US 20080235136A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2008/0235136 A1**

Kemper et al. (43) **Pub. Date: Sep. 25, 2008**

(54) **SYSTEM FOR PERSONAL AUTHORIZATION CONTROL FOR CARD TRANSACTIONS**

(76) Inventors: **Lynn Kemper**, San Carlos, CA (US); **Akshey Shawn Vij**, Mountain View, CA (US); **Robin O'Connell**, San Francisco, CA (US)

Correspondence Address:
TOWNSEND AND TOWNSEND CREW LLP
TWO EMBARCADERO CENTER, 8TH FLOOR
SAN FRANCISCO, CA 94111 (US)

(21) Appl. No.: **12/129,217**

(22) Filed: **May 29, 2008**

Related U.S. Application Data

(63) Continuation of application No. 11/747,659, filed on May 11, 2007, which is a continuation of application No. 10/093,002, filed on Mar. 5, 2002, now Pat. No. 7,389,275.

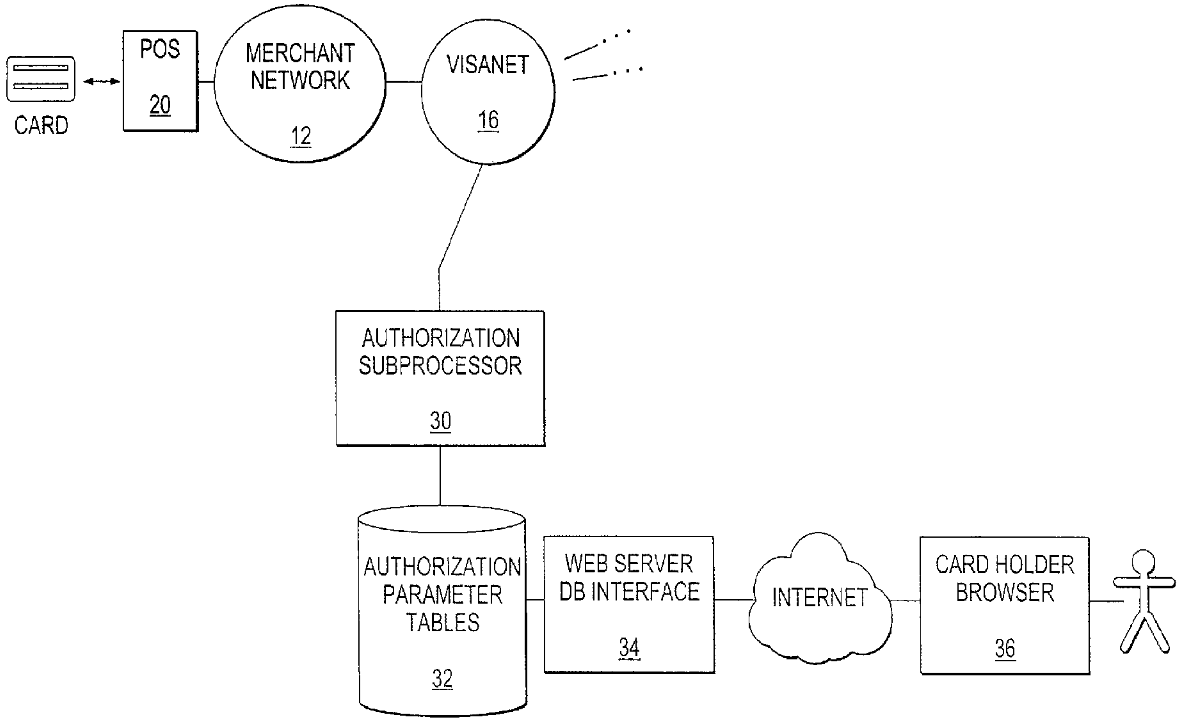
Publication Classification

(51) **Int. Cl.**
G06Q 20/00 (2006.01)

(52) **U.S. Cl.** **705/44**

(57) **ABSTRACT**

An authorization system allows for cardholder-provided parameters to a personal authorization subsystem. The parameters can be selected by the cardholder to limit the authorizations that would otherwise be granted on the card. The parameters can indicate limits by frequency, dollar amount, merchant, geographic location, time of day, combinations thereof, or the like. Authorization for a given transaction, even where authorized by an issuer and a network operator, might be denied based on self-constraints set by the cardholder. In some variations, messages are sent to the cardholder based on constraints set by the cardholder and transactions might be approved and messaged, or denied and messaged.



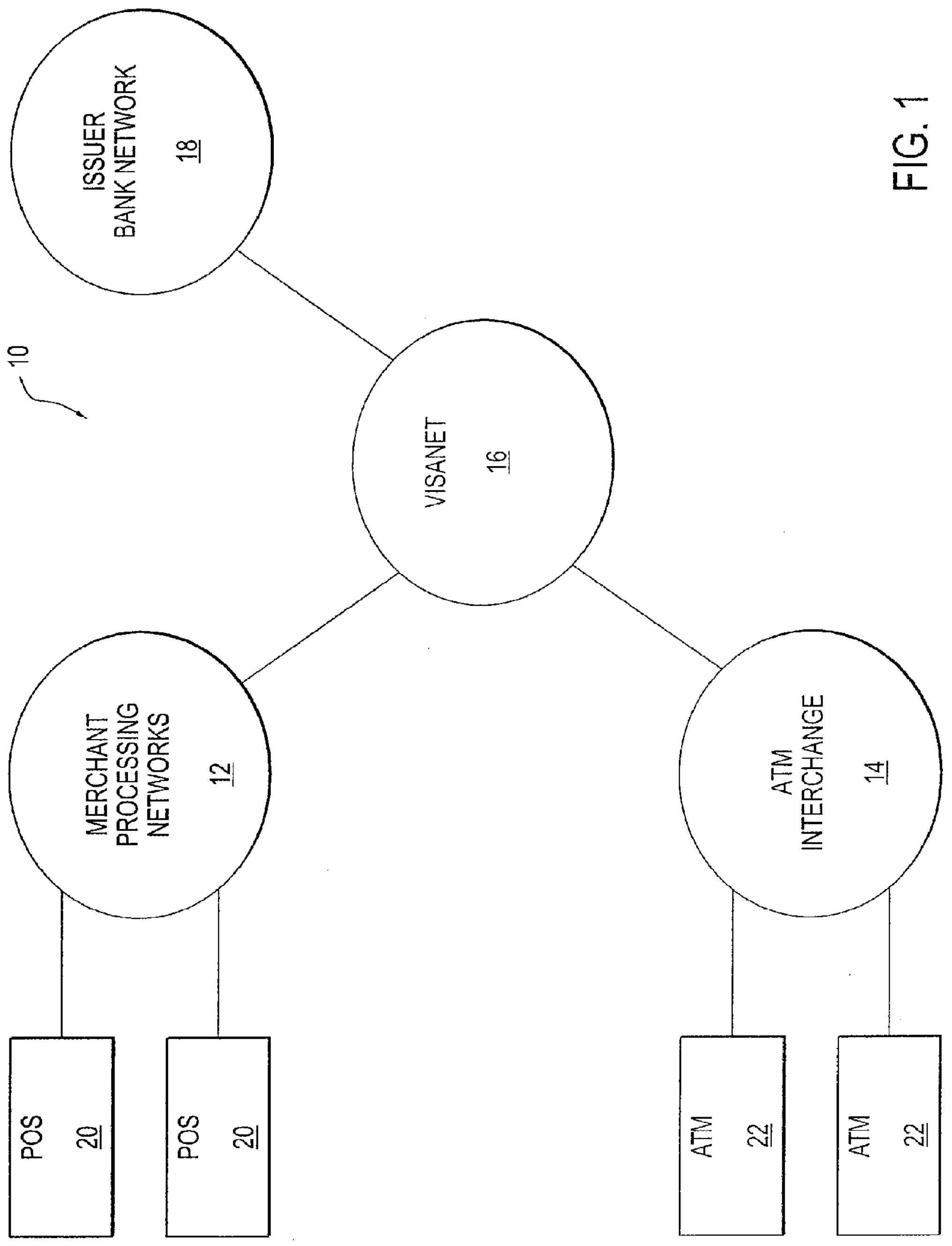

10
ISSUER
BANK NETWORK
18
VISANET
16
MERCHANT
PROCESSING
NETWORKS
12
ATM
INTERCHANGE
14
POS
20
POS
20
ATM
22
ATM
22

FIG. 1

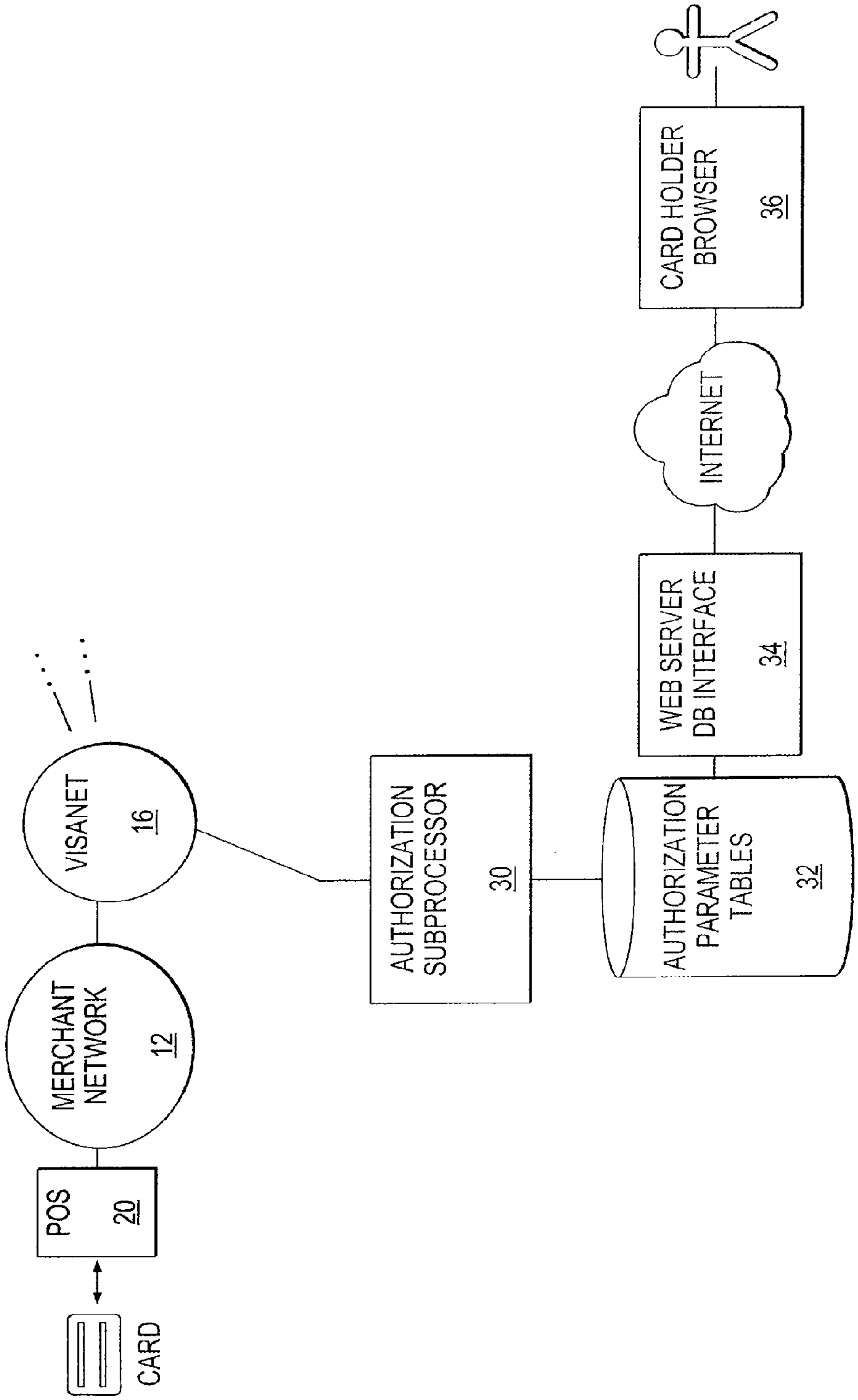

CARD
POS
20
MERCHANT NETWORK
12
VISANET
16
AUTHORIZATION SUBPROCESSOR
30
AUTHORIZATION PARAMETER TABLES
32
WEB SERVER DB INTERFACE
34
INTERNET
CARD HOLDER BROWSER
36

FIG. 2

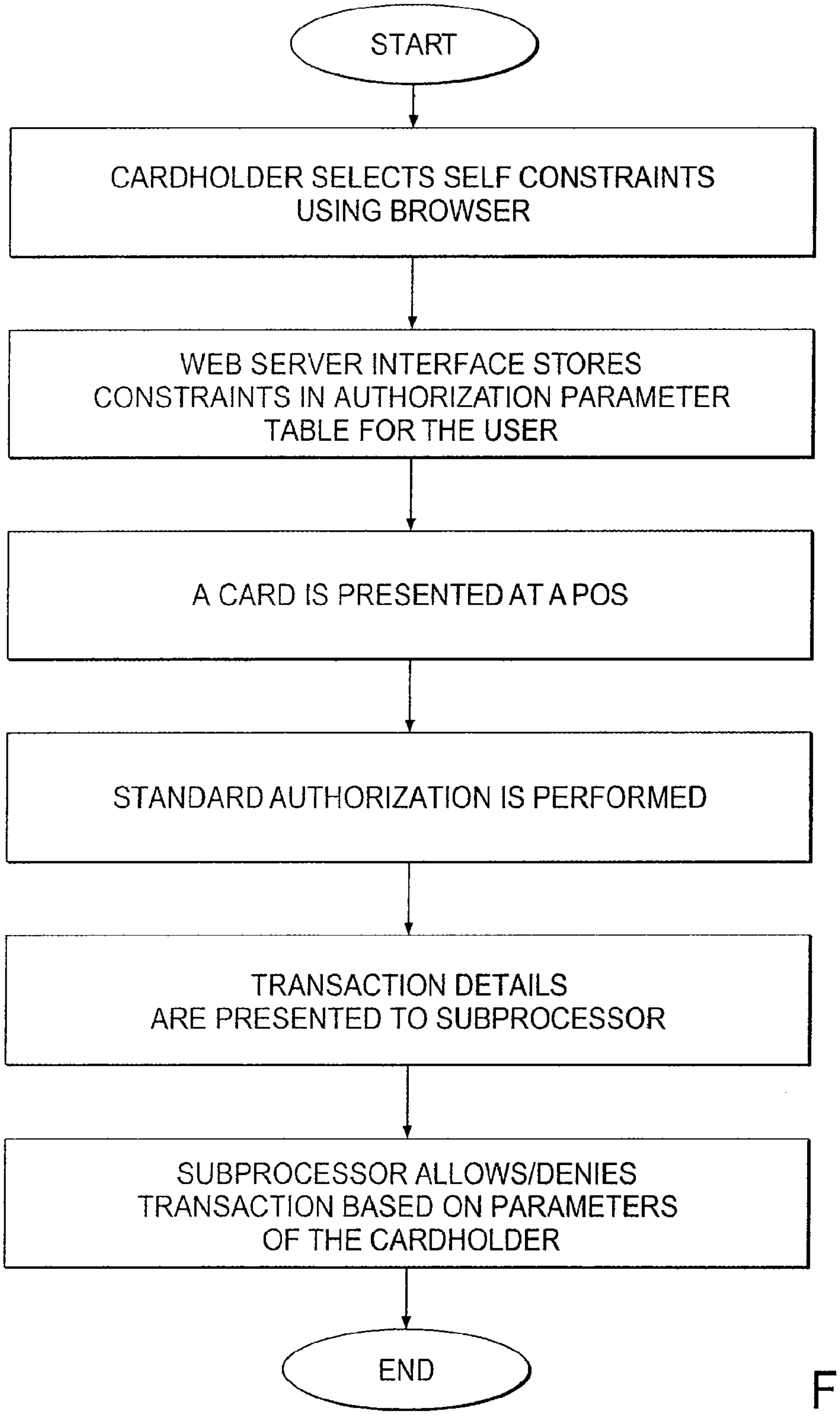
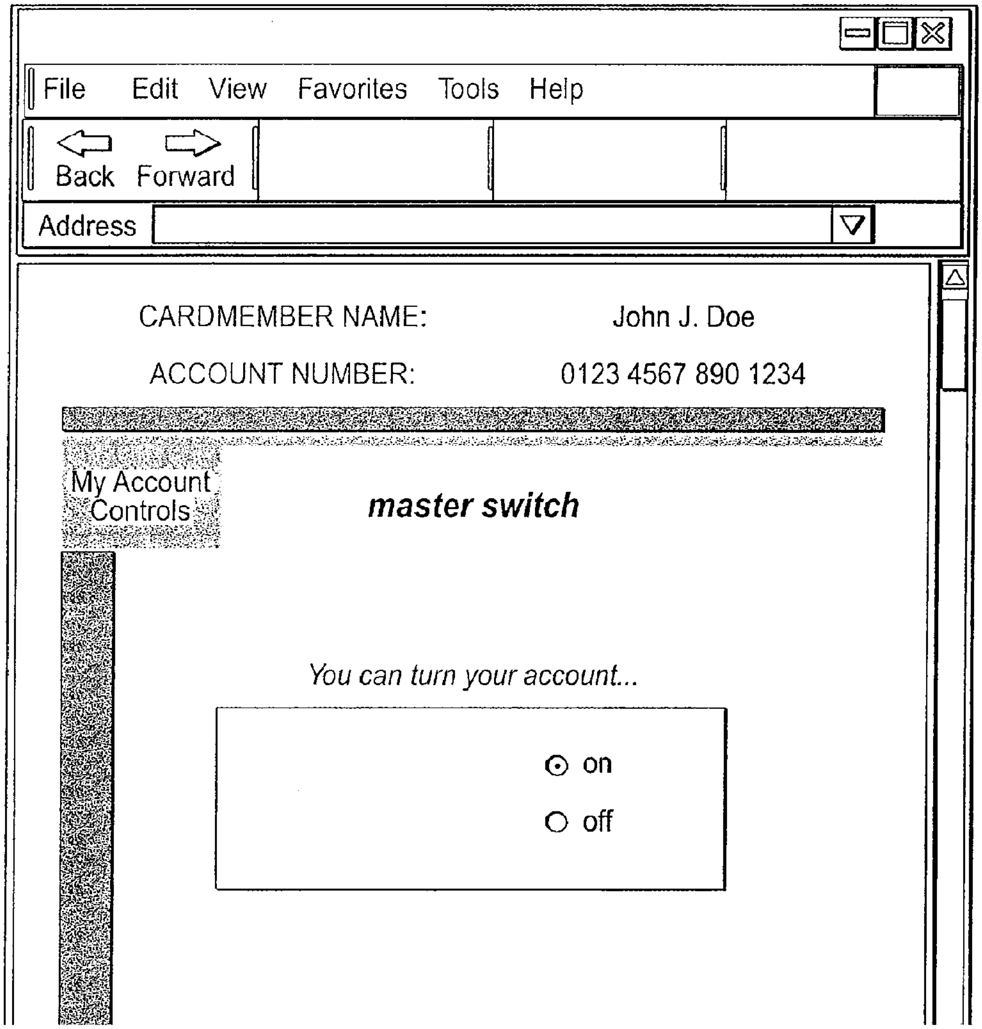

START
CARDHOLDER SELECTS SELF CONSTRAINTS USING BROWSER
WEB SERVER INTERFACE STORES CONSTRAINTS IN AUTHORIZATION PARAMETER TABLE FOR THE USER
A CARD IS PRESENTED AT A POS
STANDARD AUTHORIZATION IS PERFORMED
TRANSACTION DETAILS ARE PRESENTED TO SUBPROCESSOR
SUBPROCESSOR ALLOWS/DENIES TRANSACTION BASED ON PARAMETERS OF THE CARDHOLDER
END

FIG. 3



CARDMEMBER NAME: John J. Doe

ACCOUNT NUMBER: 0123 4567 890 1234

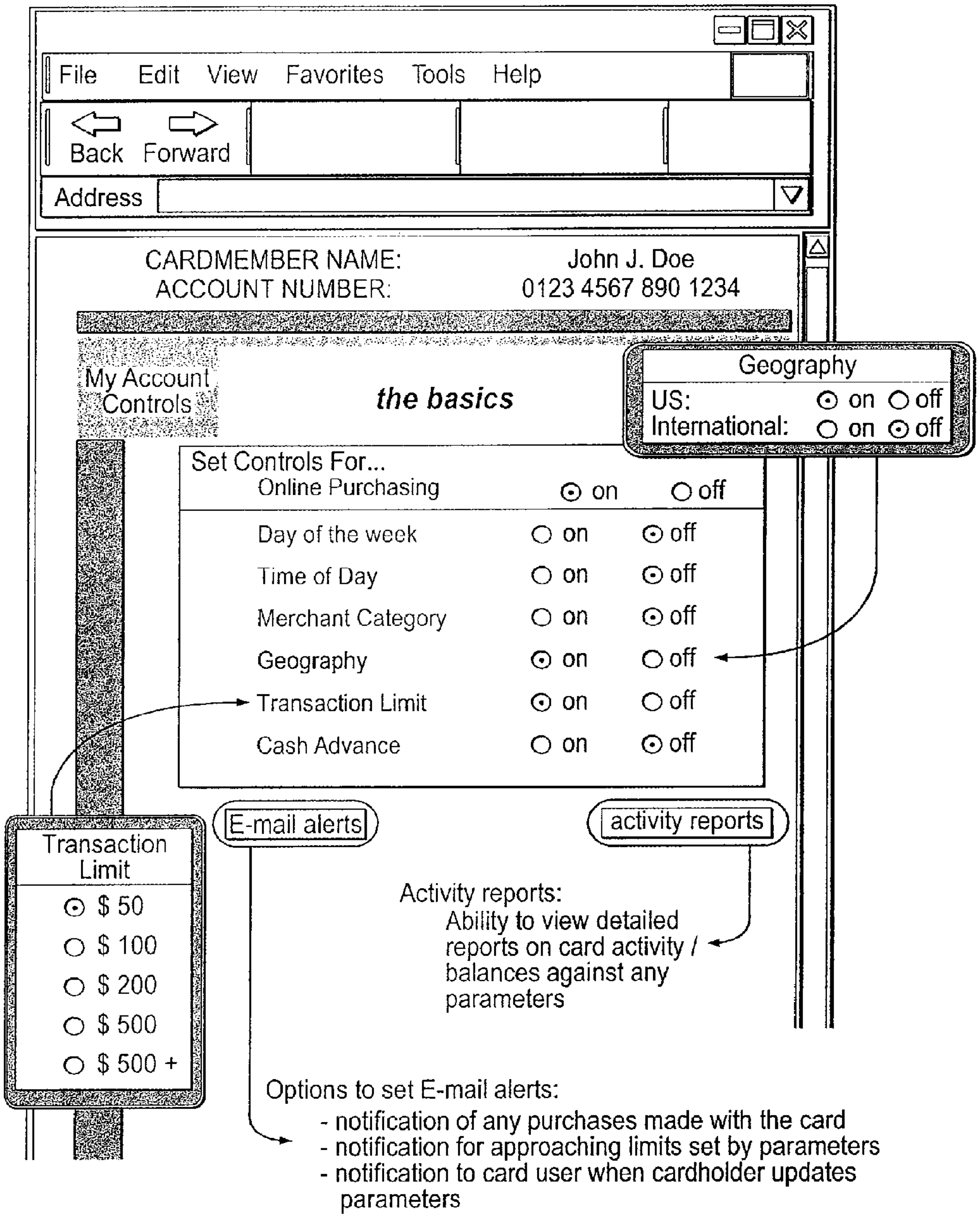
master switch

You can turn your account...

⦿ on

○ off

FIG. 4(a)



CARDMEMBER NAME: John J. Doe
ACCOUNT NUMBER: 0123 4567 890 1234

Geography		
US:	● on	○ off
International:	○ on	● off

Set Controls For...		
Online Purchasing	● on	○ off
Day of the week	○ on	● off
Time of Day	○ on	● off
Merchant Category	○ on	● off
Geography	● on	○ off
Transaction Limit	● on	○ off
Cash Advance	○ on	● off

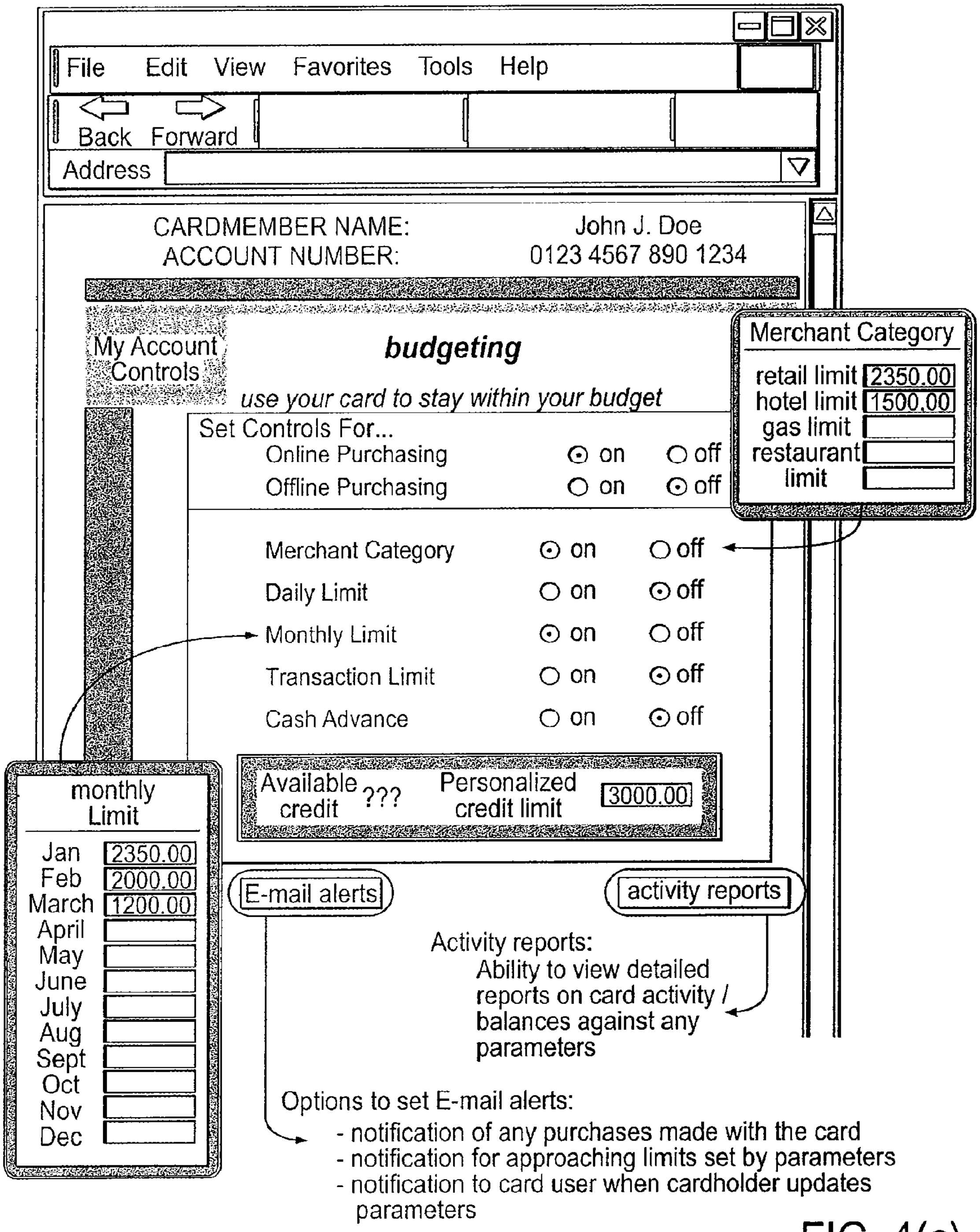
Transaction Limit

● $ 50
○ $ 100
○ $ 200
○ $ 500
○ $ 500 +

Activity reports:
Ability to view detailed reports on card activity / balances against any parameters

Options to set E-mail alerts:
- notification of any purchases made with the card
- notification for approaching limits set by parameters
- notification to card user when cardholder updates parameters

FIG. 4(b)



CARDMEMBER NAME: John J. Doe
ACCOUNT NUMBER: 0123 4567 890 1234

budgeting

use your card to stay within your budget

Set Controls For...

Online Purchasing	⊙ on	○ off
Offline Purchasing	○ on	⊙ off
Merchant Category	⊙ on	○ off
Daily Limit	○ on	⊙ off
Monthly Limit	⊙ on	○ off
Transaction Limit	○ on	⊙ off
Cash Advance	○ on	⊙ off

Available credit ??? Personalized credit limit 3000.00

Merchant Category

retail limit	2350.00
hotel limit	1500.00
gas limit	
restaurant limit	

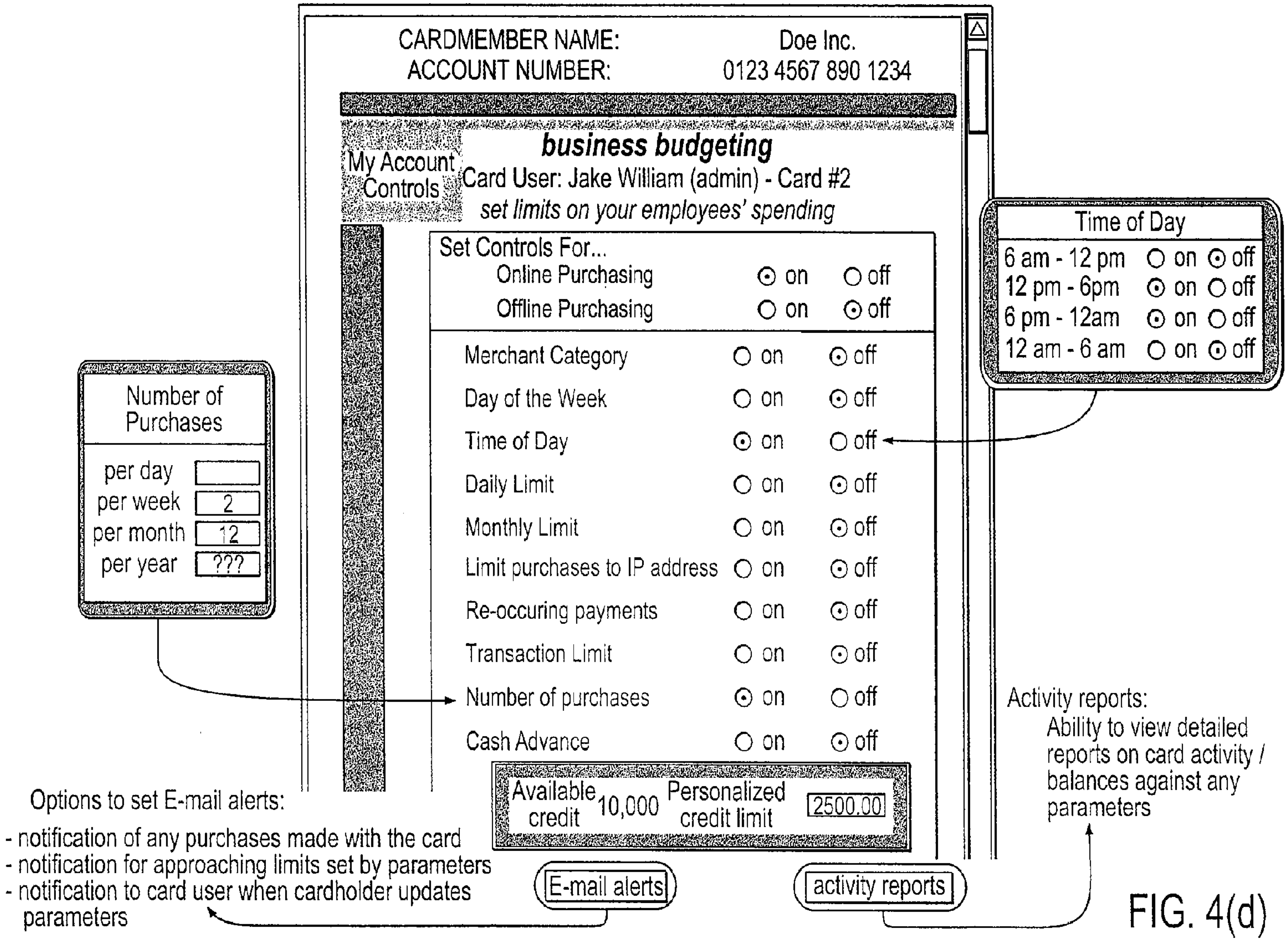
monthly Limit

Jan	2350.00
Feb	2000.00
March	1200.00
April	
May	
June	
July	
Aug	
Sept	
Oct	
Nov	
Dec	

Activity reports:
Ability to view detailed reports on card activity / balances against any parameters

Options to set E-mail alerts:
- notification of any purchases made with the card
- notification for approaching limits set by parameters
- notification to card user when cardholder updates parameters

FIG. 4(c)



CARDMEMBER NAME: Doe Inc.
ACCOUNT NUMBER: 0123 4567 890 1234

My Account Controls

business budgeting

Card User: Jake William (admin) - Card #2

set limits on your employees' spending

Set Controls For...		
Online Purchasing	⊙ on	○ off
Offline Purchasing	○ on	⊙ off
Merchant Category	○ on	⊙ off
Day of the Week	○ on	⊙ off
Time of Day	⊙ on	○ off
Daily Limit	○ on	⊙ off
Monthly Limit	○ on	⊙ off
Limit purchases to IP address	○ on	⊙ off
Re-occuring payments	○ on	⊙ off
Transaction Limit	○ on	⊙ off
Number of purchases	⊙ on	○ off
Cash Advance	○ on	⊙ off

Available credit 10,000 Personalized credit limit 2500.00

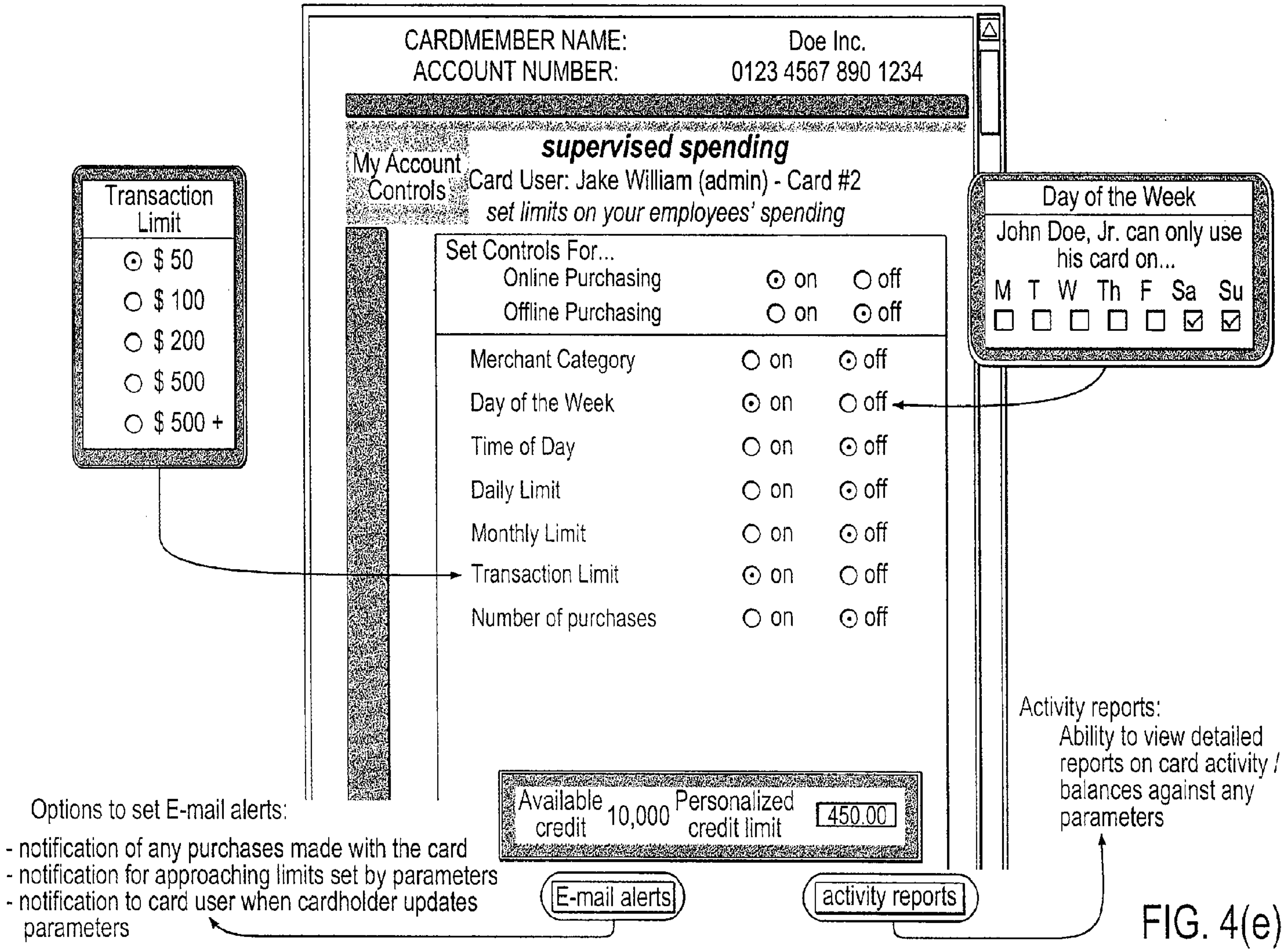
Time of Day		
6 am - 12 pm	○ on	⊙ off
12 pm - 6pm	⊙ on	○ off
6 pm - 12am	⊙ on	○ off
12 am - 6 am	○ on	⊙ off

Number of Purchases	
per day	
per week	2
per month	12
per year	???

Options to set E-mail alerts:
- notification of any purchases made with the card
- notification for approaching limits set by parameters
- notification to card user when cardholder updates parameters

Activity reports:
Ability to view detailed reports on card activity / balances against any parameters

FIG. 4(d)



CARDMEMBER NAME:	Doe Inc.
ACCOUNT NUMBER:	0123 4567 890 1234

My Account Controls

supervised spending

Card User: Jake William (admin) - Card #2

set limits on your employees' spending

Set Controls For...		
Online Purchasing	● on	○ off
Offline Purchasing	○ on	● off
Merchant Category	○ on	● off
Day of the Week	● on	○ off
Time of Day	○ on	● off
Daily Limit	○ on	● off
Monthly Limit	○ on	● off
Transaction Limit	● on	○ off
Number of purchases	○ on	● off

Available credit 10,000 Personalized credit limit 450.00

Transaction Limit

● $ 50
○ $ 100
○ $ 200
○ $ 500
○ $ 500 +

Day of the Week

John Doe, Jr. can only use his card on...

M	T	W	Th	F	Sa	Su
☐	☐	☐	☐	☐	☑	☑

Options to set E-mail alerts:

- notification of any purchases made with the card
- notification for approaching limits set by parameters
- notification to card user when cardholder updates parameters

Activity reports:

Ability to view detailed reports on card activity / balances against any parameters

FIG. 4(e)

SYSTEM FOR PERSONAL AUTHORIZATION CONTROL FOR CARD TRANSACTIONS

FIELD OF THE INVENTION

[0001] The present invention relates to financial transaction processing systems in general and more specifically to financial transaction processing systems that relate a transaction to a cardholder and include authorization systems that authorize or deny credits or debits related to transactions.

BACKGROUND OF THE INVENTION

[0002] Credit card transactions are a common method of effecting payment in connection with a transaction. In a typical transaction, a cardholder selects merchandise or services and presents a card, such as a VISA® credit card, check card or debit card, to a merchant. Before the merchant releases the merchandise or performs the service, the merchant will typically get authorization for a charge in the amount agreed on for the merchandise or service, at the point-of-sale.

[0003] Today, most authorizations are electronic, where the merchant obtains the cardholder name, account number and possibly other information. The merchant transmits that information, along with transaction-specific information, possibly including a merchant identifier, a transaction amount and a transaction description. The merchant transmits the information as part of an authorization message directed through an authorization network to a card issuer. When a card issuer approves a transaction, the merchant is given certain assurances that the merchant's bank account will be credited with the amount of the transaction and accordingly is willing to release the goods or services to the purchaser.

[0004] The cardholder generally agrees to pay for any transactions applied to the cardholder's account. In some cases, however, the cardholder's issuer financial institution (FI) or the network operator will be liable to the merchant instead of the cardholder, as in the case of a stolen card being used after the cardholder notified the issuer FI. Naturally, the issuer FI and network operator have a large incentive to limit the number of transactions for which they are liable. As a result, the typical merchant agreement requires that the merchant perform an authorization before the risk of nonpayment passes from the merchant to the issuer FI or the network operator and the issuer FI and network operator place constraints on authorizations.

[0005] For example, where a card is typically used for small transactions relating to groceries and gasoline, frequent transactions relating to expensive jewelry might prompt the authorization system to deny the transaction as a suspect activity even if ultimately the cardholder is legitimately purchasing jewelry. The denial serves to protect the issuer FI and limit the liability of the issuer FI for transactions that the cardholder might later indicate as being fraudulent. The authorization system would not necessarily deny transactions that were not intended by the cardholder, and is generally limited to denying transactions under conditions that the issuer FI or the network operator might deem indicative of fraud. The issuer FI might also deny authorization where the transaction amount would cause the cardholder's credit limit to be exceeded.

[0006] In many cases, the openness and independence of the card network makes it more difficult to control the uses of the cards, but that becomes even more important where the cards used in the card network are so widely accepted and pervasive.

BRIEF SUMMARY OF THE INVENTION

[0007] In one embodiment of an authorization system according to the present invention, a cardholder provides parameters to a personal authorization subsystem. The parameters can be selected by the cardholder to limit the authorizations that would otherwise be granted on the card. The parameters can indicate limits by frequency, dollar amount, merchant, merchant type, credit limits, geographic location, time of day, combinations thereof, or the like. In a preferred embodiment, the cardholder provides the parameters to the cardholder's issuer financial institution, which integrates the cardholder authorizations with the issuer financial institution authorization process. The issuer financial institution is independent of the merchants accepting the card and the card network operator operates an open, independent network for accepting the cards of many issuer financial institutions usable with many independent merchants.

[0008] For a further understanding of the nature and advantages of the invention, reference should be made to the ensuing description in conjunction with the accompanying drawings

BRIEF DESCRIPTION OF THE DRAWINGS FIG. **1** is a block diagram of a transaction system wherein the present invention might be used.

[0009] FIG. **2** is a more detailed block diagram illustrating aspects of an authorization subprocessor and a cardholder's interaction with the subprocessor.

[0010] FIG. **3** is a flowchart illustrating a process of authorization control.

[0011] FIGS. **4**(*a*)-(*e*) illustrate aspects of a user interface usable to set cardholder authorization parameters.

DETAILED DESCRIPTION OF THE INVENTION

[0012] FIG. **1** is a block diagram of a transaction system **10**. As shown there, transaction system **10** includes a merchant processing networks **12**, an automated teller machine (ATM) interchange **14** coupled to a transaction network **16**, such as the VISANET® network, which is in turn coupled to an issuer bank network **18**. As shown, a plurality of point of sale (POS) terminals **20** are coupled to merchant processing network **12** and a plurality of ATM's **22** are coupled to ATM interchange **14**. It should be understood that the typical transaction system couples many merchant networks, ATM interchanges and issuer bank networks, in addition to merchant bank networks.

[0013] In a typical operation of transaction system **10**, a card is presented to a POS terminal **20** and a transaction is generated between a cardholder and a merchant that 1) debits a cardholder's account at the cardholder's issuer bank, 2) credits a merchant's account at the merchant acquirer bank and generates the necessary electronic messages for settlement among the banks and other transaction processing. As part of the transaction, an authorization will be performed, wherein the merchant gathers up the transaction information and sends an authorization request message to the network and receives back an authorization result, such as "approved", "denied", "ask for ID", etc.

[0014] FIG. **2** is a more detailed block diagram illustrating aspects of authorization. In one such process, a card is presented to POS terminal **20** which includes means for reading card contents, such as a magnetic card reader or a smartcard reader. POS terminal **20** is coupled to merchant network **12** and transaction network **16**, which performs authorizations to protect the issuer FI or the network operator.

[0015] Transaction network **16** is also coupled to an authorization subprocessor **30**, which can cause an otherwise allowable transaction to be denied, based on cardholder-provided authorization parameters available in an authorization parameter table (APT) of a plurality of authorization parameter tables **32**. A cardholder's APT can be populated and updated or modified by a web server database interface **34** under the direction of a web browser **36** operated by the cardholder. As used herein, the cardholder refers to the person or persons that that issuer FI holds responsible for payment. A legitimate card presenter, i.e., the person presenting the card in a transaction, might be the cardholder, but could also be other authorized agents, such as a person to whom an additional card was issued. While this description describes a Web client-server based interface, it should be understood that other interfaces, such as direct connections, local network connections, kiosks, telephone interfaces or the like would be used instead to allow a cardholder to modify the APT associated with that cardholder's account.

[0016] In a typical operation, illustrated in FIG. **3**, the cardholder (i.e., one of those ultimately responsible for non-fraudulent transactions on the card) will create, modify or update the corresponding APT to set self constraints using a browser and the linked-to web server interface stores such self constraints in the corresponding APT. Once the APT contains the cardholder supplied self constraint parameters, if a card is presented at a POS terminal, a normal authorization process occurs, wherein the issuer FI or network owner criteria for allowing the transaction are tested. If the issuer FI and network owner would deny the transaction, no further processing is needed and a denial message can be sent to the POS terminal. However, if the issuer FI and network owner would approve the transaction, the transaction details are then presented to the authorization subprocessor. The authorization subprocessor approves or denies the transaction based on the cardholder's APT, which contains constraints set by the cardholder.

[0017] While the self constraints are set by the cardholder and therefore could easily be overridden by the cardholder himself or herself, they nonetheless constrain the cardholder's account, at least by denying transactions where the cardholder unintentionally exceeds constraints, another card carrier exceeds the constraints and also constrain fraudulent use of the card that is only detectable in advanced based on constraints set by the cardholder.

[0018] The authorization subprocessor is described above as acting to approve or deny a transaction. In some embodiments, the authorization subprocessor might, in addition to or in lieu of approval/denial, perform cardholder notifications. A cardholder notification is a message to the cardholder, or to a system designated by the cardholder, that a transaction occurred and fell within cardholder-set parameters. In some cases, the transaction is also denied, but typically the transaction is allowed, with notification. Such details can be specified by the cardholder in the parameters. The notification messages can be by mail, by telephone, by pager, by e-mail, by instant message, or by other messaging methods currently known or otherwise.

Examples of Constraints

[0019] Detailed examples of some of the possible constraints will now be described. Such constraints are specified in the APT. For ease of management, the constraints might be grouped for the cardholder into a few categories of constraints, as follows:

[0020] Transaction Type

- **[0021]** Deny cash advances, but allow purchases.

[0022] Transaction Amount

- **[0023]** Allow a transaction below a set limit
- **[0024]** Allow transaction if total transactions would remain below a limit (personalized credit limit)
- **[0025]** Allow transaction if total transactions in a set time period are below a limit
- **[0026]** Daily Limits
- **[0027]** Limit on number of transactions

[0028] Transaction Details

- **[0029]** Allow transaction only during set times of the day (this allows the cardholder to in effect, indicate that any transaction made between midnight and 5 AM is a priori a fraudulent transaction)
- **[0030]** Allow transaction only during set times of the week (e.g., movie purchases not allowed during the week)
- **[0031]** Allow offline transactions, but not online (telephone, Internet, etc.) transactions
- **[0032]** Allow online transactions, but only from pre-specified IP addresses
- **[0033]** Allow transactions based on geographic location (e.g., block purchases outside U.S.)
- **[0034]** Allow transactions based on the merchant category type (e.g., restaurants and hotels but not retail stores)

[0035] Other Limits

- **[0036]** Preauthorization for one-time transactions
- **[0037]** Recurring Payment Authorization
- **[0038]** Varying controls from card carrier to card carrier
- **[0039]** Instant Cut-off (useful when the cardholder is aware of the theft but the issuer FI has not yet detected it or is still processing the cardholder's request for closing their account.)

[0040] Arbitrary combinations of these constraints might also be possible, such as a cardholder specifying that cash advances are allowed within the U.S., but not outside the U.S. and outside the U.S. transactions are allowed, but only for merchants in the food, medical, travel and lodging categories during a prespecified date range. As another example, a parent cardholder might get an e-mail whenever a child card carrier effects an online purchase.

[0041] In addition to constraints, the APT might also contain data that directs other actions unrelated to authorization. One such action is ancillary messaging, wherein under cardholder selected conditions, a message (such as a pager message, e-mail message or instant message) is sent to a prespecified address if the conditions are met. Such conditions include card carriers that are minors effecting a transaction with an inappropriate merchant. In some cases, the cardholder might set the condition such that an e-mail is generated with every transaction, thus allowing for the electronic collection of receipts. The messages might be selective, such that only approvals result in messages or only denials result in messages (and might include the reason for the denial).

User Interfaces

[0042] Examples of the user interfaces that might be presented to a cardholder via a cardholder browser are shown in FIGS. **4**(*a*)-(*e*). Other user interfaces might also be used, such as a calendar view where the cardholder could click on calendar days to allow or deny transactions for those dates. Another user interface might provide a listing of various merchant types to allow that cardholder to set predetermined ranges for each of a plurality of merchant types.

Variations

[0043] In the above, described system, the cardholder creates, modifies or updates the cardholder's APT via a Web interface. In another variation, the cardholder can interact with a telephone voice response unit (VRU) or automatic response unit (ARU) using the telephone keypad, to interact with a server that performs the requested actions on the APT. In a useful combination, the Web interface is accessible from a Web page maintained by the issuer FI for card customers. Such a Web interface might be provided to show transaction details and other account information. In some embodiments, the e-mail messages sent to the cardholder could include a hypertext link to a page showing details of the transaction so the cardholder can jump directly to a detail page from an e-mail.

[0044] Where multiple card carriers (i.e., persons with cards to present for purchases who are not necessarily the cardholder responsible for the account) are present, the user interface might allow for any variations of constraints to be selected and be different for different car carriers.

[0045] In a permissive variation, the authorization subprocessor never denies an authorization that would have otherwise been granted by the issuer FI or network operator, but just sends a message to the prespecified location when the transaction hits certain constraints. This might be useful where a cardholder needs or wants to observe transactions as they happen, to allow for early intervention. This might be useful for businesses where the card carriers are employees empowered to make purchases for the business.

[0046] Cardholder specified constraints, implemented in an authorization system has now been described. As explained, the cardholder can apply constraints to the use of a card, typically to constrain the purchases of other authorized card carriers and of unauthorized users operating with transaction patterns not likely to be used by the cardholder and thus not constraining on the cardholder (e.g., limited to selected countries, times of day, size of transactions that the cardholder would not participate in), but could also be used by the cardholder to constrain the cardholder himself or herself for particular transactions. The latter might be useful for budget controls or controls on inadvertent spending.

[0047] As will be understood by those familiar with the art, the present invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. For example, the authorization subprocessor can be integrated in with the authorization processor that applies the issuer FI or network operator criteria to the transaction. As another example, while the present invention is described primarily with reference to credit cards, it is also usable for debit card transactions. As yet another example, while the present invention is described primarily with to merchant POS terminals, it should be understood that other systems for initiating purchase transactions might be used instead, without departing from the scope of the invention, such as the use of a merchant payment server, a PC-based cardholder terminal, a telephone, etc. or other location or system a cardholder might interface to in making a purchase, possibly even including systems where the cardholder does not interface to a system at all.

[0048] Accordingly, the disclosure of the preferred embodiments of the invention is intended to be illustrative, but not limiting, of the scope of the invention which is set forth in the following claims.

1.-**2**. (canceled)

3. A system comprising:

an authorization subprocessor configured to deny a transaction based on a plurality of user selected authorization parameters and constraints;

an authorization parameter table database coupled to the authorization subprocessor; and

an interface coupled to the authorization parameter table database, wherein the interface is configured to be in communication with a telephone, wherein the telephone allows a user to select a combination of authorization constraints from a plurality of authorization constraints, and allows the user to select authorization parameters associated with the selected authorization constraints, wherein the selected authorization constraints and the selected authorization parameters are used by the authorization subprocessor to determine whether or not a transaction is authorized.

4. The system of claim **3**, wherein the authorization parameter table database stores at least two sets of authorization constraints and parameters for the user.

5. The system of claim **3** further comprising the telephone operatively coupled to the interface.

6. The system of claim **3** wherein the authorization parameters include listings of selectable values from which the user may select the authorization parameters.

7. The system of claim **3** wherein the authorization parameters include listings of selectable values from which the user may select the authorization parameters, the selectable values including amounts of money or days of the week.

8. The system of claim **3** wherein the transaction is a credit card transaction.

9. The system of claim **3** wherein the telephone additionally allows a user to select an activity report or notification option for notifying the user of purchases made.

10. A method comprising:

receiving from a telephone, user selections of a combination of authorization constraints from a plurality of authorization constraints;

receiving from the telephone, user selections of authorization parameters associated with the user selected constraints; and

storing the user selected authorization constraints and the user selected authorization parameters in an authorization parameter table database,

wherein an authorization subprocessor uses the user selected authorization constraints and the user selected authorization parameters to determine if a conducted transaction is authorized or not.

11. The method of claim **10** further comprising using the authorization subprocessor to determine if the transaction is authorized.

12. The method of claim **10** wherein the transaction is a credit card transaction.

13. The method of claim **10**, wherein the authorization parameter table database stores at least two sets of authorization constraints and parameters for the user.

14. The method of claim **10** wherein the authorization parameters include listings of selectable values from which the user may select the authorization parameters, the selectable values including amounts of money or days of the week.

15. A device comprising:

a telephone, wherein the telephone is configured to receive user selections of a combination of authorization constraints from a plurality of authorization constraints, receive user selections of authorization parameters associated with the user selected constraints, and store the user selected authorization constraints and the user selected authorization parameters in an authorization parameter table database, wherein an authorization subprocessor uses the user selected authorization constraints and the user selected authorization parameters to determine if a conducted transaction is authorized or not.

16. The device of claim **15** wherein the telephone if further configured to be in communication with an interface, the interface being coupled to the authorization parameter table database.

17. The device of claim **15** wherein the transaction is a credit card transaction.

18. The device of claim **15**, wherein the authorization parameter table database stores at least two sets of authorization constraints and parameters for the user.

19. The device of claim **15** wherein the authorization parameters include listings of selectable values from which the user may select the authorization parameters, the selectable values including amounts of money or days of the week.

* * * * *