



(22) Date de dépôt/Filing Date: 2000/04/07

(41) Mise à la disp. pub./Open to Public Insp.: 2001/10/07

(51) Cl.Int.⁷/Int.Cl.⁷ G06K 19/06, H04L 12/16

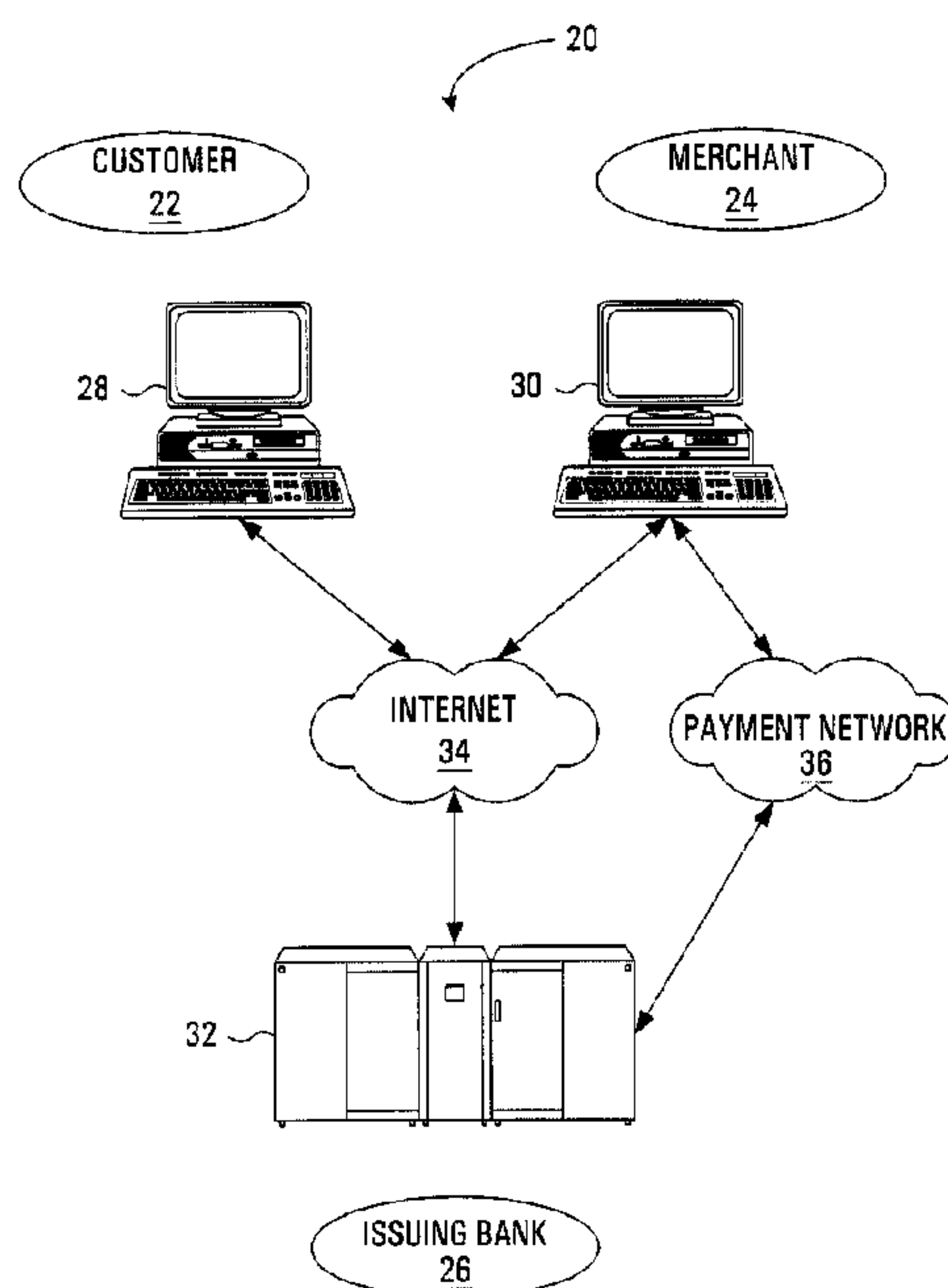
(71) Demandeur/Applicant:
REVCARD FINANCIAL CORPORATION, CA

(72) Inventeurs/Inventors:
ABDALLA, ANDREW, CA;
MAVRIDIS, JOHN, CA

(74) Agent: SMART & BIGGAR

(54) Titre : METHODE ET SYSTEME POUR FOURNIR DES SERVICES RELIES AUX CARTES DE DEBIT PAR
L'INTERMEDIAIRE D'UNE INFRASTRUCTURE DE CARTES DE CREDIT

(54) Title: METHOD AND SYSTEM FOR PROVIDING DEBIT CARD SERVICES OVER A CREDIT CARD
INFRASTRUCTURE



(57) **Abrégé/Abstract:**

A system and method of permitting a customer to obtain a secure single-use or limited-use debit card for a predetermined amount and for a particular purpose. In virtual form, the customer purchases a prepaid debit card number with a customer-specified available funds' limit and expiry date. Optionally, the customer chooses to add his own name and address in these respective fields of the prepaid debit card or have an alphanumeric string attributed to him for these fields by the system allowing for greater privacy. Prepaid debit cards will also be available in pre-set denominations and currencies with limited term or customer-specified expiration dates. A prepaid debit card transaction system is also provided. A prepaid debit card transaction system allows the issuing institutions to verify the security features that exist by establishing that the information that is available on the face of a prepaid debit card (number and expiration date) correlates with the address, name or other data elements that have been given or attributed to the customer.



Abstract of the Disclosure

A system and method of permitting a customer to obtain
5 a secure single-use or limited-use debit card for a
predetermined amount and for a particular purpose. In
virtual form, the customer purchases a prepaid debit card
number with a customer-specified available funds' limit and
expiry date. Optionally, the customer chooses to add his own
10 name and address in these respective fields of the prepaid
debit card or have an alphanumeric string attributed to him
for these fields by the system allowing for greater privacy.
Prepaid debit cards will also be available in pre-set
denominations and currencies with limited term or customer-
15 specified expiration dates. A prepaid debit card transaction
system is also provided. A prepaid debit card transaction
system allows the issuing institutions to verify the
security features that exist by establishing that the
information that is available on the face of a prepaid debit
20 card (number and expiration date) correlates with the
address, name or other data elements that have been given or
attributed to the customer.

Title: Method and System for Providing Debit Card Services Over a Credit Card Infrastructure

Field of the Invention

5

This invention relates to a system and method for facilitating online commerce over a public network such as the Internet or an interactive T.V. cable network. More particularly, this invention relates to a system and method for conducting online transactions using a single-use or limited-use debit card for specific or limited purchases over a computer network. This invention also relates to a system for processing prepaid debit card transactions.

15 **Background of the Invention**

Online commerce has experienced dramatic growth in recent years and this growth is expected to continue into the coming decades. Internet service providers are more and more connecting users to the Internet at no cost, thus eliminating barriers to an Internet connection. At the same time, merchants are increasingly developing sites on the World Wide Web (or simply "WWW" or "Web") that customers can access and order goods and/or services. It is fairly common for a customer to browse a merchant's catalogue, select a product, place an order for the product, and pay for the product all electronically over the Internet.

Typically, the customer pays for the goods and/or services ordered over the Internet with a credit card. In January 2000, credit cards accounted for approximately 93%

of e-commerce online purchases over the Internet (source: Ernst & Young, Global Online Retailing Report, 01-2000). In a typical online transaction, a merchant sends an order form and requests that the customer enters personal data such as his name, address and telephone number, as well as credit card information including account number and expiration date. The customer then returns the completed order form containing the credit card information to the merchant over the Internet. The merchant effects a verification in order to validate the credit card number, as well as to confirm whether the payment can be charged to the credit card. Credit card verification is usually conducted on a well-established credit card network and is well known to the persons skilled in the art. Specific examples of credit card networks include VisaNet.RTM.network and Veryphone.RTM.network.

A deficiency with the above-described online commerce model is the security of the credit card data as it travels over the Internet. The credit card information can be intercepted in route, copied into a database, and used to make purchases unauthorised by the owner of the credit card. Effectively, in an automated environment, an impostor can repeatedly use the stolen credit card data to conduct many online transactions before the owner of the credit card even becomes aware that the credit card data has been stolen. This has resulted in a large number of users being reluctant to provide their credit card information to an online merchant. An additional area of uncertainty resides in the merchant himself. Under the current online commerce model, making use of a credit card is predicated on trust between the merchant and the purchaser. This is necessary

because the credit card number and other related data is transmitted to the merchant during a transaction. At the merchant's site, there remains the risk of fraud from internal sources since data which would allow one to use a customer's card for additional purchases to the full value of a customer's credit has been given to a party who is not the customer's financial institution. According to an online retailing report published by Ernst & Young in January 2000, approximately 57% of all Internet users do not want to provide their credit card number to an online merchant.

There have been numerous attempts to address the security aspect of credit card use over computer networks, and in particular over the Internet such as encryption algorithms and digital signatures among others. Typically, such methods require the use of proprietary software to be used by the online merchant, the credit card issuer and the customer.

Another deficiency in this traditional online commerce model is that it excludes potential customers that do not have access to credit cards. For example, teenagers wishing to purchase audio tracks from an Internet site typically do not have access to credit cards. Although their parent(s) or guardian(s) may have access to a credit card, they may be reluctant to provide the teenager with this credit card information. On the basis of the global online retailing report published by Ernst & Young in January 2000, 37% of all Internet users do not have access to a credit card.

30

Another proposed solution to the above-described problem is electronic cash commonly referred to as "Digicash" or "ecash". The use of "ecash" requires the customer and the merchant to maintain "ecash" accounts on a computer hard drive and to perform transactions on a basis of these accounts.

A deficiency of this type of method is that it requires the customer and the merchant to maintain a separate "ecash" account and to acquire certain software products allowing the transactions between a customer and merchant to take place. As a result, this type of method requires establishing a separate and new transaction infrastructure to support transactions effected by "ecash". Consequently, this type of online commerce model does not integrate well with existing credit card network systems and will require a significant amount of testing and time before such commerce models acquire the level of acceptance and trust associated with the existing credit card services. In addition, by requiring merchants to change their existing practices and implement the new system infrastructure and protocols, an increase in the merchant's costs is incurred thereby reducing the profits of the merchant and/or resulting in higher prices for the customer.

25

Finally, a customer may wish to conceal his identity or other personal information while effecting a transaction for certain goods or services effected entirely over the computer network such as the downloading of a particular software program, content or service. This type of confidentiality is not provided by the above-described methods.

30

Consequently there exists a need in the industry to provide an improved type of purchasing mechanism making use of the existing credit card infrastructure and providing improved security for network transactions.

5

Summary

The invention covers methods and systems for the issuance of prepaid debit cards, transaction processing of
10 prepaid debit card purchases as well as supplementary card services.

In accordance with a broad aspect, the invention provides a method for providing debit card services in a
15 network through a credit card infrastructure.

In accordance with a broad aspect, the invention provides a method for issuing a prepaid debit card over a network. The method includes receiving a set of information
20 data elements associated to a customer over a communication link. The set of information data elements includes payment information and available funds' limit or amount. In a specific example, the credit limit is determined by a payment amount. The method also includes processing the set
25 of data elements to determine on a basis of the payment information an authorization data element, the authorization data element being indicative of either one of an approved transaction or a refused transaction. The method also includes generating credit data elements indicative of a
30 prepaid debit card when the authorization data element is indicative of an approved transaction.

In accordance with another broad aspect, the invention provides a method for processing a transaction associated to a prepaid debit card over a network.

5 In accordance with another broad aspect, the invention provides supplementary card services.

The invention allows a customer to acquire a prepaid debit card being characterized by a short-term expiration
10 date, an available funds' limit, a user name and an address. In a specific example, the expiration date, name and address are comprised of alphanumeric code fields.

The short-term expiration date may be selected by the
15 customer acquiring the prepaid debit card or may be assigned a default value by the system issuing the prepaid debit card. The prepaid debit card expires after a pre-set delay determined by the short-term expiration date to allow for the processing of the debit card transaction.

20

In a specific example, the prepaid debit card may be in a virtual form or a physical form.

Physical form prepaid debit card may be embodied in
25 many different forms including a magnetic strip or bar code embedded on a substrate, a numerical representation of the information on a substrate among others. In a specific example of implementation of the physical prepaid debit card, the latter is activated by dialling a pre-set
30 telephone number and providing the personal identification number that accompanied the prepaid debit card when the

latter was received. The physical prepaid debit card may be purchased in a particular pre-set denomination and currency.

Virtual form prepaid debit cards may be embodied in a data structure including a plurality of data elements stored on a computer readable storage medium such as a computer diskette, hard drive or mass storage device. In a very specific example of implementation, the data structure is a computer file. In a specific example of implementation of the virtual prepaid debit card, the latter is active upon issuance and has available funds' limit that the customer specified, generally for a particular transaction.

Advantageously, the invention allows the use of the current credit card infrastructure for effecting transactions at the merchant level. Effectively, the prepaid debit card is transparent to the eyes of the merchant who processes the transaction as if it was a standard credit-based credit card.

Another advantage of the present invention is that it provides security to the purchaser since the available funds' limit of a prepaid debit card may be set to be close to the value of the purchase being effected.

Yet another advantage of the present invention is that it provides security for the debit card issuer since the debit card is prepaid and therefore the credit risk associated to conventional credit cards is fully reduced or entirely eliminated.

Yet another advantage of the present invention is that it allows greater access to online electronic commerce transactions since customers who cannot necessarily qualify for a conventional credit card are able to purchase a prepaid debit card. This in turn opens a greater market for online merchants.

Other aspects and features of the present invention will become apparent to those ordinarily skilled in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying figures.

Brief Description of the Drawings

15

FIG. 1 is a block diagram of an online commerce system in accordance with an embodiment of the invention;

FIG. 2 is a block diagram depicting an interaction between a customer computing unit and a bank computing centre in accordance with an embodiment of the invention;

FIG. 3 is a block diagram depicting an interaction between a customer-computing unit, a bank computing centre and a merchant-computing unit in accordance with an embodiment of the invention.

Detailed Description

FIG. 1 shows an online commerce system for conducting online commerce transactions. For general discussion

purposes, three participants to an online commerce transaction are shown namely a customer 22, a merchant 24, and an issuing bank 26. These three participants play the primary roles in the online commerce transaction. The
5 customer 22 and merchant 24 may represent individual people, entities, or businesses. Although labelled as "bank", the issuing bank 26 may represent other types of credit card issuing institutions, such as credit card companies, card sponsoring companies, or third party issuers under contract
10 with financial institutions without detracting from the spirit of the invention. It is further noted that other participants may be involved in some phases of the transaction, such as an intermediary settlement institution, but these participants are not shown in the drawings.

15

Each participant is equipped with a computing system to facilitate online commerce transactions. The customer 22 has a computing unit 28 in the form of a personal computer, although other types of computing units may be used
20 including laptops, notebooks, hand-held computers, set top boxes, and the likes. The merchant 24 has a computing unit 30 implemented in the form of a computer server, although other implementations are possible. The bank 26 has a computing centre 32 shown as a main frame computer in the
25 drawings. However, the bank computing centre may be implemented in other forms, such as a mini computer, a PC server, a network site set of computers, and the likes.

The computing units 28, 30 and 32 are connected with
30 each other via a data communication network 34. In a specific example of implementation, the network is a public network. In the illustrated implementation, the network 34

is embodied as the Internet. In this context, the computing units 28, 30, and 32 may or may not be connected to the Internet at all times. For instance, the customer-computing unit 28 may employ a modem to occasionally connect to the Internet 34, whereas the bank-computing centre 32 might maintain a permanent connection to the Internet 34. It is to be noted that the network 34 may be implemented as other types of networks, such as interactive television (ITV) network.

10

The merchant computing unit 24 and the bank computing unit 32 are interconnected via a second network 36, referred to as a "payment network". The payment network represents existing networks that presently accommodate transactions for credit cards, debit cards and other types of financial banking cards. Specific examples of the payment network include the VisaNet.RTM.network and the Veryphone.RTM.network.

20

The electronic commerce system 20 is implemented at the customer 22 and bank 26 sites. In a very specific example of implementation, the electronic commerce system 20 is implemented as computer software modules loaded on to the customer computing unit 28 and the bank computing centre 32. In this configuration, the merchant-computing unit 30 does not require dedicated software to participate in the online commerce transaction supported by the online commerce system 20.

30

Generally speaking, the invention relates methods and systems for the issuance of prepaid debit cards, transaction

processing of prepaid debit card purchases as well as supplementary card services.

There are three distinct phases supported by the online commerce system 20 namely a registration phase, a transaction phase, and a payment authorization phase.

During the registration phase, the customer 22 requests a prepaid debit card from the issuing bank 26. The issuing bank 26 creates a prepaid debit card for the customer and assigns a user name and address to the card. The user name and address is retained in a data record at the issuing bank 26 and is also communicated to the customer 22.

During the transaction phase, the customer 22 provides the merchant with the prepaid debit number. Since the prepaid debit number has a limited available funds' amount and a limited life, a thief that intercepts the prepaid debit number is limited in the amount of damage that can be done. Moreover, if the prepaid debit number is such that it is limited to a single use, a thief that intercepts the prepaid debit number is prevented from using it for illicit gain.

During the payment authorization phase, the merchant 24 submits the prepaid debit card number over the conventional payment network 36 to the issuing bank 26 for approval. The issuing bank 26 identifies the number as a prepaid debit card number, as opposed to a conventional credit card number. The issuing bank 26 then processes the authorization request using its conventional processing system on the basis of the prepaid debit card number. Alternatively, a

parallel prepaid debit card processing system in a functional relationship with the conventional processing system processes the authorization request for the prepaid debit card number. After the processing, the issuing bank 26
5 returns the authorization's reply to the merchant 24.

I. Issuance of debit cards

The prepaid debit card may be in a virtual form or a
10 physical form.

In its virtual form, the prepaid debit card is in a digital format for use in online transactions. Virtual form prepaid debit cards may be embodied in a data structure
15 including a plurality of data elements stored on a computer readable storage medium such as a computer diskette, hard drive or mass storage device. In a very specific example of implementation, the data structure is a computer file. The issuing bank 26 issues the virtual form prepaid debit card
20 to the customer 22 in the form of a signed digital certificate binding the customer to the bank. Optionally, issuing bank 26 may also issue a software module that can be invoked when using the prepaid debit card to conduct a transaction on the Internet 34. The prepaid debit card is
25 configured to be used by the customer in one or more areas of commerce in which the customer typically employs a credit card, a debit card, a bankcard, or other type of financial services card.

30 FIG. 2 shows the online commerce system 20 during a registration phase for issuance of a prepaid virtual debit card. This phase involves the customer 22 requesting a

prepaid debit card from the issuing bank 26, and the issuing bank creating and issuing the prepaid debit card to the customer. The information exchange between the customer computer 28 and the bank computer 32 during the registration phase are illustrated as enumerated lines between the two entities.

The customer computer 28 has a central processing unit comprising a processor 40, a volatile memory 44 (e.g., RAM), and a non-volatile memory 42 (e.g., ROM, hard disk drive, floppy disk drive, CD-ROM, etc.). The customer computer 28 also has a network I/O 46 (input/output) for accessing the Internet 34. The network I/O 46 can be implemented, for example, as a dial-up modem or as a permanent network connection.

The customer computer 28 runs an operating system 48 that supports multiple applications. The operating system 48 is preferably a multitasking operating system that allows simultaneous execution of multiple applications in a graphical windowing environment.

Several software components are stored in memory 42 including a browser 52 and a registration module 56. These software components load into volatile memory 44 when launched and execute on the processor 40 atop the operating system 48. The browser software 52 originally exists on the customer computer 28, whereas the registration module 56 is downloaded to the customer computer 28 during the registration process.

In a specific example of implementation, the memory 42 includes a virtual prepaid debit card store 50 to securely hold a digital representation of the prepaid debit card received from the issuing bank.

5

The bank computer 32 includes a prepaid debit card transaction processing system ("PCTPS") 100. The prepaid debit card transaction processing system 100 may be a system integral to the issuing bank's computer centre 32 or may be
10 a remote system. In the case that it is a remote system, a secure link is provided between the issuing bank computer and the remote system through a local, public or private network. The PCTPS includes an account manager 60, a prepaid debit card number generator 62 and a customer database 64.
15 For the purpose of the description the PCTPS 100 and accompanying modules form an integral part of the bank computer 32. It is to be understood that the PCTPS 100 and accompanying modules may be located on a remote module without detracting from the spirit of the invention.

20

In a specific example of implementation, the account manager 60 and prepaid debit card number generator 62 are implemented in software that executes on the bank computer 32. In a specific example of implementation, the prepaid
25 debit card number generator 62 is a random number generator that creates random numbers in the same format as conventional credit card numbers. In another alternative implementation, the prepaid debit card number generator 62 includes a database of numbers, each number in the database
30 being in a format analogous to conventional credit card numbers. The prepaid debit card number generator 62 also includes a functional unit capable of selecting a number

from the database and assigning it as the prepaid debit card number. Other variations on the prepaid debit card number generator 62 are possible without detracting from the spirit of the invention as will be readily apparent to the person skilled in the art. The software modules 60 and 62 may be executed individually or integrated into the same software program. The account manager 60 then stores the prepaid debit card number generated by the prepaid debit card number generator 62 in the customer database 64. The account manager 60 also stores additional information for each prepaid debit card such as funds available, expiration date, user name and other information that may be of use. Preferably, the prepaid debit card numbers generated by the prepaid debit card number generator may be re-used when the debit card expires. More specifically, the prepaid debit card number generator 62 maintains a database storing a list of prepaid non-expired debit card numbers along with their respective expiration dates. When the expiration date of a given debit card indicates that the debit card has expired, the debit card number may be returned to the pool of available debit card numbers thereby allowing the reuse of debit card numbers. In another example, the prepaid debit card number generator 62 is operatively connected to the customer database 64 such as to provide the prepaid debit card number generator 62 with the debit card numbers in use. When a prepaid debit card expires, the entry is removed from the customer database 64 by the account manager 60 and the debit card number can be recycled. Preferably, before a record associated to a given prepaid debit card from the customer database 64 is removed, the account manager 60 performs a verification to determine whether any prepaid amount remains unused for that given debit card. In the

negative, the record associated to the given prepaid debit card is removed and the debit card number is returned to the pool of available numbers. If there remains any unused prepaid amount, the account manager 60 does not remove the
5 record associated to the given prepaid debit card. Variations on the policy of unused prepaid amounts may vary without detracting from the spirit of the invention. For example, the account manager 60 may remove the record associated to the given prepaid debit card even though there
10 remains an unused prepaid amount. In this case, the customer associated to the prepaid debit card loses his prepaid amount for failure to use them prior to the expiration date.

In a specific example, the prepaid debit card numbers
15 generated by the prepaid debit card number generator 62 include a definable token or code which allows to distinguish the prepaid debit numbers from conventional credit cards. Alternatively, the definable token or code may be included in a different field such as the card holder
20 name, address or any other suitable field. Preferably, the definable token or code is included in a data field commonly transmitted from the customer to the merchant and subsequently to the issuing bank during a credit card transaction.

25

The registration phase between the customer 22 and issuing bank 26 will now be described with respect to FIG. 2. During a very specific operation on the Web, the customer comes across a banner advertising a prepaid debit card
30 sponsored by the issuing bank. The banner may be part of the bank's website, or part of a statement to its customers, or included as advertisement in other Web contents. The

customer activates the banner by clicking the banner icon with a mouse pointer. This action submits a request for a prepaid debit card application. In response, the customer downloads the registration module 56 from the Web to the
5 customer computer 28. This initial registration step is illustrated by flow arrow 1 from the Internet 34 to the customer computer 28.

The registration module 56 automatically launches to
10 aid the customer in the completion of the online application. In a specific example of implementation, the registration module 56 is configured to provide step-by-step instructions. The customer fills out various fields related to personal and financial matters, such as name, address,
15 telephone number, social security number, presently owned credit cards, bank affiliations, and the likes. Some of these information fields may be omitted and others added without detracting from the spirit of the invention. The customer also provides data related to the amount of the
20 prepaid debit card, the expiration date and the payment method for the purchase of the prepaid debit card. The payment method for the prepaid debit may be in the form of a conventional credit card number, a debit card, "ecash" or any other suitable payment method.

25

The customer completes the prepaid debit card application and submits the application to the issuing bank (flow arrow 2 in FIG. 2). The registration module 56 facilitates this communication between the consumer and the
30 issuing bank. The application itself, or the registration module 56, contains the necessary routing information to direct the application over the Internet 34 to the bank-

computing center 32. The issuing bank reviews the application and the method of payment to determine whether the customer should be authorized to obtain a prepaid debit card. Since the purchase of the prepaid debit card is
5 effected on the basis of already authorized credit or available funds, such as an existing credit or a debit card linked to a bank account, the issuing bank does not need to verify if the customer is credit worthy and may grant or deny the prepaid debit card on the basis of the available
10 funds or available credit associated to the selected payment method. If a prepaid debit card is denied, the issuing bank 26 returns a message to the customer 22 indicating that the prepaid debit card application has been denied and no prepaid debit card will be issued. Conversely, if a prepaid
15 debit card is to be granted the issuing bank 26 returns a message indicating that a prepaid debit card will be granted, assuming that the remaining registration steps are satisfied.

20 Assuming that a prepaid debit card is granted, the issuing bank creates a customer account record in the customer database 64 and issues a request to the prepaid debit card number generator 62 to obtain a prepaid debit card number and/or other type of customer identifier to that
25 account. The bank supplies the prepaid debit card number and any additional information required to uniquely identify the prepaid debit card to the customer prepaid debit card number and uniquely associates the prepaid debit card to a specific customer.

30

In a specific implementation, the bank supplies the prepaid debit card number and any additional information

using a transmission link through the Internet. In an alternative implementation, the bank supplies the prepaid debit card number and any additional information through some means other than online transmission. Fig. 2 shows the prepaid debit card number and any additional information being stored on a floppy disk 68 and mailed to the customer using conventional postal carriers (flow arrow 3 in FIG. 2). Using regular mail provides an added level of security in that the bank can verify through the mailing address that a customer having the registered name and address truly lives at the place inscribed on the online registration form. This increases the bank's confidence that the customer did not submit a fraudulent application. Another benefit is that the software on floppy disk 68 might contain cryptographic modules to secure communication between the customer and issuing bank. The information associated to the prepaid debit card is deposited in the virtual prepaid debit card store 50 on the customer computer 28. At this point, the customer has been issued a prepaid debit card.

In a specific example of implementation, the prepaid debit card is activated upon issuance by the bank. In an alternative example, the customer activates the prepaid debit card by performing a certain activation process. The certain activation process may include calling a pre-determined telephone number associated to a verification system and providing certain information to the verification system. Alternatively, the certain activation process may include accessing a certain website and submitting a certain form containing activation data elements. Many secure activation processes may be used to activate the prepaid

debit card without detracting from the spirit of the invention.

5 The prepaid debit card number is designed to have a finite life, as determined by the issuing bank or by the customer. The shorter the duration, the less likelihood of fraud resulting from the prepaid debit card number being stolen and re-used prior to the end of its life. When the expiration term lapses, the prepaid debit card number is no
10 longer valid.

In a specific example of implementation, the prepaid debit card number is valid for only one transaction. For added security, the prepaid debit card number can be linked
15 to another data element to ensure authenticity. For example, the prepaid debit card number may be linked to the expiry date, an address associated to a user, a verification code or other.

20 The registration process is described above as an interaction between the customer 22 and an issuing bank 26. It is noted that a third party may handle some or all of the registration and issuing tasks on behalf of the bank. However, for discussion purposes, the issuing bank is
25 assumed to perform all of the functions of a bank and an issuing institution.

In summary, with respect to the virtual card:

- The customer accesses a designated website capable of
30 issuing a prepaid debit card through a network link by providing a network address. Alternatively, the customer accesses a designated website capable or

issuing a prepaid debit card through a real-time link at the website of an online merchant.

- 5 • In a specific example of implementation, the designated website is a secure website implementing an information gathering system. The system prompts a customer to indicate the preferred credit card issuer anywhere in the world, where it would be recommended that he use his own credit card issuer or the default credit card issuer.
- 10 • Once the credit card issuer is chosen, the customer will choose the currency for the prepaid debit card that he wishes to use.
- Once the currency is chosen, the customer will choose the amount of the transaction.
- 15 • Once the amount of the transaction is chosen, the customer will choose his preferred method of payment.
- The customer will then choose to be identified by his own name or by a pre-set alphanumeric string. The pre-set alphanumeric string allows the prepaid debit
- 20 card to be used without the merchant obtaining the identity of the customer. This in turn permits a transaction between a customer and a merchant to remain anonymous from the customer's point of view while being securely paid from the merchant's point
- 25 of view;
- Once the method of payment is chosen, the customer will input the information necessary to make the payment for the prepaid debit card and the applicable service charges.
- 30 • When the payment is processed through the Internet in the traditional manner, a prepaid debit card issuing

system will generate a debit card number that may be used for purchases for up to such an amount as chosen and prepaid for by the customer. The system will recognize a name that either is the name of the customer, if that option was chosen, or alternatively recognize an alphanumeric string that will have been assigned.

- The system will populate fields in the card record to implement the optional security algorithm and identification tokens and codes for the prepaid debit card transaction processing system (the "PCTPS"). Examples of such security algorithms may also include key systems such as the RSA algorithm among others.
- The customer will then be prompted to print a receipt of this transaction for their own records;
- The system updates the data records of the issuing bank and/or the records of the PCTPS.
- The customer inputs the information relating to the prepaid debit card number, the expiration date and the name to the corresponding fields of an e-commerce retailer's checkout system or, alternatively request that our system transport this information to those fields if the customer has accessed the system through the website of the e-merchant or from a list of participating merchants identified on the designated website capable of issuing a prepaid debit card.

The above description describes the registration and issuance of a virtual prepaid debit card. As a variant, the prepaid debit card may be issued in physical form. In its

physical form, the prepaid debit card may be embodied in the same medium as conventional credit cards such as magnetic strips, electronic chips embedded in a substrate among many others. Alternatively, the physical prepaid debit card may
5 simply take the form of a printed support medium such as cardboard or paper on which information is printed uniquely identifying the prepaid debit card.

With respect to the physical prepaid debit card:

- 10 • A customer may purchase a prepaid debit card for a particular value at a point-of-purchase.
- The customer can then select the expiration date that is appropriate for his intended use and the customer can inscribe the expiration date on the card.
- 15 • The expiration date can be inscribed into the magnetic swipe of the card at the time of the purchase, either automatically by the electronic dispenser of the card or by the agent at the point-of-purchase.
- 20 • The customer then calls a predetermined telephone number and activates the prepaid debit card.
- Alternatively, the customer can request that the agent at the point-of-purchase immediately activate the prepaid debit card.

25

II. Processing of prepaid debit card transactions

FIG. 3 shows the online commerce system 20 during a transaction phase. This phase involves the customer 22
30 engaging in an online commerce transaction with the merchant 24. The information exchanged between the customer computer

28, the merchant computer 30, and the bank computer 32 during the transaction phase are illustrated as enumerated lines.

5 The customer invokes the browser 52 to surf the Web for a particular product or service, or to visit a website of a particular merchant. Suppose that the customer decides to commence an online transaction with the merchant, such as purchasing a product from the merchant. The customer
10 downloads an order form from the Web and stores it in volatile memory 44 (flow arrow 1 in FIG. 3). The order form is typically configured as an HTML (hypertext markup language) form. The customer fills out the order form 70 to purchase a desired product from the merchant. The order form
15 70 includes a payment section that requires the customer to enter a credit card number for payment of the goods.

 The order form may require the customer to enter information pertaining to the purchase, like the purchase
20 price, the model or item number, the merchant name, and the like. Upon reaching the method of payment field in the order form, the customer provides the prepaid debit card number in the same fashion as a conventional credit card. Example of methods used to provide prepaid debit card information
25 include entering on a key board the prepaid debit card number and other information fields, providing a digital representation of the prepaid debit card such as a file among others.

30 The customer then submits the completed order form 70 over the Internet 34 to the merchant computer 30.

III. Authorization Phase

The authorization phase involves the merchant 24 seeking authorization from the issuing bank 26 to honor the customer's prepaid debit card number received by the merchant in the commerce transaction with the customer.

The merchant 30 receives the prepaid debit card number from the Internet and processes the prepaid debit card number using its conventional computer system. There is no software components added to the merchant computer as part of the online commerce system 20. Rather, the merchant computer 30 treats the prepaid debit card number of the online commerce card no differently than it treats a standard credit card number. In fact, the merchant computer 30 most likely will not be able to distinguish between the two types of numbers.

The transaction data in the order form is captured by the merchant, sent to the payment network 36 and subsequently sent to the issuing bank 26 for authorization and payment in the same manner as any other credit card purchase. The merchant computer submits a request for authorization over a payment network 36 to the bank-computing center 32. This illustration is simplified for discussion purposes, as other participants will most likely be involved. For instance, the merchant computer 30 typically submits the request for authorization to its acquiring bank (not shown) by conventional means. The acquiring bank validates the authorization request by verifying that the merchant is a valid merchant and that the debit card number in the format of a credit card number

represents a valid number. The acquiring bank then forwards the authorization request to the issuing bank. The routing to the issuing bank via the payment network is handled through conventional techniques.

5

When the bank computer 32 receives the authorization request, it first examines the prepaid debit card number to determine whether it is a valid number.

10

In a first form of implementation, the issuing bank 26 will recognize the purchase as being made from a prepaid debit card by the appearance of a definable token or code in the data fields transmitted to the payment network 36 by the merchant. Requests for authorization that do not contain the
15 identifying token or code will be processed according to the issuing bank's conventional credit card authorization procedures. After identifying the card as a prepaid debit card purchase with the optional additional security feature, the issuing bank's credit card authorization system will, if
20 required, transmit the same data to the prepaid debit card transaction processing system ("PCTPS").

25

In a second form of implementation, the issuing bank 26 will process the request for authorization according to the
issuing bank's conventional credit card authorization
procedures. If the issuing bank recognizes the purchase as
being made from one of its conventional credit cards, it
will process the request according to its conventional
credit card authorization procedures. If the issuing bank
30 does not recognition the purchase as being made from one of
its conventional credit cards, it will forward the request
for authorization to prepaid debit card transaction

processing system for processing. The prepaid debit card transaction processing system 100 will search the customer database 64 to determine whether the purchase was paid by a valid prepaid debit card on a basis of the data fields transmitted to the payment network 36 by the merchant. In the negative, the prepaid debit card transaction processing system 100 will return a failure message to the issuing bank which will in turn return an authorization failure message to the merchant computer. In the affirmative, the prepaid debit card transaction processing system 100 will process the request for authorization.

In a third form of implementation, the issuing bank 26 will first transmit the request for authorization to the prepaid debit card transaction processing system. If the prepaid debit card transaction processing system does not recognize the purchase as being made from a prepaid debit card, it will return the request for authorization to the issuing bank conventional processing along with a failed message. The request for authorization will then be processed according to the issuing bank's conventional credit card authorization procedures. In this form of implementation, a definable token or code may be used but not required.

25

The prepaid debit card transaction processing system may be a system integral to the issuing bank's computer centre 32 or may be a remote system. In the case that it is a remote system, the same data is transmitted securely to the remote system via a local, public or private network.

30

The PCTPS authorizes the purchase by applying the security algorithm against the incoming data and the data captured at card issuance. In a specific example of implementation, the prepaid debit card number is forwarded to the account manager 60. The account manager 60 uses the prepaid debit card number as an index to transaction records in the customer database 64. If no records are found, the number is deemed invalid and the bank computer 32 returns a message disapproving the transaction to the merchant computer 30. If a record is found, the account manager 60 examines any extra transaction information which is typically included in the authorization request to double check the accuracy of the request.

After the request is processed, the processing system 100 returns an authorization response to the account manager 60. The PCTPS will then forward an industry standard authorization reply to the issuing bank 26. The bank-computing center 32 then returns the authorization reply to the merchant computer 30 via the payment network 36. Alternatively, the issuing bank may wish that the PCTPS send the authorization reply directly to the payment network 36 with a notification message to the issuing bank 26.

The PCTPS will handle merchant charge-backs in a similar fashion.

The preceding steps assume that the authorization request was successful. If that is the case, the available funds' limit of the customer's prepaid debit card is drawn down in the amount of the authorization, and the transaction is logged for future posting.

III. Card services

A system for purchasers and card issuers to perform the following functions via a computer network or telephone
5 system:

a) Card inquiry and status check

As a variant, the prepaid debit card system provides
10 functionality allowing cardholders to access the prepaid debit card system through a secure means. In a specific example, a dial-up connection including an authentication process is used to connect the customer with the prepaid debit card system. The customer provides the system with
15 data elements such as account number, name and expiry data. The system processes the data elements and if they are valid responds by sending a signal to the customer including account information such as for example:

- 1) Balance remaining
- 20 2) Transaction history

b) Transfers between cards and other financial vehicles

As a variant, the prepaid debit card system provides
25 functionality allowing cardholders to access the prepaid debit card system through a secure means. In a specific example, a dial-up connection including an authentication process is used to connect the customer with the prepaid debit card system. An interface is provided so that a debit
30 card holder may identify himself and is able to transfer amounts between prepaid debit cards, between a prepaid debit card and either one of a bank account, a conventional credit

card or other financial vehicle. The interface will also allow the card holder to identify himself as owning more than one prepaid debit card. The interface also allows transferring amounts between an expired prepaid debit card and a new prepaid debit card, a bank account, a conventional credit card or other financial vehicle. Optionally, the interface may allow the customer to modify the expiry date of his prepaid debit card.

10 c) Currency translations

As a variant, the prepaid debit card system provides functionality allowing cardholders to access the prepaid debit card system through a secure means. In a specific example, a dial-up connection including an authentication process is used to connect the customer with the prepaid debit card system. An interface is provided so that a debit card holder may identify himself and allow converting the currency of the prepaid debit card to another currency. In a specific example of implementation, the prepaid debit card transaction processing unit 100 comprises a currency conversion functional unit operative to map a first amount represented in a first currency to a second amount represented in a second currency. The mapping is effected on a basis of a data element indicative of an exchange rate between the first currency and the second currency. In a first specific example, the data element indicative of an exchange rate is stored on a computer readable medium operative connection to the currency conversion functional unit. The currency conversion functional unit may be embodied in a software module implementing a currency conversion algorithm. In this case the software module is

adapted to be executed on a computing platform such as the bank computing centre. Alternatively, the currency conversion functional unit is hard coded into a hardware unit. In a specific example of implementation, the currency conversion functional unit has an input coupled to a data stream, the data stream including currency conversion data elements. The data stream allows an improvement in the accuracy of the exchange rate. The currency conversion module may also include a commission calculation unit to calculate the commission associated with the currency conversion.

Advantageously, the use of a currency conversion functional unit facilitates the exchange between different currencies.

d) Gift sending

A Web interface will allow customers to purchase prepaid debit cards for secure delivery to third parties. The prepaid debit card details will be sent by encrypted e-mail to the intended recipient.

As a variant, the prepaid debit card transaction processing system provides functionality allowing deposits to be made to the prepaid debit card. In a specific example of implementation, each record in the customer database is associated to a prepaid debit card and comprises a prepaid debit card number and a payment card number. The payment card number is in the same format as conventional credit card numbers. Alternatively, each record in the customer database comprises either one of a prepaid debit

card number and a payment card number as well as an index allowing a mapping to be establish between a payment card number and the corresponding debit card number. The payment card number may be associated to the same expiry date as the prepaid debit card number or alternatively to its own respective expiry date. Other variations in the arrangement of the customer database 64 are possible without detracting from the spirit of the invention. A feature of the prepaid debit card having a payment card number is that the use of the payment card number authorizes the deposit of funds to the prepaid debit card but does not authorize any purchase to take place. Advantageously, prepaid debit cards provided with payment card numbers may be used to facilitate payment from a first party to a second party without the debit card number ever being provided. Since the payment card number only allows deposits, a thief would have no incentive of obtaining it thereby improving the security of the system.

The person skilled in the art will appreciate that the prepaid debit card may be associated to a payment card number in the same format as conventional credit card numbers and no debit card number. In this configuration, the prepaid debit card can receive deposits of funds to the prepaid debit card but cannot authorize any purchase.

25

The processing of a request for authorization with a payment card number may be effected substantially as the processing of a request for authorization with a prepaid debit card number. The difference is that a request with a payment card number will be denied if the transaction is for a purchase. If the request for authorization is accepted, the available funds' limit of the customer's prepaid debit

30

card is increased by the amount of the authorization, and the transaction is logged for future posting.

In another variant, the prepaid debit card transaction processing system 100 allows the restriction of the field of use of the prepaid debit card. Example of restrictions may include country(ies) in which the prepaid debit card may be used, merchants where the prepaid debit card may (not) be used, allowed maximum/minimum transaction amounts among others. Advantageously, the restrictions as to the use of the prepaid debit card provide an additional level of security for the customer. In a specific example of implementation, the restrictions are incorporated in a restriction data field in each record of the customer database 64. For each type of restriction supported by the prepaid debit card transaction processing system 100, the restriction data field is assigned a unique code. When an authorization request is processed by the prepaid debit card transaction processing system 100, the restriction data field is checked against the data elements provided by the merchant and a determination is made whether a restriction preventing the transaction from taking place applies. If a restriction applies, the request for authorization is denied.

25

As yet another variant, the prepaid debit card system 100 is integrated into a separate network distinct from an issuing bank. In this configuration, the prepaid debit card system 100 is suitable for use in business to business transactions. In a specific example, businesses sign up for a prepaid debit card and interact directly with the prepaid debit card system 100 over a private communication link or

30

the internet to effect transaction. In this fashion, the involvement of the issuing bank can be avoided and consequently, the costs typically charged by the bank in the form of the transaction fees or commissions can also be
5 avoided.

Although the present invention has been described in considerable detail with reference to certain preferred embodiments thereof, variations and refinements are possible
10 without departing from the spirit of the invention. Therefore, only the appended claims and their equivalents should limit the scope of the invention.

Claims:

1. A method for providing a prepaid debit card.
5
2. A method for providing a prepaid debit card suitable for use in conjunction with a conventional credit card infrastructure.
- 10 3. A method for issuing a prepaid debit card over a network, said method comprising:
 - 15 - receiving a set of information data elements associated to a customer over a communication link, the set of information data elements including payment information;
 - processing the set of data elements to determine on a basis of the payment information an authorization data element, the authorization data element being indicative of either one of an approved transaction
20 and a refused transaction;
 - generating credit data elements indicative of a prepaid debit card when the authorization data element is indicative of an approved transaction.
- 25 4. A method for processing a transaction over a network, the transaction involving a prepaid debit card.
5. A system for providing a prepaid debit card.
- 30 6. A system for processing a transaction over a network, the transaction including a prepaid debit card.

7. A prepaid debit card as described in the specification.

8. A prepaid debit card being characterized by:

- 5 - a debit card number data element;
- a user name;
- an expiry date;
- a currency;
- a prepaid debit limit.

1/3

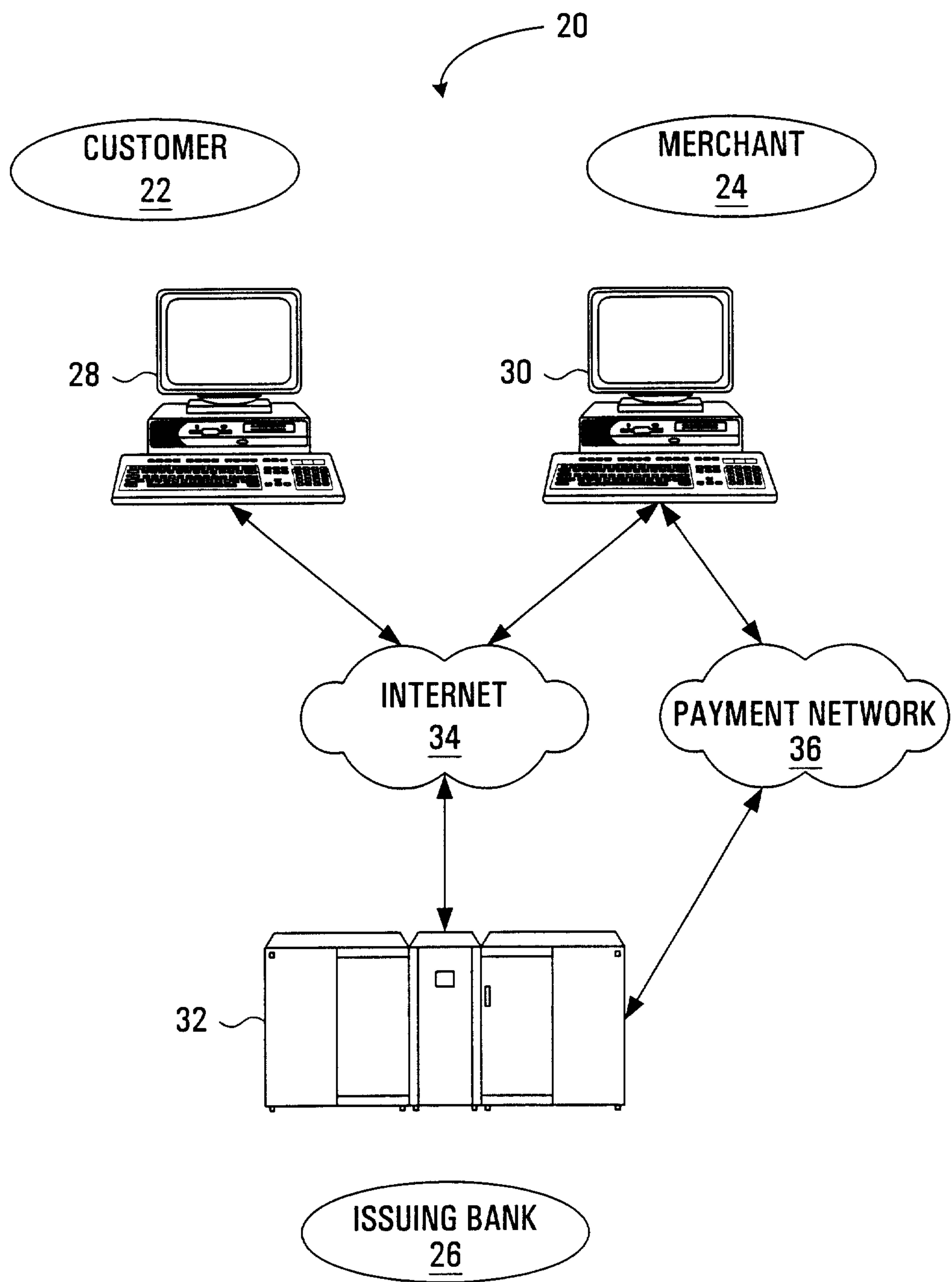


FIG. 1

2/3

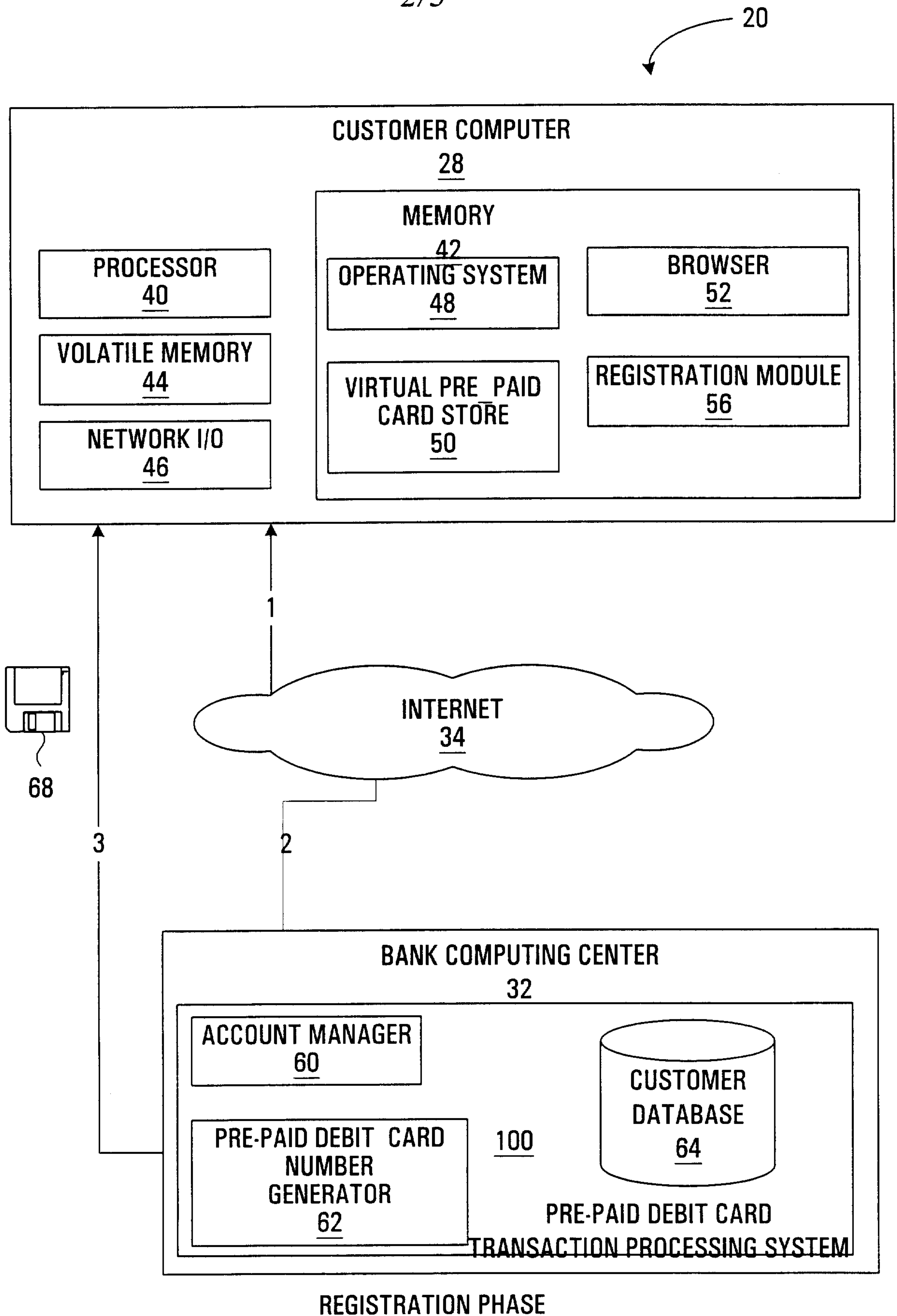
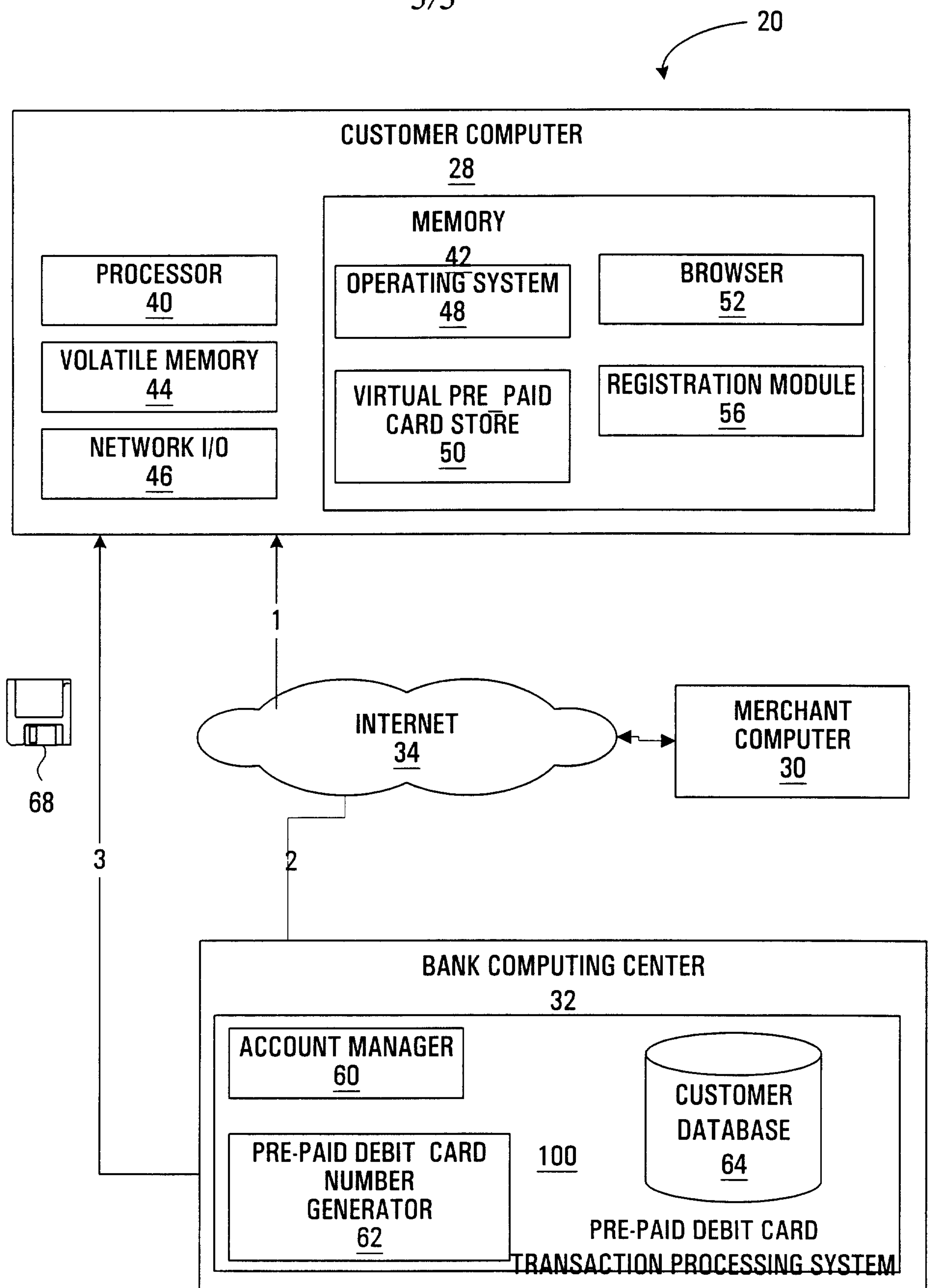


FIG. 2

3/3



REGISTRATION PHASE

FIG. 3

