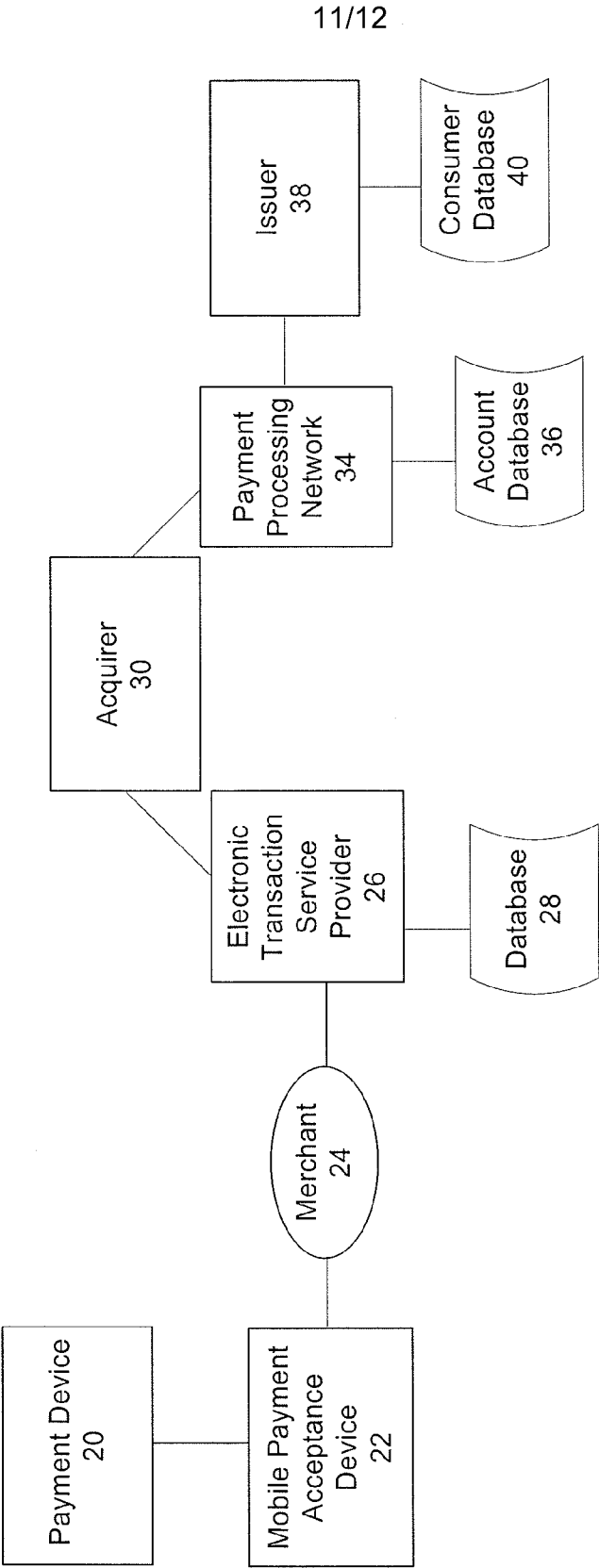


Figure 10

10



11/12

Figure 11

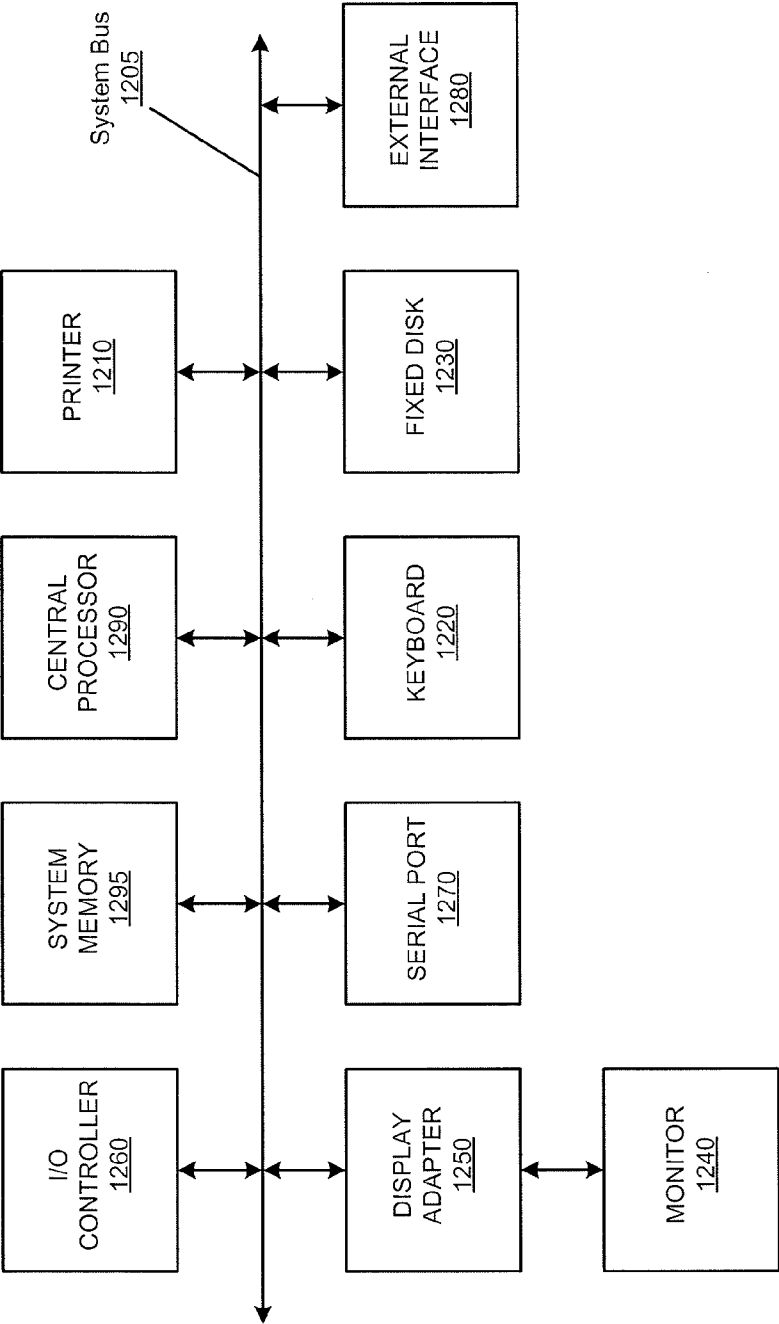


Figure 12