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

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
3 April 2008 (03.04.2008)

(10) International Publication Number
WO 2008/039942 A1

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

(21) **International Application Number:**
PCT/US2007/079772

(22) **International Filing Date:**
27 September 2007 (27.09.2007)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
60/848,570 27 September 2006 (27.09.2006) US

(71) **Applicant** *(for all designated States except US):* **ELECTRONIC COMMERCE PROTECTION CORPORATION** [US/US]; 15600 N.E. 8th Street, Suite Bl, PMB 386, Bellevue, WA 98008 (US).

(72) **Inventor; and**
(75) **Inventor/Applicant** *(for US only):* **NEFF, C , Andrew** [US/US]; 3048-164th Place N.E., Bellevue, WA 98008 (US).

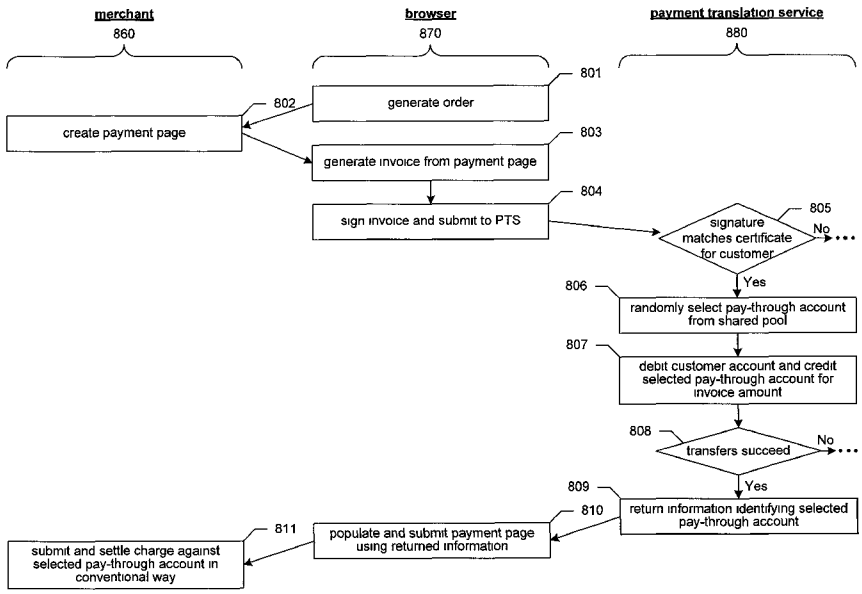
(74) **Agents: LAWRENZ, Steven, D.** et al; Perkins Coie LLP, P.O. Box 1247, Seattle, WA 9811 1-1247 (US).

(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, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available):* ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, 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:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(54) **Title:** MECHANISM FOR FRAUD-RESISTANT CONSUMER TRANSACTIONS



(57) **Abstract:** A facility for conducting a financial transaction is described. The facility receives a purchase order identifying a customer and an amount of a payment to be made by the identified customer to a payee. The customer identified by the purchase order has an individual account. The facility selects an account from a pool of accounts designated as being shared by a number of customers including the identified customer. The shared pool does not include the identified customer's individual account. The facility transfers the identified amount from the identified customer's individual account to the selected account of the shared pool. The facility causes information identifying a credit card number for the selected account of the shared pool to be provided to the payee for use in effecting the payment.

WO 2008/039942 A1

MECHANISM FOR FRAUD-RESISTANT CONSUMER TRANSACTIONS

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of US Provisional Application No. 60/848,570, filed September 27, 2006, which is hereby incorporated by reference in its entirety.

TECHNICAL FIELD

[0002] The described technology is directed to the field of technology supporting financial transactions, and, more particularly, to the field of technology supporting secure financial transactions.

BACKGROUND

[0003] The card numbers used by Customers in consumer credit and debit transactions today are vulnerable to fraud and misuse largely because they are static identifiers. That is, the same identifier that is used in a first transaction can immediately be used again in subsequent transactions not authorized by the Customer. Interception of the credit/debit number is not a concern now, since SSL, which is almost universally used, maintains a private communication channel between Customer and Merchant. However, by submitting the card number at all, the Customer gives up control of it to the Merchant - at least in principle. Dishonest merchants can abuse this control. More commonly, the Merchant accidentally reveals (i.e., loses) the card data to a dishonest intruder, or to a dishonest employee.

[0004] Card Organizations (VISA, MasterCard, etc.) and their participating Financial Institutions have tried to counter this vulnerability by demanding more identifying information (e.g., 'name', 'address', CCV, etc.) from the Customer as part of each transaction in order to authorize payment. However, all of these pieces of information are themselves only static identifiers. At best their use only delays

exposure to the very same fraud vulnerability, i.e., abuse by dishonest or insecure Merchants. In fact, requiring that customer to provide additional identifying information to the merchant may give rise to greater risk to identity theft or other forms of fraud enabled by this identifying information in the case of a dishonest or insecure merchant.

[0005] Information security techniques that address this threat much more robustly do exist. These techniques (e.g., digital signatures, one time use hardware tokens, etc.) achieve a much higher level of fraud protection by using a unique identifier for each transaction which can be generated only by the proper individual. Unfortunately, it has been difficult to introduce them to the general population because of the huge legacy effect imposed by the existing credit and debit card systems, as well as a reluctance by Customers to adopt less convenient processes, even when more secure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Figure 1 is a block diagram showing some of the components typically incorporated in at least some of the computer systems and other devices on which the facility executes.

[0007] Figures 2-5 are data flow diagrams showing interactions performed in accordance with the technique.

[0008] Figure 6 is a flow diagram showing steps typically performed by the facility in order to perform a system initialization process.

[0009] Figure 7 is a flow diagram showing steps typically performed by the facility in order to complete a customer registration process.

[0010] Figure 8 is a flow diagram showing steps typically performed by the facility in order to conduct a secure online payment.

DETAILED DESCRIPTION

[0011] A software facility for supporting fraud-resistant consumer transactions ("the facility") is provided that uses a shared, recirculating pool of "pay-through accounts" as the basis for individual consumer charges. When a customer has

placed an order with a web merchant and is ready to make an online payment to pay for the order, an invoice reflecting the amount of the payment to be made is signed using a private key of the customer and submitted to a payment translation service. After verifying that the signature is valid, the payment translation service selects a pay-through account from a pool of pay-through accounts that are shared across a number of different customers, such as all of the customers having an account at the same financial institution as the customer in question. Because each pay-through account in the pool can be used to make payments on behalf of different customers at different times, the pay-through accounts in the pool are sometimes referred to as "recirculating." The payment translation service then transfers the amount of the payment from the customer's account at the financial institution to the selected pay-through account, and returns information identifying a credit or debit card number associated with the selected pay-through account to the customer. This information is then submitted to the merchant, which uses it to submit and settle a charge against the selected pay-through account. This approach has the advantage that it uses standard, existing banking mechanisms and procedures, without the need to recognize charge transactions as corresponding to one-time use credit card numbers, or do any special processing for them. Ultimately, by standard settlement processes, the amount transferred from the customer's account to the selected pay-through account is transferred to the merchant.

[0012] In various embodiments, the facility provides a number of different approaches to exchanging any necessary data. These include having the customer cut and paste information between a first browser window corresponding to a browsing session with the merchant in the second browsing window corresponding to a browsing session with the payment translation service; a customized browser, or browser plug-in that automatically handles all necessary exchange of information; a shopping portal hosted by the payment translation service or financial institution, through which the customer does all of his or her shopping, and which intercepts exchanges between the customer's browser and the merchant's server as necessary to implement the facility; and augmentation of merchants' web sites to direct the customer to interact with the payment translation service in a way that results in

payment information for the pay-through account being provided by the payment translation service to the merchant.

[0013] By providing this payment translation service in some or all of the ways described above, the facility provides additional security to consumer transactions without imposing a significant burden on customers, without requiring any changes to the existing credit card and debit card charge settlement processes and mechanisms, and requiring few or no changes to the websites provided by and the processes performed by merchants.

[0014] Figure 1 is a block diagram showing some of the components typically incorporated in at least some of the computer systems and other devices on which the facility executes. These computer systems and devices 100 may include one or more central processing units ("CPUs") 101 for executing computer programs; a computer memory 102 for storing programs and data-including data structures, database tables, other data tables, etc.-while they are being used; a persistent storage device 103, such as a hard drive, for persistently storing programs and data; a computer-readable media drive 104, such as a CD-ROM drive, for reading programs and data stored on a computer-readable medium; and a network connection 105 for connecting the computer system to other computer systems, such as via the Internet, to exchange programs and/or data-including data structures. In various embodiments, the facility can be accessed by any suitable user interface including Web services calls to suitable APIs. While computer systems configured as described above are typically used to support the operation of the facility, one of ordinary skill in the art will appreciate that the facility may be implemented using devices of various types and configurations, and having various components, such as wireless telephones and similar devices.

[0015] Figures 2-5 are data flow diagrams showing interactions performed in accordance with the technique. Figure 2 shows a financial institution computer system 200 and a customer account 201. It shows an online merchant 210 from which the customer may make a purchase. It shows a card organization computer system 220 with which the online merchant computer system interacts to settle a charge transaction, and a financial institution service provider/PNV computer system

230. It shows a payment translation service 250 that establishes a shared pool of pay-through accounts 251 .

[0016] Figure 3 shows the customer performing a check-out process 361 at the merchant to conclude a purchase. The customer's browser transmits a digitally-signed invoice 362 to the payment translation service 250. In response, after verifying that the invoice was properly signed by the customer, the payment translation service chooses a particular pay-through account to use for the transaction.

[0017] Figure 4 shows the payment translation service performing a debit customer process 464, in which the existing customer account 201 is debited 482 and the selected pay-through account 251 is credited 481 , both by the amount indicated by the invoice. The payment translation service then transmits payment card information 465 associated with the selected pay-through account-such as a credit card or debit card number associated with the selected pay-through account—to the merchant and/or to the customer's computer system. This information for the pay-through account credit card number is inserted 466 into the merchant's check¬out form.

[0018] Figure 5 shows the merchant submitting a charge against the pay-through account payment card in a conventional matter to a charge-settlement process, in which the charge is settled in a conventional matter. In particular, the merchant sends the charge 567 to the card organization computer system 220. The card organization computer system 220 sends the charge 568 to the financial institution service provider computer system 230. The financial institution service provider computer system 230 sends the charge 569 to the financial institution computer system 200, which causes the merchant's account to be credited for the amount of the charge, and the selected pay-through account to be debited for the amount of the charge.

[0019] Figures 6-8 are flow diagrams showing sample implementations of processes performed by the facility. Figure 6 is a flow diagram showing steps typically performed by the facility in order to perform a system initialization process. The facility typically performs these steps once to initialize operations for a particular financial institution. In steps 601-605, the facility loops through each of a large

number of pay-through accounts to populate a pool of pay-through accounts that is shared across the customers having accounts with the financial institution, such as 1,000 pay-through accounts, or 10,000, or 100,000. In step 602, the facility creates a new checking account constituting a new pay-through account. The created checking account has an account number, a credit card number, and a zero balance. In some embodiments, the created checking account has a debit card number rather than a credit card number. In some embodiments, accounts of types other than checking accounts, such as savings accounts, are created to serve as pay-through accounts.

[0020] In step 603, the facility activates the credit card number for the pay-through account created in step 602. In step 604, the facility adds to the pay-through account created in step 602 to the shared pool of pay-through accounts. In step 605, if additional pay-through accounts remain to be created, then the facility continues in step 601 to create the next one, else these steps conclude.

[0021] Those skilled in the art will appreciate that the steps shown in Figure 6 and in each of the flow diagrams discussed below may be altered in a variety of ways. For example, the order of the steps may be rearranged; substeps may be performed in parallel; shown steps may be omitted, or other steps may be included; etc.

[0022] Figure 7 is a flow diagram showing steps typically performed by the facility in order to complete a customer registration process. The facility typically performs the customer registration process for each customer of the financial institution for whom payment translation is enabled. In step 701, the facility obtains a digital certificate associated with the customer that can be used to verify signatures made by the customer with a private key possessed by the customer and corresponding to the digital certificate. In some cases, the private key and digital certificate are created for the customer by or on behalf of the facility. In step 702, the facility associates the certificate with the customer's account with the financial institution, such as by storing the certificate in a row of a table corresponding to the customer's account. After step 702, these steps conclude, and the customer can proceed to make online payments using the facility. In some embodiments, the facility associates authorization credentials other than a digital certificate with the

customer, such as a password used by the customer, an image feature used to authenticate the user, biometric attributes used to authenticate the user, details of the challenge-response mechanism, details of a time-based access generator, etc. Where the authentication credentials already associated with the customer's account, such as where a password used by the customer to access the financial institution's online banking website is already associated with the customer's account, then the steps of Figure 7 are unnecessary and can be omitted by the facility.

[0023] Figure 8 is a flow diagram showing steps typically performed by the facility in order to conduct a secure online payment. The flow diagram is organized into three columns: a column 860 containing steps performed by a merchant's server, a column 870 containing steps performed by the customer's browser, and a column 880 containing steps performed by the payment translation service. As will be discussed below in greater detail, some of these steps can be performed in ways different than those shown, and/or by different computer systems.

[0024] In step 801, the customer's browser generates an order by interacting with the merchant's website. In response, in step 802, the merchant's server creates a payment page - i.e., Checkout page - that includes both a total amount due from the customer and fields for providing payment information identifying a credit card to pay that amount. In step 803, the browser uses information from the payment page received from the merchant to generate an invoice, which contains at least the amount due from the payment page. In step 804, the browser signs the invoice using the customer's private key, and submits the signed invoice to the payment translation service, along with information identifying the customer, such as the customer's account number.

[0025] In step 805, if the payment translation service is able to verify the signature on the invoice it receives from the customer's browser against the certificate for the customer, then the facility continues in step 806, else this process terminates. In step 806, the payment translation service selects a pay-through account from the shared pool of pay-through accounts. In some embodiments, the selection of step 806 is random. In some embodiments, the facility bases this selection on such factors as the balances of the pay-through accounts, and/or the

times at which the pay-through accounts were last selected for use in a transaction. In some embodiments, only pay-through accounts whose balances are zero are eligible for selection.

[0026] In step 807, the payment translation service debits the customer's account and credits the pay-through account selected in step 806, both for the amount due shown by the invoice. In some embodiments, the debited customer account is a depositary account of the customer's, such as a checking, savings, or brokerage account. In some embodiments, the debited customer account is a credit or charge account or other line of credit. In some embodiments, the facility uses ACH transfers to effect the debit and credit options of step 807. In step 808, if both the debit and credit operations of step 807 succeed, then the facility continues in step 809, else any succeeding debit or credit operation is reversed and this process terminates. In step 809, the payment translation service returns information identifying the pay-through account selected in step 806 to the customer's browser. Such information may include, for example, a credit card number, expiration date, CCV, account holder name, billing address, etc. In some embodiments, the payment translation service further stores a record of the transaction, identifying at least the customer account, the pay-through account, and the amount, to facilitate later reversal of the transaction if this turns out to be necessary.

[0027] In step 810, the customer's browser populates and submits the payment page created by the merchant in step 802 using the information returned by the payment translation service in step 809. In step 811, when the merchant's server receives the submitted payment page, the merchant uses standard, conventional techniques to submit and settle a charge for the amount due against the pay-through account selected in step 806. This entire submission and settlement process can be performed by all of the involved systems without any understanding about the nature of the pay-through account or special-case processing therefor. These steps then conclude.

[0028] In some embodiments (not shown), when the pending charge or charges are settled against a pay-through account—i.e., its balance returns to zero—as part of returning the pay-through account to the pool for re-use, the facility performs a verification information reset process. This process involves altering some or all of

the verification information associated with the pay-through account, such as expiration date, CCV, cardholder name, billing address, etc. By performing such alterations, the facility further reduces any opportunity for fraudulent re-use of pay-through accounts.

[0029] In various embodiments, the facility uses a variety of techniques to manage communications between the customer, the merchant, and the payment translation service. These include, but are not limited to, the following:

Customer Cut-and-Paste

[0030] The two communication channels, (1) between Customer and Merchant, and (2) between Customer and FI are implemented as two distinct web browser "windows," or "tabs." The Customer submits to the Merchant the payment chit information she received from the PTS via "cut-and-paste" - a feature already available in all major browsers.

[0031] This approach has the advantage that there is no need for client software that lies outside of standard web browser functionality. All new functionality is embodied in PTS web pages so that deployment is trivial. No Merchant participation is required.

Shopping Portal. Hosted by the FI or PTS

[0032] Customers shop at Merchant sites via a web "connection" that goes "through" the Customer's FI, or trusted representative of the FI. During the most of the shopping experience, the intermediate FI server merely passes data to and from Customer and Merchant. Only at point of "checkout" does the FI server modify the data stream. It does so by automating the "cut-and-paste" operation in that variation. In some embodiments, Customers authenticate themselves at the beginning of the shopping session, so that per-transaction authentication may be redundant, and hence is eliminated in some embodiments.

[0033] In various embodiments, the intermediate FI connection is enabled by one of two mechanisms:

1. Customers are encouraged to do their online shopping safely by starting at a site such as http://safeshop.mvFI.com .

2. Customer web browser is configured to use FI server as a proxy server via a transparent protocol such as SOCKS for all browser traffic.

[0034] This approach has all the advantages of customer cut-and-paste. Additionally, there is no impact on customer shopping experience, creating no disincentive for using the facility.

Special Purpose Client Browser Plug-in

[0035] A browser plug-in approach, similar to the mechanism by which Macromedia's nearly ubiquitous Flash player is integrated into browsers, can similarly avoid creating any adverse impact on customer shopping experience. In fact, the shopping experience my even be improved since the plug-in can automate much of the form filling required at checkout time. Also, the potential to steer Customers towards using the new payment methodology is good. Again, absolutely no Merchant participation is required.

[0036] The plug-in may either provide an explicit mechanism for the customer to invoke a secure payment, and/or may automatically recognize merchant Checkout pages and automatically invoke a secure payment in a response. As for the former, the plug-in may, for example, provide a toolbar button for invoking a secure payment. As to the latter, the plug-in can automatically recognize a Checkout page by examining the document object model ("DOM") for each page retrieved and displayed by the browser, looking for such indicators of a Checkout page as fields having names such as "card number," "CCV," "billing address," etc. The plug-in can also analyze content on each page other than field names, including text or image content, as well as top-level attributes for the page such as the protocol used to retrieve the page.

Adapted Browser

[0037] Any techniques implemented in a browser plug-in can instead or also be directly integrated into shipping versions of one or more browsers. A customer using such a browser would not need to download or install the browser plug-in described above.

Merchant Cooperation

[0038] Merchants "embed" the payment functionality in their Checkout pages. In particular, a merchant adds to its Checkout page a control, such as a button, that, when activated by the user, sends a request to the PTS server providing invoice data. The PTS server returns a web page that performs customer authentication, after which it assigns a pay-through account and returns a copy of the merchant's Checkout page with information about the selected pay-through account pre-populated. The user can then submit this copy of the merchant's Checkout page to the merchant by activating a submit control included in the page returned by the PTS server.

[0039] The technology to support this is partially illustrated by, for example, embedded YouTube videos. Examples of existing payment systems that require Merchant participation are PayPal and Google Checkout.

[0040] In some embodiments, rather than collecting customer authentication information in a webpage served by the PTS server, the merchant further adds a mechanism to its Checkout page that collects this authentication information from the user when the control is activated and forwards it to the PTS server. In some embodiments, this functionality is provided using a javascript window or other appropriate approaches.

[0041] This approach has the advantage that Customer shopping experience can be enhanced and behavior modifications encouraged without the need for a client plug-in. Additionally, much of the form parsing capability required of the software can be drastically simplified if not completely eliminated.

[0042] Those skilled in the art will appreciate that a variety of other mechanisms may be used to exchange the data used by the facility.

[0043] While the foregoing principally describes transaction authorization from the customer taking the form of a digital signature on an invoice or purchase order that is based upon information from the merchant, in various embodiments the facility employs a wide variety of other authorization mechanisms. For example, authorization made be performed using a customer password, such as a password already used by the customer to access the financial institution's online banking site;

an image features selection authentication system; a challenge and response authentication system; a time-based access code generator; or a variety of other mechanisms.

[0044] It will be appreciated by those skilled in the art that the above-described facility may be straightforwardly adapted or extended in various ways. For example, the facility may be used with various kinds of financial institutions, merchants, and account types. While the foregoing description makes reference to particular embodiments, the scope of the invention is defined solely by the claims that follow and the elements explicitly recited therein.

CLAIMS

I claim:

1. A method in a computing system for conducting a financial transaction, comprising:

creating a pool of accounts to be shared by a plurality of customers;

activating a credit card number for each of the accounts of the shared pool;

receiving a purchase order identifying a customer among the plurality of customers and an amount of a payment to be made by the identified customer to a payee, the purchase order bearing a signature, the identified customer having an individual account not among the shared pool of accounts;

only if the signature can be verified to have been formed by the identified person:

selecting one of the accounts of the shared pool;

debiting the identified amount from the identified customer's individual account;

crediting the identified amount to the selected account of the shared pool; and

causing to be provided to the payee information identifying the credit card number activated for the selected account of the shared pool,

such that the payee may submit and settle a credit card charge for the identified amount against the identified credit card number, and ultimately against the selected account of the shared pool, without having to map the provided information identifying the credit card number to the identified customer's individual account.

2. A computer-readable medium whose contents cause a computing system to perform a method for conducting a financial transaction, the method comprising:

receiving a purchase order identifying a customer and an amount of a payment to be made by the identified customer to a payee, the identified customer having an individual account;

in response to receiving the purchase order, selecting an account from a pool of accounts designated as being shared by a plurality of customers including the identified customer, the shared pool not including the identified customer's individual account;

transferring the identified amount from the identified customer's individual account to the selected account of the shared pool; and

causing information identifying a credit card number for the selected account of the shared pool to be provided to the payee for use in effecting the payment.

3. The computer-readable medium of claim 2, the method further comprising, before the selecting, transferring, and causing, verifying that the identified customer has authorized the purchase order.

4. The computer-readable medium of claim 3 wherein the verifying comprises successfully verifying that a signature on the purchase order is consistent with a digital certificate associated with the identified customer.

5. The computer-readable medium of claim 3 wherein the verifying comprises determining that a password provided by the identified customer matches a password associated with the identified customer.

6. A method in a computing system for conducting a financial transaction, comprising:

receiving a purchase order identifying a customer and an amount of a payment to be made by the identified customer to a payee, the identified customer having an individual account;

selecting an account from a pool of accounts designated as being shared by a plurality of customers including the identified customer, the shared pool not including the identified customer's individual account;

transferring the identified amount from the identified customer's individual account to the selected account of the shared pool; and

causing information identifying a payment card for the selected account of the shared pool to be provided to the payee for use in effecting the payment.

7. The method of claim 6 wherein the information identifying a payment card comprises a credit card number.

8. The method of claim 6 wherein the information identifying a payment card comprises a debit card number.

9. The method of claim 6 wherein the information identifying the payment card comprises a payment card number associated with the selected account of the shared pool, together with verification information associated with the payment card number that is distinct from the payment card number.

10. The method of claim 9 wherein the verification information comprises a CCV.

11. The method of claim 9 wherein the verification information comprises at least a portion of a billing address.

12. The method of claim 9, further comprising:

determining that a charge transaction submitted by the payee against the selected account of the shared pool has been settled;

in response to the determining, altering the verification information associated with the payment card number;

subsequent to the altering, receiving a second purchase order identifying a second customer having an individual account and a second amount to be paid to a second payee; and

in response to receiving the second purchase order:

transferring the second identified amount from the identified second customer's individual account to the selected account of the shared pool, and

causing to be provided to the second payee the payment card number associated with the selected account of the shared pool, together with altered verification information associated with the payment card number.

13. The method of claim 6 wherein the information identifying a payment card for the selected account of the shared pool is provided to the payee by providing the information identifying a payment card for the selected account of the shared pool to the identified customer to enable the identified customer to manually paste the identifying information into one or more fields of a form posted to a web server operating on behalf of the payee.

14. The method of claim 6 wherein a proxy server provides to the payee the information identifying a payment card for the selected account of the shared pool by automatically injecting the identifying information into a browser session between the identified customer and a web server operating on behalf of the payee.

15. The method of claim 6 wherein the information identifying a payment card for the selected account of the shared pool is provided to the payee by automatically prefilling the identifying information into one or more fields of a form which is then posted to a web server operating on behalf of the payee,
and wherein the automatic prefilling is performed by a component integrated into a browser used by the customer, wherein the integration is performed by an extensibility mechanism provided in connection with the browser.

16. The method of claim 15 wherein extensibility mechanism a browser plug-in.

17. The method of claim 15 wherein extensibility mechanism a browser toolbar.

18. The method of claim 6 wherein the information identifying a payment card for the selected account of the shared pool is provided to the payee

by automatically prefilling the identifying information into one or more fields of a form which is then posted to a web server operating on behalf of the payee,
and wherein the automatic prefilling is performed by functionality included in a version of a browser shipped by the browser's lender.

19. The method of claim 6 wherein the information identifying a payment card for the selected account of the shared pool is provided to the payee by automatically prefilling the identifying information into one or more fields of a form which is then posted to a web server operating on behalf of the payee,
and wherein the automatic prefilling is performed before the form is served to a browser used by the customer.

20. One or more hardware devices collectively providing a payment information data structure corresponding to a payment for a distinguished amount on behalf of a distinguished customer having an account for exclusive use of the customer, comprising:

a credit card number having a one-to-one relationship with a distinguished one of a pool of accounts shared across a plurality of customers including the distinguished customer, the distinguished shared account having been randomly selected from shared accounts among the pool of shared accounts without regard for the specific identity of the distinguished user, the distinguished amount having been transferred from the distinguished customer's account to the distinguished shared account; and

at least one piece of confirmatory information associated with the credit card number,
such that the contents of the data structure may be submitted by a merchant to a credit card charge clearance network to obtain payment of the distinguished amount.

21. The hardware devices of claim 20 wherein the hardware devices comprise a computer memory that stores the payment information data structure.

22. The hardware devices of claim 20 wherein the hardware devices comprise a data transmission network that conveys the payment information data structure.

23. The hardware devices of claim 20 wherein the confirmatory information comprises a cardholder name associated with the credit card number that does not match the distinguished customer's name.

24. The hardware devices of claim 20 wherein the confirmatory information comprises a billing address associated with the credit card number at which the distinguished customer does not receive mail.

25. A method for conducting financial transactions, comprising:

receiving a purchase order identifying a first customer and an amount of a first payment to be made by the first customer to a first payee, the first customer having an individual account;

transferring the amount of a first payment from the first customer's individual account to a distinguished pay-through account;

causing information identifying a payment card number for the distinguished pay-through account to be provided to the first payee for use in effecting the first payment;

receiving a purchase order identifying a second customer and an amount of a second payment to be made by the second customer to a second payee, the second customer having an individual account;

transferring the identified amount of the second payment from the second customer's individual account to the distinguished pay-through account; and

causing information identifying a payment card number for the distinguished pay-through account to be provided to the second payee for use in effecting the second payment.

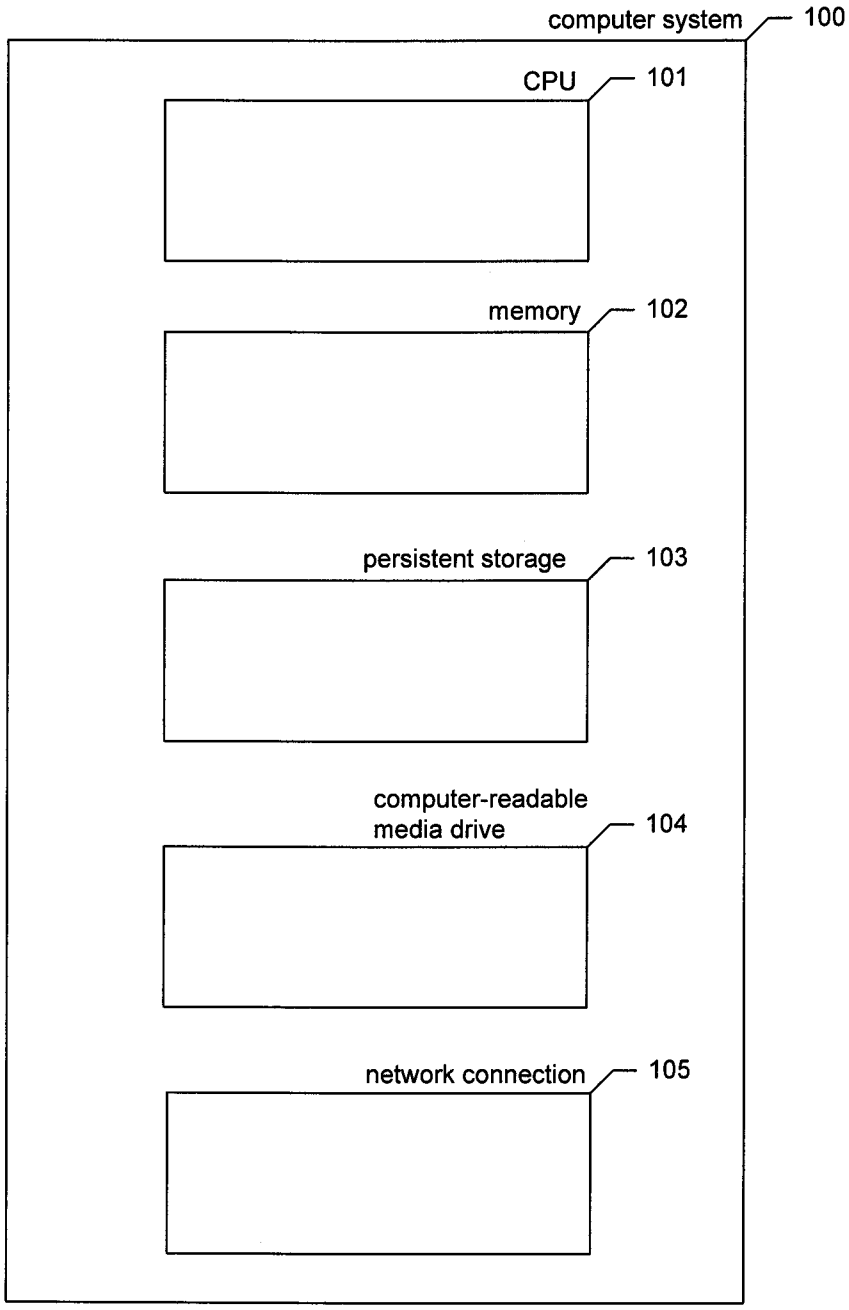

computer system
100
CPU
101
memory
102
persistent storage
103
computer-readable
media drive
104
network connection
105

FIG. 1

Private Pay e-Commerce Transaction

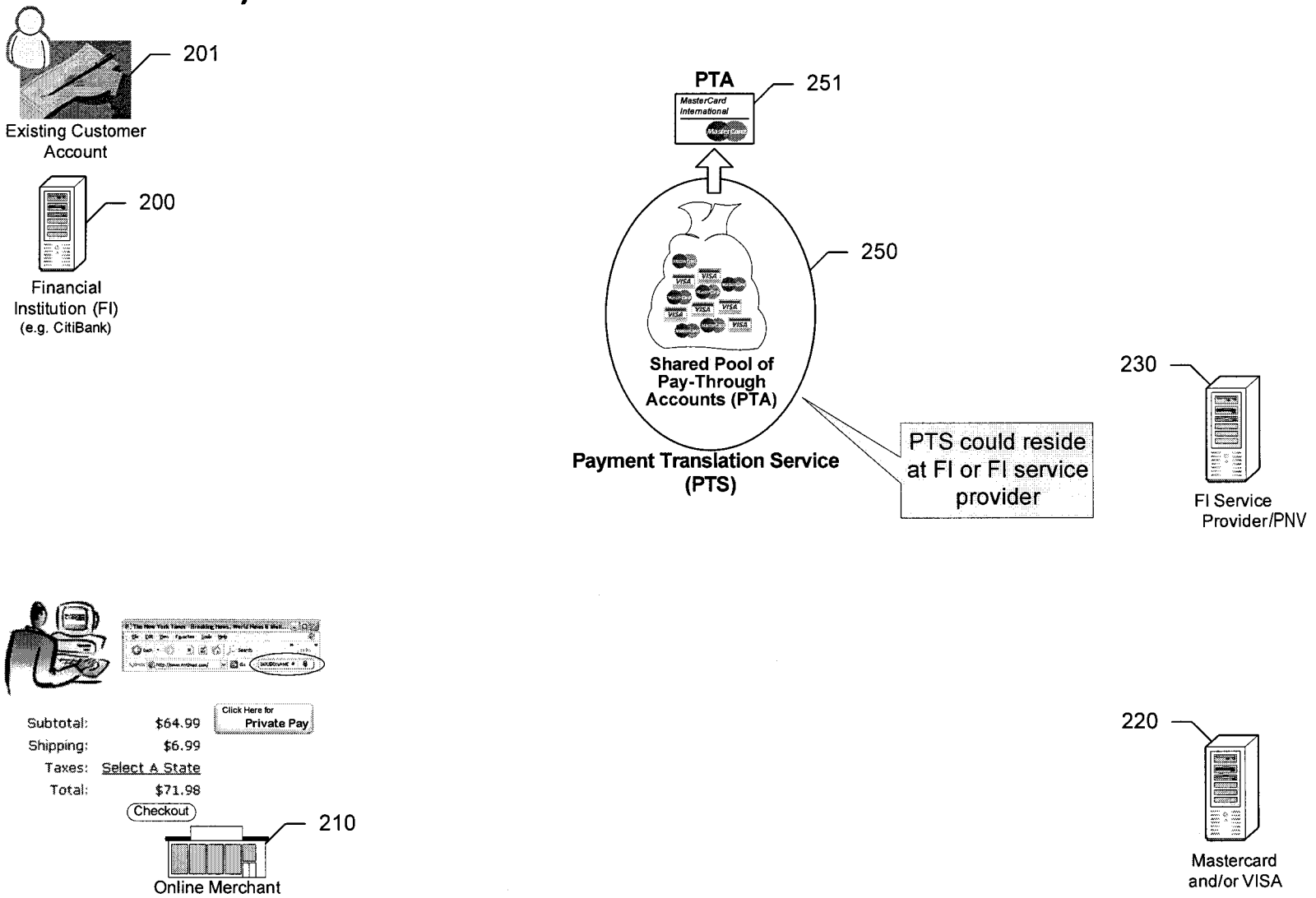


FIG. 2

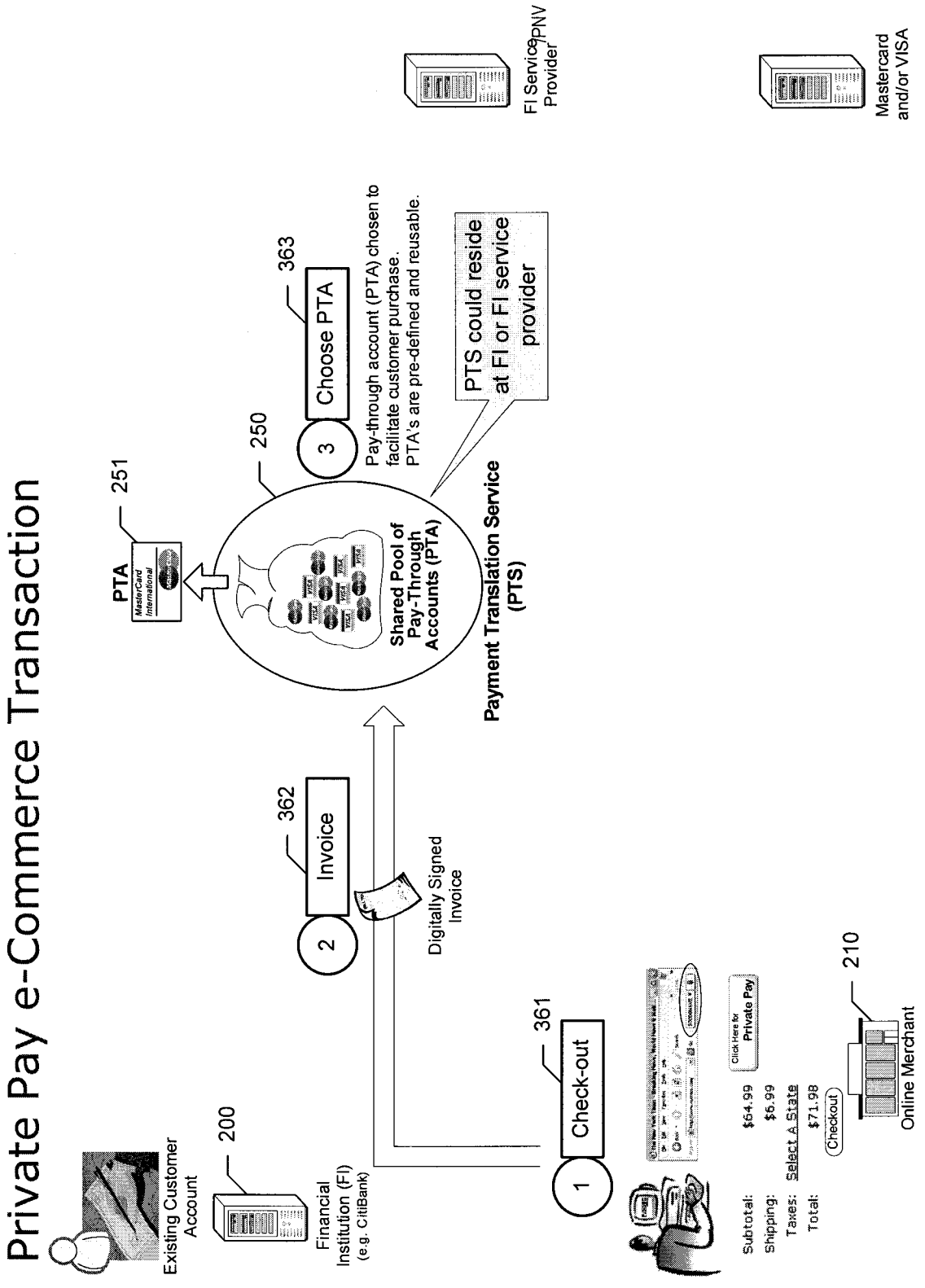

Private Pay e-Commerce Transaction
Existing Customer Account
200
Financial Institution (FI) (e.g. CitiBank)
1
Check-out
361
2
Invoice
362
Digitally Signed Invoice
3
Choose PTA
363
Pay-through account (PTA) chosen to facilitate customer purchase.
PTA's are pre-defined and reusable.
250
Shared Pool of Pay-Through Accounts (PTA)
Payment Translation Service (PTS)
PTS could reside at FI or FI service provider
PTA
251
FI Service Provider
PNV
Mastercard and/or VISA
Subtotal: $64.99
Shipping: $6.99
Taxes: Select A State
Total: $71.98
Checkout
Click Here for Private Pay
210
Online Merchant

FIG. 3

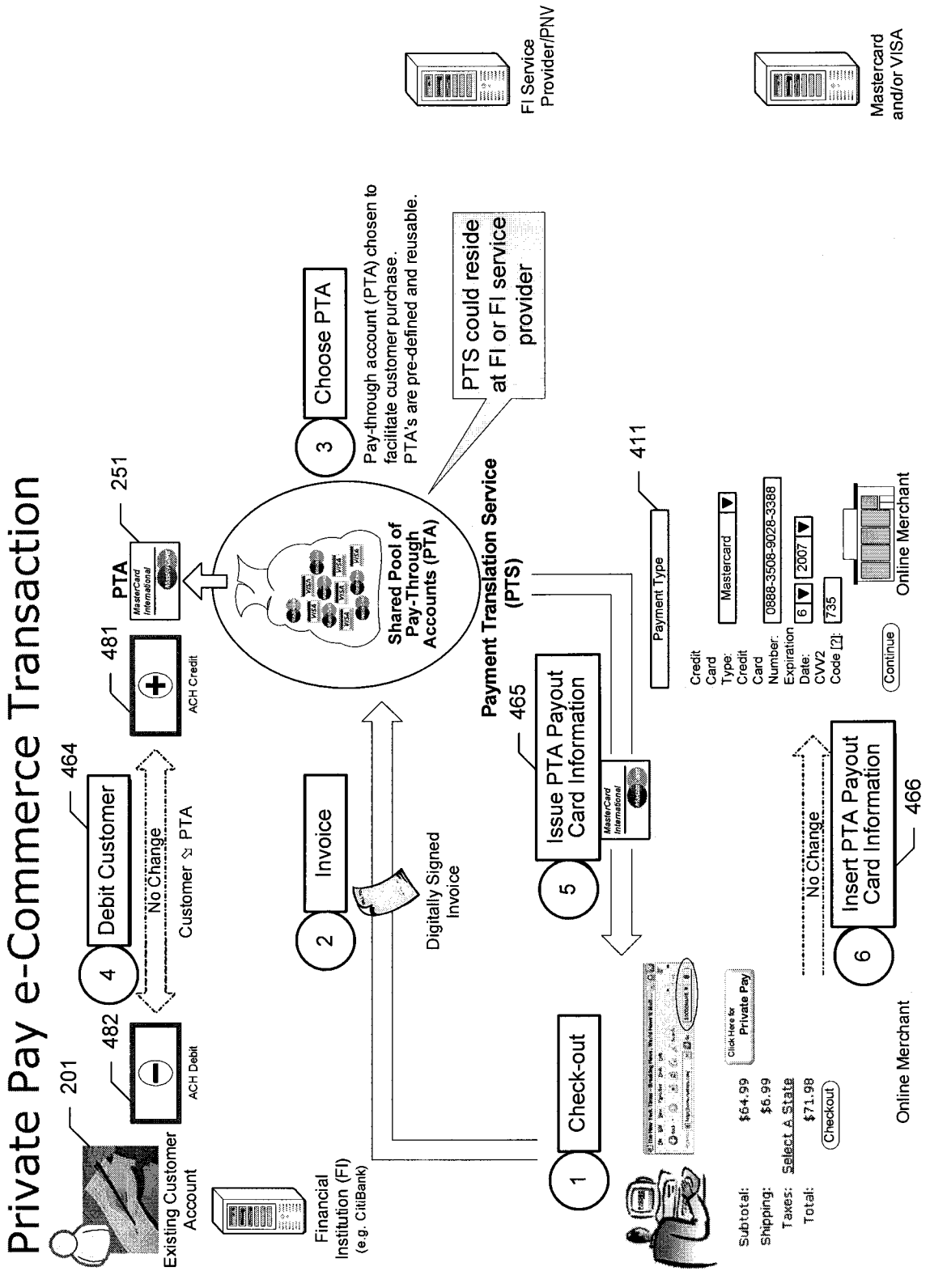

Private Pay e-Commerce Transaction
201
Existing Customer Account
482
ACH Debit
Financial Institution (FI) (e.g. CitiBank)
464
4 Debit Customer
No Change
Customer ⇆ PTA
481
ACH Credit
PTA
251
2 Invoice
Digitally Signed Invoice
3 Choose PTA
Pay-through account (PTA) chosen to facilitate customer purchase. PTA's are pre-defined and reusable.
Shared Pool of Pay-Through Accounts (PTA)
PTS could reside at FI or FI service provider
Payment Translation Service (PTS)
465
5 Issue PTA Payout Card Information
411
Payment Type
Credit Card Type:
Credit Card Number:
Expiration Date:
CVV2 Code [2]:
Mastercard
0888-3508-9028-3388
6
2007
735
Continue
Online Merchant
FI Service Provider/PNV
Mastercard and/or VISA
1 Check-out
Subtotal: $64.99
Shipping: $6.99
Taxes: Select A State
Total: $71.98
Checkout
Click Here for Private Pay
No Change
6 Insert PTA Payout Card Information
466
Online Merchant

FIG. 4

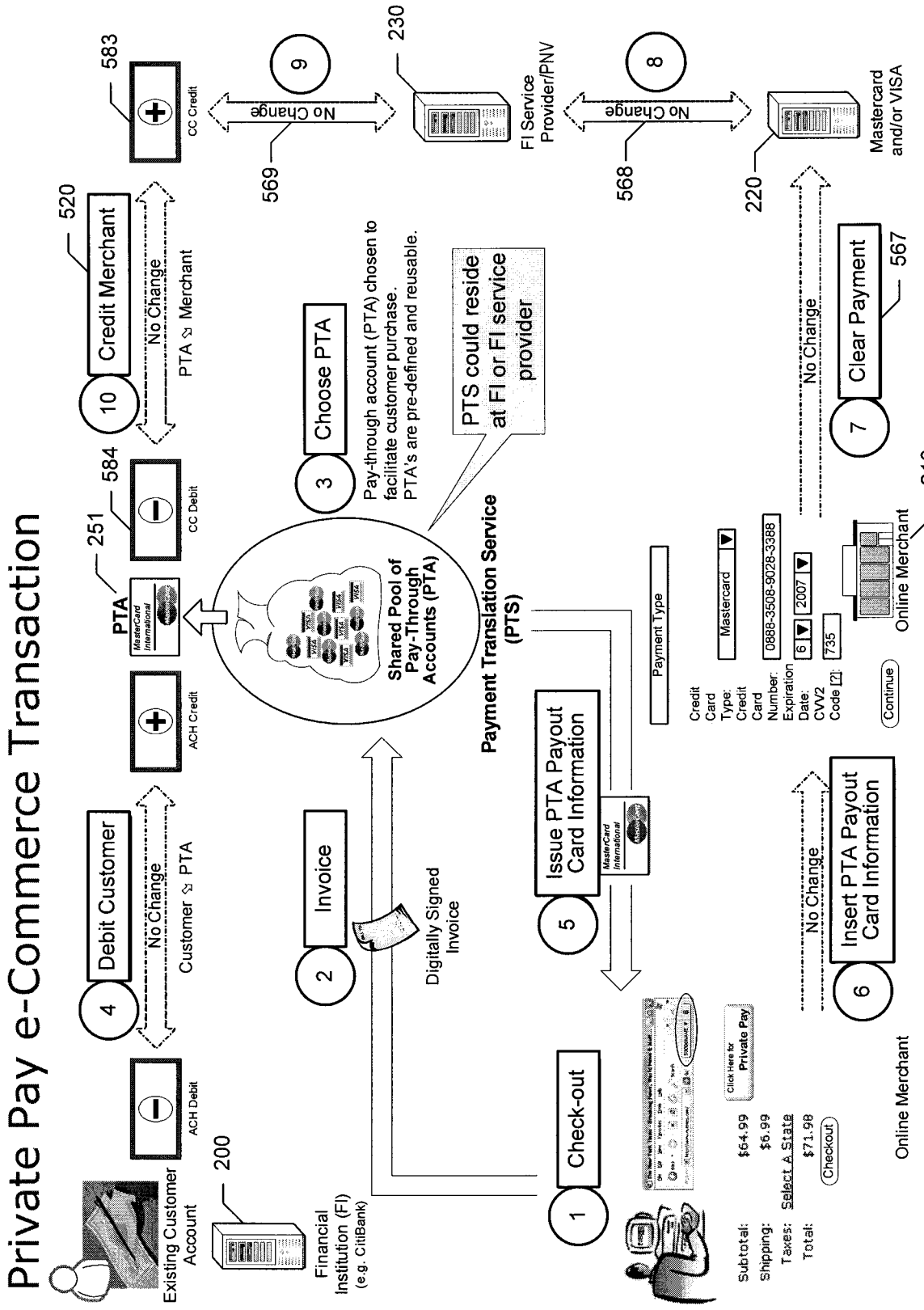

Private Pay e-Commerce Transaction
Existing Customer Account
200
Financial Institution (FI) (e.g. CitiBank)
ACH Debit
ACH Credit
CC Debit
CC Credit
PTA
251
584
583
520
Credit Merchant
Debit Customer
No Change
Customer ⇆ PTA
No Change
PTA ⇆ Merchant
1 Check-out
2 Invoice
Digitally Signed Invoice
3 Choose PTA
Pay-through account (PTA) chosen to facilitate customer purchase.
PTA's are pre-defined and reusable.
Shared Pool of Pay-Through Accounts (PTA)
PTS could reside at FI or FI service provider
Payment Translation Service (PTS)
4 Debit Customer
5 Issue PTA Payout Card Information
6 Insert PTA Payout Card Information
7 Clear Payment
8 No Change
9 No Change
10 Credit Merchant
569
568
220
230
210
567
FI Service Provider/PNV
Mastercard and/or VISA
Online Merchant
Payment Type
Credit Card Type:
Mastercard
Credit Card Number:
0888-3508-9028-3388
Expiration Date:
6
2007
CVV2 Code [2]:
735
Continue
Subtotal: $64.99
Shipping: $6.99
Taxes: Select A State
Total: $71.98
Checkout
Click Here for Private Pay

FIG. 5

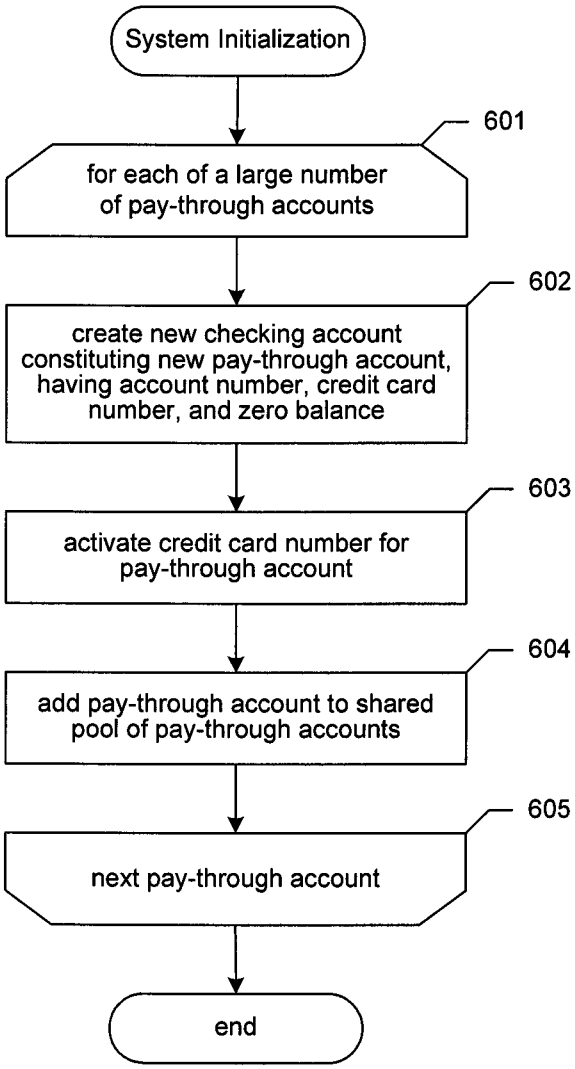

System Initialization
601
for each of a large number of pay-through accounts
602
create new checking account constituting new pay-through account, having account number, credit card number, and zero balance
603
activate credit card number for pay-through account
604
add pay-through account to shared pool of pay-through accounts
605
next pay-through account
end

FIG. 6

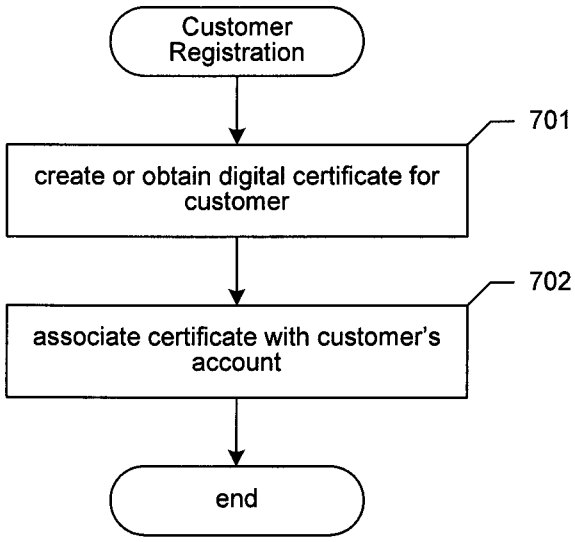

Customer Registration
701
create or obtain digital certificate for customer
702
associate certificate with customer's account
end

FIG. 7

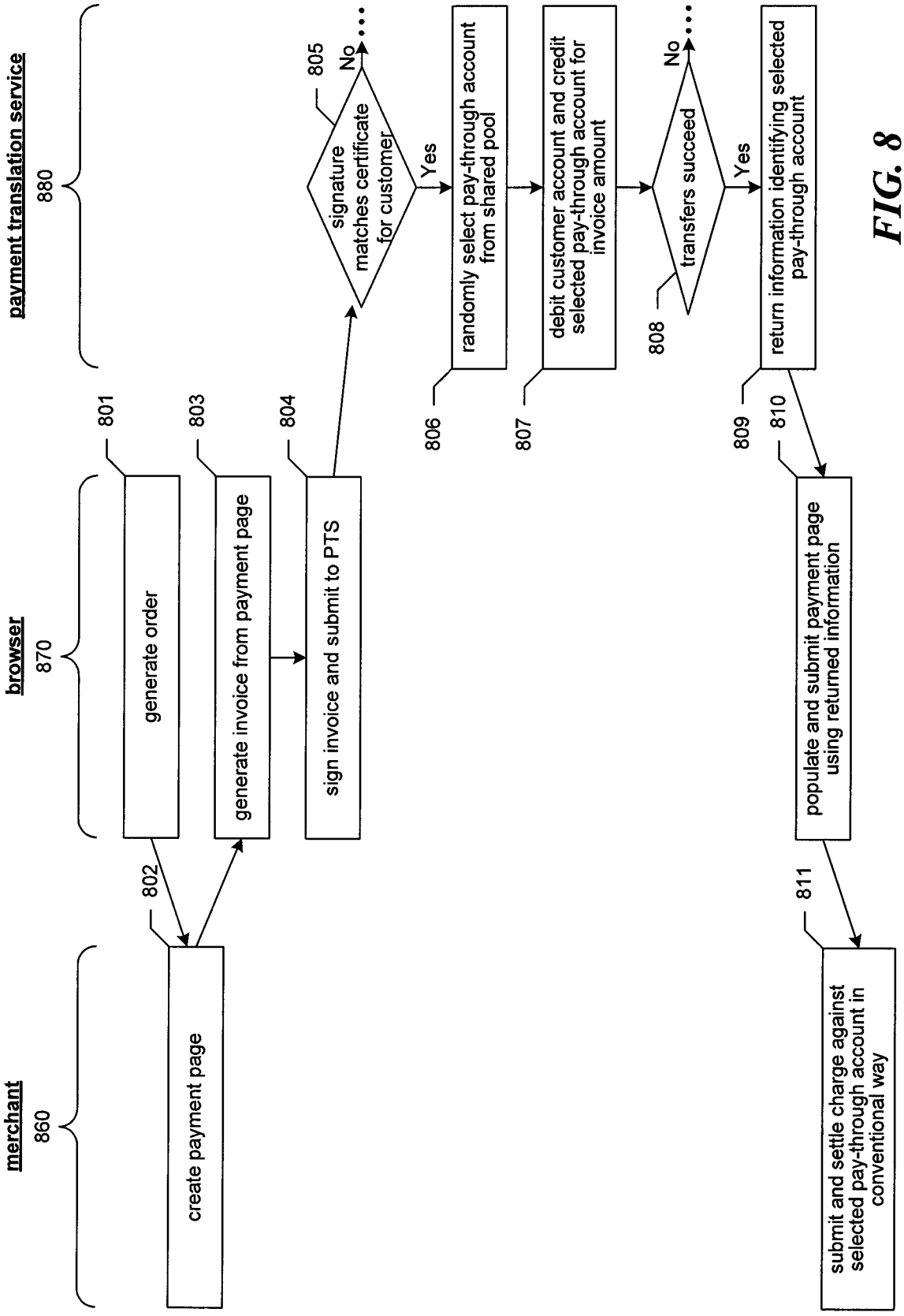

merchant
860
create payment page
802
browser
870
generate order
801
generate invoice from payment page
803
sign invoice and submit to PTS
804
payment translation service
880
805
signature matches certificate for customer
No
Yes
806
randomly select pay-through account from shared pool
807
debit customer account and credit selected pay-through account for invoice amount
808
transfers succeed
No
Yes
809
return information identifying selected pay-through account
810
populate and submit payment page using returned information
811
submit and settle charge against selected pay-through account in conventional way

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 07/79772

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 40/00 (2007.10)
USPC - 705/40
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8): G06Q 40/00 (2007.10)
USPC: 705/40

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 705/1 , 35, 39, 77; 902/41

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Electronic databases: USPTO WEST (PGPB, USPT, EPAB, JPAB); Google Scholar
Search Terms Used: shared or common pool or accounts, user or customer or consumer, transaction fraud, credit or debit or purchase card, payment or purchase order or payee, selecting or identifying account, identifying user or customer or consumer et

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2006/0064372 A1 (Gupta) 23 March 2006 (23.03.2006) Abstract, Fig 1-2, and para [0005], [0018]-[0027], [0033]-[0040], [0052]-[0062])	1-25
Y	US 2005/0131826 A1 (Cook) 16 June 2005 (16.06.2005) Abstract, and Fig 4 & 7, and para [0004]-[0008], [0017]-[0022], [0038]-[0043])	1-25
A	US 2005/0246278 A1 (Gerber et al.) 03 November 2005 (03.11.2005)	1-25
A	US 6,853,987 B1 (Cook) 08 February 2005 (08.02.2005)	1-25
A	US 2004/0039686 A1 (Klebanoff) 26 February 2004 (26.02.2004)	1-25

☐ Further documents are listed in the continuation of Box C. ☐

♦ Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 December 2007 (24.12.2007)	**0 1 FEB 2008**
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774