(54) Title: SYSTEM FOR AND METHOD OF EFFECTING PAYMENTS ONLINE AND OFFLINE

(57) Abstract:
A method and system for effecting payments online and offline is disclosed wherein an online payment service (OPS) allows a customer to utilize a credit card issued to the OPS for purchasing on the Internet. The customer provides the Internet merchant with the OPS issued credit card information. Therefore, the customer may make a purchase without providing his personal credit card information. The merchant authenticates and bills the OPS without having any knowledge of the customer, thereby maintaining the customer’s privacy. In another embodiment, there is provided a payment system wherein customers can assign restrictions to a transaction instrument.
Abstract

A method and system for effecting payments online and offline is disclosed wherein an online payment service (OPS) allows a customer to utilize a credit card issued to the OPS for purchasing on the Internet. The customer provides the Internet merchant with the OPS issued credit card information. Therefore, the customer may make a purchase without providing his personal credit card information. The merchant authenticates and bills the OPS without having any knowledge of the customer, thereby maintaining the customer's privacy. In another embodiment, there is provided a payment system wherein customers can assign restrictions to a transaction instrument.
SYSTEM FOR AND METHOD OF EFFECTING PAYMENTS ONLINE AND OFFLINE

Field

The invention relates generally to commercial transactions between parties including online transactions, and more particularly to a system and method of effecting payments in such transactions.

Background

There has been explosive growth in the use of credit cards and debit cards in commercial transactions. There has been an explosive growth in the popularity and importance of electronic commerce and in the use of credit cards and debit cards online. This has led to a corresponding growth in fraudulent transactions including card theft, card cloning and misappropriation of credit information and bank account numbers. The overall growth of the Internet is mirrored by the e-commerce market. Wharton Research, January 2000 predicts that consumer online spending in North America will reach $133 billion within four years. Reasons for this staggering growth rate is due to the rapid increase in access to the Internet, good marketing, and the relative convenience of shopping online. Fraud in electronic commerce is more difficult to prevent.

Secondly as the number of online purchasers and the number of purchases increase, so too does the information trail regarding these transactions. Since the transaction instrument for most online purchases is a credit card, purchasers of products on the Internet are usually required to provide the vendor with personal information (often far beyond merely his name and address) and generally his credit card number and expiry date. Purchase and demographic information is gathered by vendors, by e-commerce enablers and by other interested parties. Often the party gathering this information utilizes or sells the collected information. A demographic profile of the customer,
including the types of purchases that he makes and the types of websites that he visits has a value to many companies, particularly those wishing to direct advertising to the customer.

Not only do databases gather personal information provided by purchasers who fill out online purchase forms, they also gather information related to the purchaser’s credit card transactions.

In a study undertaken by Ernst & Young, 97% of potential customers who did not purchase online were uncomfortable sending credit card information over the Internet. The user may be uncomfortable for a number of reasons. He may not trust the Internet vendor to limit the use of the credit card to the intended transactions. Or, he simply may want to make his purchase anonymously, not unlike making a cash purchase at a grocery store.

While many purchasers are unconcerned with providing personal and credit card information, particularly to major vendors, there is a significant segment of the population that is hesitant to supply such information. These users are not only concerned that their credit card may be used fraudulently; rather, they are also concerned that others may know what they have purchased with their credit card, and from whom. This hesitancy may be based upon a concern regarding the use of such information. It may be because the user does not want to be placed on an Internet mailing list. Or, in a growing number of cases, it may simply be because the purchaser wants to maintain his privacy.

Whether for reasons of maintaining anonymity, reluctance to provide information that is thought to be extraneous, or simply because of the time involved in filling out a form, some Internet purchasers are hesitant to provide this information. Some are reluctant to use their credit cards on the Internet, particularly in dealing with unknown merchants, because they are not comfortable with what will become of their history of purchases.
Beyond privacy concerns, Internet sales are sometimes lost because the merchant can not afford to accept a credit card for a purchase value that is less than some minimum amount dictated by the credit card company.

Some solutions are available to solve some of these problems.

A number of payment systems and controls with in those systems have been developed, such as travellers’ cheques, signatures on cards, authorization systems, personal information inclusions on physical cards, and expiry dates. However, a system of precise control over card use does not exist. Reflecting the need for confidentiality, a number of companies have been established to provide Internet users with identity-management services. For example, companies exist that provide customers with the ability to browse the web without revealing their identity. Other companies provide an identity manager that allows the user to control what bits of personal information are shared or sold to marketers. Other companies offer services that allow the use of anonymous email or anonymous chat room discussions.

For users wishing to avoid filling in forms, a number of these identity management systems are available in which the customer needs only to fill in one form. A formfiller company then provides the customer with a service that automatically fills in any future forms related to purchases made on the Internet. In general, the information provided by the customer to the formfiller company need not be an accurate depiction of the customer other than the information related to his credit card.

Identity management of formfiller companies address only part of this problem. They do not address the concern of the user wanting to make a purchase online using his credit card because to make such a purchase the credit card number (and consequently the identity of the user) must be divulged.

While the credit card is still the simplest transaction instrument for effecting payments online, there are a number of other methods available to pay for products purchased on the Internet. These include digital checking accounts whereby electronic checks are sent
over the Internet and cleared on-line. This latter method includes smart cards and stored value cards. While these methods can facilitate microcash purchases and need not utilize the customer’s credit card on-line, they are not designed to protect the user’s identity or his purchase history.

Another method of making online purchases without using a credit card is by using some form of digital cash. Companies may provide a digital cash service that allows the user to maintain the same anonymity as with real cash. These services also allow the user to make small purchases without the merchant being charged with a minimum transaction cost. The drawback of these digital cash services is that they require the cooperation of the merchant. A purchase can not be made with a merchant that does not subscribe to the service.

For those not having a credit card or not wishing to make a credit card purchase, there are services available which will allow the purchaser to be billed through an Internet Service Provider or through the user’s telephone company. These purchases, however, are not anonymous and require the cooperation of the merchant or subscription to an outside payment agency.

For a customer wanting to maintain anonymity for his financial transactions, a number of companies provide offshore credit cards. This service, however, is generally only available to customers willing to maintain significant cash balances with the issuing institution. The set up and maintenance costs of such accounts can also be very expensive.

A customer wishing to maintain Internet and purchase anonymity while maintaining the easy use of a credit card currently has to establish a relationship with several companies and interface those services in a somewhat complicated and expensive manner.

One way a user can completely maintain his anonymity in making a purchase is to use an anonymous web browser services and to also utilize an offshore credit card that does not relate to this true identity. Such credit cards are available from a number of offshore
banks but they are expensive both for the original set up and for the sizeable cash balance required from the issuer. This is a time consuming and cumbersome process. The offshore credit card remains vulnerable to abuse.

Banks and merchants also would benefit from increased security because they often take the credit risk of fraudulent credit card use and can reduce the significant costs they incur in preventing, detecting and recovering abused credit.

There is also risk associated with offline purchases, namely the risk of fraud and credit theft. These risks exists to both the transaction instrument holder and the issuing bank. Currently, there are minimal restrictions available to personal transaction instrument holders for modification to the transaction instrument other than credit limit and cancelling the transaction instrument. These restrictions, however, are in most cases set by the issuing bank.

Currently transaction instruments issued to corporations, such as "corporate purchasing cards", are available for modification of restrictions including:

- credit limit;
- dollar amount per day, month, billing cycle or transaction;
- number of transactions per day, month, or billing cycle;
- non-renewing credit;
- supplier type and merchant industry restrictions; and
- limits by employee.

However corporate purchasing cards are not widely available to the general public and also do not allow each user control over their restrictions.

It is clear that it would be beneficial to provide:

a) A simple payment system that enables customers to securely conduct physical payment transactions without exposing their credit card information to fraud; and
b) A simple online payment service that enables customers to anonymously and securely conduct online payment transactions and particularly to effect payments online.

Summary

Broadly stated, embodiments of the invention are payment systems that addresses the aforementioned problems. In one embodiment, the payment systems use physical and virtual payment cards which are controlled according to specific parameters that can be preset or dynamically determined.

According to an embodiment of the invention, there is provided a method of effecting payments online comprising the steps of: ordering the use of a purchasing card from an online payment service (OPS); receiving purchasing card information; shopping online; and providing the purchasing card information to effect payment.

According to another embodiment of the invention, there is provided a method of effecting payments online comprising the steps of: receiving an order for a purchasing card from a customer; securing payment from the customer for the order; and assigning a purchasing card to the customer, the purchasing card comprising a predetermined limit, the purchasing card being usable by the customer to purchase anything online.

According to another embodiment of the invention, there is provided a system for effecting payments online comprising: a customer network; a merchant network, the customer network in communication with the merchant network for shopping online; and a online payment service (OPS) network, the OPS network in communication with the customer network for creating a credit identity for a customer on the customer network prior to a purchase being made at the merchant network.

According to another embodiment of the invention, there is provided an online payment service (OPS) for effecting payments online comprising: a receiver for receiving an order for a purchasing card from a customer; processing means for securing payment from the
customer for the order; and a notifier for notifying the customer of purchase card information.

According to another embodiment of the invention, there is provided a method of creating a credit identity for effecting payments to an online merchant comprising the steps of: authenticating a customer; assigning a purchasing card to the customer; allowing the customer to use the purchasing card to effect a payment to an online merchant; the payment being made without the customer having to reveal his identity to the online merchant.

According to another embodiment of the invention, there is provided a method of effecting a payment comprising the steps of: obtaining a transaction instrument; assigning restrictions to the transaction instrument; and making a purchase with the transaction instrument within the restrictions.

According to another embodiment of the invention, there is provided a transaction instrument for effecting payments, the transaction instrument being issued from an issuing bank to a user, the user having control over restrictions placed on the transaction instrument.

Advantages of embodiments of the current invention include the following:

Reduction in fraudulent transactions.

Controlling use of cards and other payment transactions.

Customers can conduct transactions with complete anonymity without the need to partner with vendors or implement or modify existing software.

The service blends seamlessly, using the current standard for processing e-commerce transactions - the credit card.
The credit card service can be combined with a complete range of additional privacy services.

It can be used anywhere on the Internet.

It does not require cooperation of online merchants.

It utilizes existing credit vehicles.

Transactions conducted using the profiled transaction instrument will reduce the risk of credit theft to the issuing bank, the merchant as well as the transaction instrument holder.

The profiled transaction instrument can be used for both online and offline purchases.

Other aspects and advantages of the invention, as well as the structure and operation of various embodiments of the invention, will become apparent to those ordinarily skilled in the art upon review of the following description of the invention in conjunction with the accompanying drawings.

**Brief Description of the Drawings**

Embodiments of the invention will be described with reference to the accompanying drawings, wherein:

FIG. 1 illustrates the current system used for effecting payment for online purchases;

FIG. 2 illustrates the system used for effecting payment for online purchases in conjunction with the present invention;
FIG. 3 illustrates the method of effecting payment for online purchases in conjunction with the present invention;

FIG. 4 illustrates system components of the OPS;

FIG. 5 illustrates the user management component of the OPS in greater detail; and

FIG. 6 illustrates another embodiment of the invention.

Similar references are used in different figures to denote similar components.

**Detailed Description**

A private payment Internet service that provides a firewall between the customer and the merchant during an Internet purchase is described. The customer utilizes his own credit card but the merchant never sees that credit card or related information. Not only is the customer anonymous to the merchant, but also the customer’s credit card bill will not show from what merchant a product or service has been purchased. Features of the present invention include the following:

The merchant does not know the identity of the customer.

The merchant has no way of identifying the customer or his bank account or credit card.

The customer’s conventional credit card bill does not reflect what purchases were made or from who those purchases were made. Only a transaction charge from the OPS is shown.

The OPS even can not determine what purchase the customer has made; only that he has utilized the OPS credit card for a particular dollar amount.
The customer is not required to fill out the merchant’s information form. This function is provided by the OPS via a form filler service.

The OPS preferably does not utilize cookies so there is no way for a merchant to acquire customer information.

The merchant has no way of sending advertisements or other unsolicited materials to the customer.

Referring to Figure 1, the current system 10 of making online purchases is illustrated. Customer 12 communicates directly with merchant 14 via customer network 16 and merchant network 18. Merchant network 18 communicates with certifying authority 20 to verify the customer’s authentication. Authentication is any process by which the customer establishes his identity in order to effect payment (password, etc.). In order for proper authentication to be established, the customer must provide personal identification information. The merchant also is able to communicate directly with customer’s financial institution.

Referring to Figure 2, the system of effecting a payment online in conjunction with the teachings of an embodiment of the current invention 26 is illustrated. Customer 12 still communicates directly with the merchant 14 via customer network 16 and merchant network 18. However, customer also communicates with OPS 22 on OPS network 24. The customer preferably initiates contact with the OPS via the customer’s bank, but also may contact the OPS directly. It is OPS 22 that authenticates customer 12 in order to effect the online payment. The customer still directly shops at merchant’s site, and provides payment at the merchant’s site. However, merchant and merchant network do not authenticate nor communicate with customer’s financial institution. The merchant does not know the identity of the actual customer. From the merchant’s vantage point, the customer is the OPS. The credit card number the merchant receives (provided by the customer) is a Visa or MasterCard number that has been issued to the OPS and assigned to the customer. The credit card account authenticated by the merchant is an OPS account. At no time are these cards physically issued to customers. In this way, the OPS
creates a credit identity that exists for only the length of time needed to effect the online payment transaction.

Referring now to Figure 3, the OPS transaction process 30 is implemented as follows:

In the first step 31, customer initiates contact with the OPS. As stated previously, the customer preferably initiates contact with the OPS via the customer's bank (use of the OPS may be a service provided by the bank), but also may contact the OPS directly. The customer enters order information and authorizes payment (to the OPS) on an SSL-secured online order form. The customer requests the use of a credit card that is issued to the OPS. The credit cards supplied to customers are "Purchasing Cards". These Purchasing Cards are heavily regulated by the Issuing Financial Institution as discussed below. A Purchasing Card assigned to a customer can be used by the customer to purchase anything online.

In a preferred embodiment, the OPS offers three types of payment for its service. The first are Type I Cards. These are prepaid by the customer via a variety of methods as is detailed below. These cards have a credit limit not exceeding the prepaid amount and are valid for a single transaction only.

The second are Type II Cards. These are preauthorized (i.e. by the customer's credit card issuer) but no payment is made until a purchase is made. These have a credit limit determined by the customer and are valid for a single transaction only.

The third are Type III Cards. These are pre-approved wherein the customer is invoiced at the end of each month. These have a predetermined credit limit and are valid for any number of transactions. These cards include an expiry date. In general, they are available to VIP customers.

In general, customers begin with a Type I card. Over time, as a relationship is formed between the customer and the OPS, the customer may be allowed access to Type II and Type III cards.
While customers in all cases will be issued a credit card number and a PIN number, no card is physically issued to the customer.

In the second step 32, order entry staff at the OPS receive the order and gathers the information necessary to collect payment from the customer. Once the payment information is received, the transaction is processed and authorization is received for payment from the OPS Financial Institution.

The order entry staff:

(i) authenticates and captures payment (in the case of Type I Cards) or preauthorization (in the case of Type II Cards) from the customer's credit card company

(ii) creates a temporary credit identity by assigning an appropriate Purchase Card for the customer, taking a Card from its inventory of available Cards.

The OPS preferably offers customers a number of payment options for obtaining the use of a Purchasing Card. Payment is via one or a combination of, the following: filling out an online form utilizing the Internet, or contacting the OPS directly either by telephone, fax, mail, or email.

In the third step 33, the temporary credit identity is created and technical support staff at the OPS post the assigned Purchase Card number onto a password protected website area upon approval of the transaction.

In the fourth step 34, a customer service operator at the OPS notifies the customer that their request for use of a Purchasing Card has either been approved or declined via email. The response is dependent upon the authorization response received from the OPS Financial Institution. If the customer has been approved, the customer service operator emails the customer to notify him to collect the credit card. The designated URL and
a unique username/password from Step 3 (valid only within a certain time period) is also attached within the email.

If the customer has been declined, they will be required to provide an alternate method of payment before proceeding to Step 5. Such alternative payment forms include check, money order or any such form of payment.

Preferably in the fifth step 35, customer retrieves the Purchasing Card details online by logging in and collecting the Purchasing Card they ordered from the URL address. The website contains the information for one Purchasing Card. Generally, the information provided on the site will enable the customer to conduct one online transaction using the Purchasing Card.

For example, if a customer purchased a $50 Purchasing Card, they would be directed to a web site listing: a total available credit limit of $50, a transaction limit of $50, the billing address associated with the Purchasing Card, and the name associated with the Purchasing Card.

In this embodiment, the customer obtains the credit card information prior to shopping online (sixth step 36 below). In an alternative embodiment, the customer obtains the credit card information at the time of actually effecting the online payment.

In the sixth step 36, the customer proceeds to shop online. The customer locates the merchandise they require on any site accepting Visa or MasterCard as method of payment. On the merchant’s shopping form, the customer uses the temporary credit identity information provided to them in Step 5 via the form filler service.

The OPS preferably establishes an online account for the customer to track their balance as well as is discussed below.

If shipment of goods is required, the customer must fill in the appropriate shipping instructions in the shipping information section of the merchant’s site.
In the seventh step 37, the OPS reconciliation process occurs. The OPS receives online statements nightly from the OPS Issuing Financial Institution listing all transactions processed on Purchasing Cards issued to the OPS that day. *How?* The OPS deducts the amount spent on each Purchasing Card from the cardholder's (the customer's) account. Any balance remaining in the customer's account is then credited toward another Purchasing Card or refunded back to them via their original method of payment.

For Type I and Type II cards that are valid only for a single transaction, any surplus in the customer's balance is refunded, usually by the same method by which payment was made. For Type II cards, the surplus may just remain in the account for future use. If an expiry date is present, any surplus may be refunded on the expiry of the card.

In the eighth step 38, the OPS payment issuer receives monthly statements from its Issuing Financial Institution regarding the balances on the Purchasing Cards. Payment is made to the Issuing Financial Institution and the Cards with zero remaining balance are returned to the inventory and reassigned to a new customer.

As mentioned previously, the OPS specifies the limits (regulations) to be placed on each Purchasing Card by the Issuing Financial Institution prior to the date they are issued to them. Once issued, the cards can be modified at anytime by the Issuing Financial Institution upon receipt of request from the OPS. The Issuing Financial Institution then upholds the limits placed on the cards.

In one embodiment, the limiting criteria used on Purchasing Cards are:

- limiting the number of transactions than can be conducted on the card during a specified time period (such as one transaction per month/year/etc.);

- limiting the credit limit amount available to the cardholder (possibly variable from one dollar up to five thousand dollars);
limiting the transaction amount available to the cardholder (possibly variable from one dollar up to five thousand dollars).

In one embodiment, for online purchases, a virtual card can be controlled by specifying restrictive parameters (for example: single transaction, 30 minute duration, fixed amount or range). The virtual Purchasing Card can also be issued using a pseudonym to provide anonymity. The virtual Purchasing Card, further, uses physical cards that can be authorized for use in advance or dynamically.

A major focus of an embodiment of the current invention is to provide Internet users an anonymous, secure and universally accepted payment method.

The online payment service of the current invention will allow its customer to buy and shop anonymously at any online merchant sites. Anonymity of the payment service is achieved by rotating a large number of Visa and/or MasterCard Purchasing Cards that the OPS possesses among its users. Every time a customer places an order with the OPS, the OPS will randomly assign one or multiple cards available in its inventory for customer use. These cards are restricted by a limited number of transactions and/or a certain period of time. The OPS will authorize its customers to make online purchases as corporate members, thereby eliminating the need for its customers to give out their own personal information when making purchases at other online merchant sites. As no customer is associated with any specific Purchasing Card, purchases issued to the OPS, customers are completely anonymous.

The payment service is also secure. In one embodiment the OPS takes the responsibility for any online theft or fraud that may occur on its corporate Purchasing Cards. Therefore, customers can use the Purchasing Card to conduct purchases over the Internet without concern that their own credit card information could be stolen. Furthermore, the OPS constantly changes the parameters of its corporate Purchasing Cards such as credit limit, expiry date, cardholder address and cardholder name, in order to reduce the chances of
fraud. Finally, the OPS preferably stores its customer information at different offshore locations to ensure that all private information about its customers will always be kept intact both online and offline.

As the payment service involves only simple credit card transactions, it does not require pre-integration with any online merchants' systems. Customers can use the anonymous payment service anywhere on the Internet where Visa or MasterCard is accepted.

In a further embodiment, in the case of a customer who wishes to purchase hard goods on the Internet but still maintain his anonymity, arrangements can be made to have the goods delivered to a post office box or to any outfit allowing its address to be used as a delivery address, such as a courier office. In the latter case, the customer will be issued an identification number. This number will also be provided to the merchant as a part of the shipping address.

In another embodiment of the invention, the customer wishing to verify his online purchases made with a Purchasing Card will see the charges shown on his regular monthly Visa bill as purchases from the OPS. There will be no indication regarding what purchases the OPS made on the customer's behalf. In fact, because of the multiplicity of transactions, merchants, and customers, even the OPS will not know what particular purchases were made by an individual customer.

As previously mentioned, the customer will also be able to check his account on the website to determine the amount of his online purchases during the month and the status of his account.

Figures 4 and 5 illustrate OPS network 24 in further detail. OPS network 24 includes OPS server 40 for facilitating transactions between OPS network 24, customer network 16 and the certifying authority. OPS server includes system components user management 41, inventory management 51, bank management 61, corporate accounting 71, site administration and data management 81.
User management receives, processes and reconciliates customer orders. Receiver 42 is used for receiving the order. If the order is placed via the Internet, then the order is received through a graphical user interface. The receiver includes the user registration module and form filling module. The customer information database 50 stores the received information.

Processing means 44 includes collecting means 46 and authenticator 48. Collecting means 46 uses a user credit pre-purchasing module for securing payment for use of a Purchasing Card. Authenticator uses a user credit release module for authenticating the customer.

A Purchasing Card is then assigned to the customer from Inventory Management 51, which includes inventory of Purchasing Cards 52.

User management 41 further includes notifier 56 and user reconciliator 58. Notifier 56 informs the customer of approval (or decline). If the customer is approved, notifier also provides access information to website 54 containing the Purchasing Card information. Reconciliator 58 receives daily statements of transactions made with various Purchasing Cards. Reconciliator 58 then accordingly adjusts each customer’s balance.

Bank Management 61 includes various links to banks and conducts the bank accounting. Payment issuer 60 receives monthly statements from the Issuing Financial Institution regarding money owed on each Purchasing Card. Payment issuer issues the payments and returns the Purchasing Cards to inventory for reassignment to a new customer.

Reconciliator 58 receives daily statements of transactions made with Purchasing Cards. Reconciliator then, accordingly adjusts each customer’s balance.

Payment issuer 60 receives monthly statements from the Issuing Financial Institution regarding money owed on each Purchasing Card. Payment issuer issues the payments and returns the Purchasing Cards to inventory for reassignment to a new customer.
Corporate accounting 71 includes accounts receivable, accounts payable and cash management modules for the OPS. Site administration and data management 81 includes means to manage the infrastructure of the OPS. Both of these are standard for any business and are not further discussed in this document. In one embodiment, the customer's bank only gets one end of each transaction. That is, each transaction will have a different issuer and customer bank.

Embodiments of the present invention also address other security issues. For example, there are a number of laws regulating the issue of credit cards. The United States has a regulation (Regulation E) that requires that for electronic fund transfers, the issuing institution must track all transactions, provide periodic statements and give customers a paper receipt when a transaction has occurred. A similar regulation is in place for the issuance of credit cards. These regulations could preclude the customer wishing to make a purchase without leaving a paper trail. Since the OPS is not issuing credit cards but merely allowing the customer to use credit cards issued to them, the paper trail is not required.

Fraud is also a major problem to Internet vendors. While Visa claims that fraudulent use of its cards is less than 0.1%, the company CyberSource (CYBS) commissioned a study that indicated that 5-25% of online credit card sales are fraudulent. One of the reasons for this discrepancy may be that Visa is seldom the victim of online fraud since the credit card company is liable only if the merchant has obtained a customer signature; an unlikely occurrence for an online purchase. Consequently, the merchant is liable for all other fraudulent purchases online. Because of the risk of fraud, there is established a sophisticated combination of firewalls, cryptography and safety nets in order to protect itself against:

- double spending (spending the same money twice);
- the use of fraudulent credit cards (cards which have not been legitimately issued);
- the use of stolen credit cards.
On such example of a safety net is a system wherein the inventory of cards comprises of cards that are issued to customers, returned to the inventory upon expiry and reissued only when all other cards have been issued. That is, each card is used once in sequence until a card is reissued. Also, the cards could have balances that decline with each subsequent issue and validation dates that change with each issue. For example, a card issued to Customer A may have a limit of $200, but when it is issued to Customer B, it will only have a balance of $100.

Through its membership requirements, there is also protection against the customer who denies making a purchase. For instance, the IP address could be used to track the customer.

Because merchants who wish to remain in business are seldom the source of fraud, the merchant related risk is low. However, certain protocols have been established to protect against phony merchants. These include, among others, the denial of service to merchants in particular countries which exhibit a high amount of fraud.

Preferably OPS does not conduct dealings in cash nor in individual transactions exceeding $5000. Since his serves to protect the OPS from the chance of anyone using the OPS for the purpose of laundering money.

In one embodiment, the OPS of the present invention operates as an anonymous prepaid credit card payment service operating in US funds. However, the service may operate in any desirable currency.

In another embodiment, in addition to the anonymous payment service described above. There is also provided a range of other complimentary services in order to create a total privacy and security solution for its customers will include, but is not limited to, the following:
1. **Cookie crushing**

A service that allows customers to periodically delete cookie files of their choice from their computer systems.

2. **Anonymous web surfing and emailing**

Complimentary anonymous web surfing and anonymous emailing services will allow customers to conduct virtually all of their online activities anonymously.

3. **Digital/Electronic wallet software**

In one embodiment, the invention also provides customers a digital wallet that features online form filling capability. The wallet will also serve as a means of secure communication between the OPS server and the customer's computer during a payment transaction between the OPS and the customer. These capabilities online form filling and instantaneous interaction between the OPS server and users will then consequently enhance customer's online shopping experience.

4. **Anonymous PickUp Service**

To complete the anonymous shopping service of the present invention, the OPS aligns itself with one or several major logistics companies. The logistics company/companies will facilitate anonymous pickup services where customers can have their physical goods purchased with OPS Purchasing Cards sent to the logistics company’s outlets and pick up the goods with a unique and anonymous identifier provided by the OPS.

Referring to Figure 6, another embodiment of the invention creates a payment system where customers create and vary the authorization profile for payment transactions conducted using a transaction instrument. Transaction instrument may include a credit
card, debit card, prepaid card and or some other form of payment system. The customer or transaction instrument-issuing bank then modifies the authorization profile at anytime to update, change and or modify various restrictions on the transaction instrument. The combination of one or several restrictions creates a "profile", specific to each transaction instrument holder, listing the user’s selected restrictions. Changes to the profile could then be enabled, disabled and or modified at anytime by the user via some form of communication system, such as but not limited to: the Internet, WAP technology, Bank Machine or Telephone Call. Additionally, a funds transfer profile could be set to access a sequentially predetermined source of funds if the primary account becomes depleted.

Preset profiles may be set by the transaction instrument-issuing bank for the convenience of their clients. These preset profiles could contain a combination of, or singularly, various restrictions grouped together so as to be easily invoked by the user by entering in a security code / Personal Identification Number (PIN) unique to each profile. Enabling a different profile could invoke a different set of restrictions appropriate for each transaction instrument holder, at that specific time.

Some restrictions that could be implemented to create a profile (in combination or singularly) by either the transaction instrument holder or the transaction instrument-issuing banks are:

- Account could be deactivated and reactivated at any time;
- Cash advances could be allowed or disallowed;
- Limits put on the time of day the credit instrument is available (e.g.: not after 3 am and not before 9 am local time for the user);
- Limits on both or either maximum and minimum transaction amounts (e.g.: the user could set his or her transaction instrument to accept only charges ranging between $20 and $140);
- Limits on the currencies available for the transaction(s) (e.g.: Rubles disallowed, only US & Canadian currencies allowed);
- Geographical limits on where the transaction instrument could be used, (e.g. within the transaction instrument holder's city, province/state, country, zip code,
area code – either singularly or in any combination);

- Which merchants the transaction instrument will work for (e.g. disallow: adult shops, online merchants / mail order / phone order transactions);
- Excluding specific items allowed to be purchased, such as computer equipment, stereos, jewellery, etc.;
- Transaction instrument holder must be present for the transaction to be conducted via some form of proximity device (e.g.: the transaction instrument holder must be in the same city for the transaction to be conducted);
- Limits on how far away the transaction instrument holder can be from the transaction instrument to conduct a purchase (e.g. an out of range / proximity restriction could be enacted if the transaction instrument is used more than 100 feet from the transaction instrument holder). The distance could be measured using either a GPS enabled device or an electronic code syncing device such as; personal digital assistant (PDA) (or a device similar to a Palm Pilot), a ‘Blackberry’ device, a cellular phone, a watch with an electronic chip, or a WAP device, or some other device able to measure distance between two items; and
- Transaction instrument holder could register their ‘self control issues’, for example restricting:
  Alcoholic beverages;
  Fast food outlets; and
  Impulsive shopping (e.g. no more than 1 purchase per hour/day).

The payment system, in one embodiment, uses physical cards that can be authorized for use in advance or dynamically.

In one embodiment, several criteria could be set in each profile allowing modification of the profiles’ authorization criteria. Verification of the authenticity of the transaction instrument holder could include either a combination of, or singularly, the following items:

- Personal Identification Number (PIN);
- Security code;
• Digital signatures;
• Written signatures;
• IP address;
• Domain Address;
• Retinal scanners;
• Voice recognition;
• Finger print readers;
• Weight scales;
• Handprint; and
• Footprint.

In another embodiment, Signature Readers could be used to restrict the transaction instrument holder from using the transaction instrument while intoxicated through the use of intoxication criteria or intoxication identifier technologies.

As well, Signature Readers could also be used to allow pre-registered users to access the account if their signature matches one on record. For example, a child of a profiled transaction instrument holder could be allowed to conduct transactions using their parent’s transaction device.

The transaction instrument can also incorporate a number of other features, which can be selected either in combination or singularly:

• Transaction instrument could have the option of not having the transaction instrument holder’s name, account number, or expiry date visibly imprinted.
• If an attempt to access the account, contrary to the restrictions established by the user, occurs at a transactional location then the transaction instrument could be:
  Confiscated/ not returned to the user;
  A telephone call and or e-mail message could be initiated to the transaction instrument holder notifying them of the violation;
  The police could be called if an emergency code is not then entered;
  A signal could be sent to police or interested parties identifying the
location of the transaction instrument holder.

- Entering a Personal Identification Number (PIN) at a bank machine of some sort could reinstate the user’s default profile.
- Transaction instrument holder must be present at the point of sale to conduct transaction (derived via an electronic device able to determine proximity)
- An emergency / panic code Personal Identification Number (PIN) could be entered at a bank machine notifying police the user was being robbed or was in immediate danger.
- Each transaction could be reported to each user or just the primary account holder via some form of communication device such as email.

Master control settings could be enabled allowing only authorized transaction instrument holders to modify the restrictions for themselves or a group of users. For example, a parent could control all transaction instruments held by his or her family. Changing the restrictions on the transaction instrument(s) could only be conducted by the transaction instrument holder authorized to make changes. For example, the following criteria could be required, but not limited to:

- Permissions could only be changed from the transaction instrument holder’s home phone number, within a specific area code, time period, by identifying themselves using a Personal Identification Number (PIN) or any combination of the above.
- Additionally, the user could over-ride transaction denial responses, enacted by the transaction instrument’s issuing bank (referred to as fraudulent use ‘red flags’) by identifying themselves via a Personal Identification Number (PIN).

The payment service in accordance with the present invention operates in two embodiments. The first allows users, other than the primary transaction instrument holder, to access funds from the primary transaction instrument holder’s account via an additional transaction instrument. That is, a single account may have several transaction instruments issued to it.
In a second embodiment, users, other than the primary transaction instrument holder, may access funds from a separate account via an additional transaction instrument. The additional transaction instrument may have restrictions placed on it by the primary transaction instrument holder.

Payment could also be provided to the other user at scheduled times/dates (e.g. used to payout allowances to children)

Additionally, different restrictive profiles can be set up for a group of transaction instrument holders, such as a family, with each transaction instrument registered to access a joint account. For example: one parent with a large credit limit need set at $5000, another parent with a smaller credit limit need set at $500, and their children and or domestic workers could be issued a transaction instrument with a credit limit need set at $40. Additionally any number of restrictions could be placed on the child’s transaction instrument (e.g. limiting where the children could use the transaction instrument)

In another embodiment, funds are ‘drawn down’ using a funds transfer profile enabled by the user. This profile could be set to access a sequentially predetermined source of funds if the primary account becomes depleted. For example, the sequential source of funds could be, but not limited to: the transaction holder’s personal line of credit, savings account, checking account, and or RRSP’s.

Preferably, transaction instrument statement are accessed online in real time. If an anonymous transaction number is used this is where the transaction instrument holder goes to look up the transaction instrument number.

The purpose of the payment system is to limit the risk of fraud or credit theft for both the transaction instrument holder and or the transaction instrument-issuing bank. The payment system allows the user to gain further control over their credit instrument by allowing them to modify a combination of restrictions at anytime. For example, transaction instrument holders who do not regularly travel outside their city, nor purchase
high-end electronic equipment regularly, can enable restricting out of town charges, as well as restricting purchases on the credit instrument to restaurants only through the payment system. The user could then remove the restriction(s) for a specified period of time and or indefinitely.

The following examples are not intended to be limiting in any way and serve only as some of the many possible scenarios that could exist within the scope of the invention.

The transaction instrument holder could select a merchant where a transaction had to occur before a credit limit restriction on the transaction instrument could be automatically raised. For example, the user could set his profile requiring that his transaction instrument be used for one transaction at a particular restaurant before the credit limit could be automatically raised to a preset higher limit of $500.

Additionally, the transaction instrument holder could set a transaction range that had to occur before the restrictions on the transaction instrument could be automatically changed. For example, the user set up his profile requiring that his transaction instrument be used for one transaction of $20-$25 before the maximum credit limit could be automatically raised to his preset higher limit.

An example of one preset profile is: restricting out of town purchases, restricting the transaction instrument’s transaction amount limit to $200, restricting purchases between the hours of 12am and 11:30 am, restricting any purchases from adult shops, computer shops, and or jewellery stores. Another possible preset profile could restrict the number of purchases conducted within a two-hour period, while not restricting the transaction amount limit. In either case each preset profile could be enabled, disabled and or modified at anytime by entering a PIN unique to that profile via some form of communication system.

In another example, a parent could assign a transaction instrument to their child to be used for purchasing clothing. In this scenario, the parent could invoke a profile (with a
set of restrictions) to be applied to the transaction instrument by entering in special PIN. The profile could include a credit limit of $200, an individual transaction limit of $60, restricting the amount of time the transaction instrument is enabled, as well as restrict the transaction instrument from being used to purchase goods other than clothing. Once the child has completed their purchases the transaction instrument could then be returned to its disabled state by entering a default PIN.

An embodiment of the invention is a total online privacy service provider, aiming to promote independent/individual Internet users’ awareness of online privacy and provide them with tools to control their own online privacy and security exposure. An embodiment of the invention allows customers to maintain anonymity for online purchases. By using their own credit cards issued to them rather than some form of cyber cash, and by virtue of the confidentiality and the credit card safety of the online payment service, this is accomplished in a simple, user friendly system. An embodiment of the invention allows its customer to make online purchases without any record of the purchase being traceable to him. Further, it allows the purchaser to deal with any web merchant; it does not require the merchant to subscribe to the service. As well, it provides the customers with control over restrictions placed on their transaction instruments.

While the invention has been described according to what is presently considered to be the most practical and preferred embodiments, it must be understood that the invention is not limited to the disclosed embodiments. Those ordinarily skilled in the art will understand that various modifications and equivalent structures and functions may be made without departing from the spirit and scope of the invention as defined in the claims. Therefore, the invention as defined in the claims must be accorded the broadest possible interpretation so as to encompass all such modifications and equivalent structures and functions.
What is claimed is:

1. A method of effecting payments online comprising the steps of:
   ordering the use of a purchasing card from an online payment service (OPS);
   receiving purchasing card information;
   shopping online; and
   providing the purchasing card information to effect payment.

2. A method of effecting payments online comprising the steps of:
   receiving an order for a purchasing card from a customer;
   securing payment from the customer for the order; and
   assigning a purchasing card to the customer, the purchasing card comprising a predetermined limit, the purchasing card being usable by the customer to purchase anything online.

3. A system for effecting payments online comprising:
   a customer network;
   a merchant network, the customer network in communication with the merchant network for shopping online; and
   an online payment service (OPS) network, the OPS network in communication with the customer network for creating a credit identity for a customer on the customer network prior to a purchase being made at the merchant network.

4. An online payment service (OPS) for effecting payments online comprising:
a receiver for receiving an order for a purchasing card from a customer;
processing means for securing payment from the customer for the order; and
a notifier for notifying the customer of purchase card information.

5. A method of creating a credit identity for effecting payments to an online
merchant comprising the steps of:
   authenticating a customer;
   assigning a purchasing card to the customer;
   allowing the customer to use the purchasing card to effect a payment to an online
   merchant; the payment being made without the customer having to reveal his identity to
   the online merchant.

6. A method of effecting a payment comprising the steps of:
   obtaining a transaction instrument;
   assigning restrictions to the transaction instrument; and
   making a purchase with the transaction instrument within the restrictions.

7. A transaction instrument for effecting payments, the transaction instrument being
   issued from an issuing bank to a user, the user having control over restrictions placed on
   the transaction instrument.
Figure 2
Customer Initiates contact with OPS

Order Received

Purchase Card Information Posted on Protected Website

Customer Notified

Purchase Card Information Retrieved

Customer Shops Online

OPS Receives Nightly Statements

OPS Receives Monthly Statements

Figure 3
Figure 6