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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 July 2001 (19.07.2001)

PCT

(10) International Publication Number
WO 01/52203 A1

(51) International Patent Classification⁷: G07F 7/10, 19/00

(21) International Application Number: PCT/IB01/00014

(22) International Filing Date: 10 January 2001 (10.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/174,912	10 January 2000 (10.01.2000)	US
09/506,693	18 February 2000 (18.02.2000)	US

(71) Applicant and
(72) Inventor: SINGH, Kunwar, C. [GB/US]; 1152 Calle Vista Drive, Beverly Hills, CA 90210 (US).

(74) Agents: GOLDHUSH, Douglas, H. et al.; Arent Fox Kintner Plotkin & Kahn, PLLC, Suite 600, 1050 Connecticut Avenue, N.W., Washington, DC 20036-5339 (US).

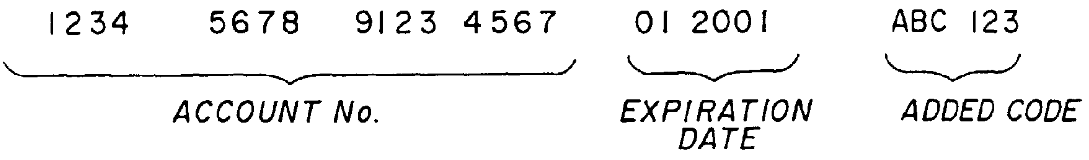
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ONLINE CREDIT CARD SECURITY SYSTEM



(57) Abstract: A method of providing secure credit card transactions includes the steps of providing first credit card account information to a card holder, with the credit card account information including a predetermined account field. A changeable account field is provided with the changeable account field containing changeable account information being changeable by the card holder. An authorization request is received from a vendor. The authorization request includes second credit card account information. Charges to the credit card account are authorized only when the second credit card account information provided by the vendor matches the first credit card account information, including changeable account information.

TITLE OF THE INVENTION:

ONLINE CREDIT CARD SECURITY SYSTEM

CROSS REFERENCE TO RELATED APPLICATIONS:

This application claims priority of United States provisional patent application Serial No. 60/174,912, filed on January 10, 2000. The contents of this provisional patent application is hereby incorporated by reference.

BACKGROUND OF THE INVENTION:

Field of the Invention:

The invention relates to the field of secure credit card transactions over networks such as the internet.

Description of the Related Art:

The significant growth in electronic commerce has resulted in a significant increase in the amount of credit card transactions which are performed over networks such as the internet. Any credit card transaction requires complete details relating to the credit card to be transmitted over the internet, to a selected vendor. The information includes the credit card account number and the expiration date, which is all of the information necessary to put charges on the card holder's account. Once the credit card information has been obtained by the vendor, there is currently no way to prevent the vendor from improperly duplicating the credit card information, and/or placing improper charges on the cardholder's account. The same problem exists in the event that an unscrupulous third party electronically eavesdrops on either the transmission of the credit card information, or the information residing on the vendor's server, therefor obtaining information necessary to place invalid or fraudulent charges on the cardholder's account. Although encryption technology can make it more difficult for any one other than the intended vendor to read the information, once the information is stored on the vendor's computer, the information is available and readable in a non-encrypted form. Employees, consultants, or other individuals could access the information and use it for improper purposes. Also, encryption technologies can be defeated. Furthermore, vendors can, once they have the appropriate credit card information, add additional charges onto the cardholder's account without explicit authorization. While these types of unauthorized charges have some protections under consumer protection laws in the United States, other jurisdictions do not offer these protections. Additionally, it is always the responsibility of the cardholder to properly identify and dispute any improper charges.

SUMMARY OF THE INVENTION:

The invention, therefore, is directed to a method of providing secure credit card transactions, comprising the steps of providing first credit card account information to a card holder. The credit card account information includes a predetermined account field, and a changeable account field. The changeable account field contains changeable account information which is changeable by the card holder. An authorization request is received by a credit card issuer from a vendor; the authorization request includes second credit card account information. Charges to the credit card account are authorized only when the second credit card account information provided by the vendor matches the first credit card account information, including the changeable account information in the changeable account field.

The invention also comprises a system for providing credit card security, with the system comprising a network for interconnecting a plurality of computing devices, and a user terminal connected to the network. The user terminal provides a user interface between a user and the network. A credit card issuer unit is connected to the network, and contains credit card account records and data, and a user programmable code field for each credit card account record. A vendor terminal is connected to the network, with the vendor terminal configured to send and receive authorization data regarding selected credit card accounts. The user, through the user terminal, can selectively access the credit card issuer unit and modify the user programmable code field of a selected account. The credit card issuer terminal will only provide authorization data to the vendor terminal if information submitted by the vendor terminal matches a current user programmable code in the user programmable code field.

BRIEF DESCRIPTION OF THE DRAWINGS:

Figure 1 illustrates a configuration of a network according to the present invention;

Figure 2 illustrates a credit card number code sequence according to the present invention; and

Figure 3 is a block diagram of a security system according to the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS:

The present invention is intended to minimize the risk of unauthorized charges being placed on a credit card account by online vendors, or parties who may have access to credit card information on the servers for vendor's web sites.

Referring to Figure 1, a simplified system diagram is provided which illustrates cardholder terminal 1, in communication with a network such as internet 2. Also in communication with network 2 is a card issuer server 3, and a vendor server 4. Cardholder terminal 1 can be a personal computer or internet terminal of a known type, and card issuer server 3 and vendor server 4 are network servers. According to the invention, when the card issuer, which is typically a bank, credit company, or other type of entity creates a credit card for a cardholder, an additional code is used in order to enable the cardholder to limit or control the validity of an account. This enables transactions to be controlled, by enabling the credit cardholder to change authorization codes of the card at will. When the card issuer issues the card, therefore, the typical credit card includes an account number and an expiration date. According to the invention, however, the card issuer would add additional codes to the credit card account company. These additional codes can be changed by the cardholder, in order to essentially invalidate the code information which had previously been provided to a vendor. Assume, for example, the added code for a particular credit card were ABC123, and this information had been provided to a vendor for charges. Until this code is changed, the account number, expiration date, and this specific combination of added code would be necessary in order to put charges on the particular credit card account. By accessing the particular account information at the card issuer's server, the cardholder could change this code, thereby making it impossible for that particular vendor to add additional charges to the card, and also make it impossible for anyone having stolen or misappropriated the credit card number to make any additional charges on the account. ABC123 could be changed, for example, to DEF999, thereby invalidating ABC123.

If a cardholder sought to change the added code to his credit card account, he would log on to network 2 via cardholder terminal 1. Logging on to the network would include appropriate network access through an internet service provider in the case of the internet, or other necessary server. He would then access card issuer server 3 using an appropriate password, using encryption, or other secure communication method if available, and access the added code portion of his credit card number. The added code could be changed within any parameters which have been predetermined by the credit card issuer, and the cardholder would receive instant confirmation of the new code over the network 2. Then, when the cardholder sought to make purchases from vendor 4, he would access vendor server 4 through network 2, and make appropriate purchases using the newly activated added code. The vendor, through server 4, would be able to virtually instantaneously receive authorization for the charges, at which point the cardholder would be free to once again access card issuer server 3, to change the added code. This provides users a significantly higher level of control with respect to credit card actions, and also allow instantaneous ability to essentially deactivate the card in the event that the card is lost or stolen.

Figure 3 illustrates a flow chart of how a credit card or account would be created according to the invention. In step 31, a credit card or account is created, wherein a permanent account number is assigned. An expiration date is assigned to the credit card, and the added code field is either left blank, or a default code is placed therein. At step 32, a user accesses card issuer server 3 from card holder terminal 1, and selects a new code, thereby invalidating the previous added code, if desired. It should be noted that it is not necessary to invalidate the previous code. At step 33, a transaction occurs, and a vendor, whom has been given the credit card information and the added code information, will attempt to receive charge authorization from card issuer server 3. If the added code information which the vendor has does not match the currently selected or currently valid added code information, authorization will not be provided, and no charges will therefore be authorized.

It should be noted that the examples of account number, expiration date, and added code are submitted as examples only, as is the network configuration of Figure 1. The invention would work with virtually any combination of letters, numbers, symbols, or other characters for the credit card information and added code, and would also work with any communication method, including telephone access, wireless communication, etc.

CLAIMS:

1. A method of providing secure credit card transactions, said method comprising the steps of:

providing first credit card account information to a card holder, said credit card account information including a predetermined account field, and a changeable account field, said changeable account field containing changeable account information being changeable by the card holder;

receiving an authorization request from a vendor, said authorization request including second credit card account information;

authorizing charges to said credit card account only when said second credit card account information provided by the vendor matches the first credit card account information, including changeable account information.

2. A method as recited in claim 1, further comprising a step of changing said changeable account information in said changeable account field, wherein when the authorization request from the vendor includes changeable account information which does not correspond to current changeable account information, the authorization request is denied.

3. A method as recited in claim 1, wherein said authorization request from the vendor, and the authorization of charges, are sent over a computer network.

4. A method as recited in claim 2, wherein said step of changing the changeable account information is performed by accessing a credit card issuer server from a user terminal on a computer network.

5. A method as recited in claim 4, wherein said step of accessing the credit card issuer server comprises the step of logging in to a credit card issuer database on the credit card issuer server, then modifying the changeable account information in a database record containing the first credit card account information.

6. A system for providing credit card security, said system comprising:

a network for interconnecting a plurality of computing devices;

a user terminal connected to said network, said user terminal providing a user interface between a user and the network;

a credit card issuer unit connected to said network, said credit card issuer unit containing credit card account records and data, and a user programmable code field therein for each credit card account record;

a vendor terminal connected to said network, said vendor terminal configured to send and receive authorization data regarding selected credit card accounts;

wherein the user, through the user terminal, can selectively access the credit card issuer unit and modify the user programmable code field of a selected account, and wherein the credit card issuer terminal will only provide authorization data to the vendor terminal if information submitted by the vendor terminal matches a current user programmable code in the user programmable code field.

7. A system as recited in claim 6, wherein said network comprises the internet.

8. A system as recited in claim 6, wherein said credit card issuer unit contains a login unit to ensure that only an authorized user can access and modify the user programmable code field for a predetermined credit card account record.

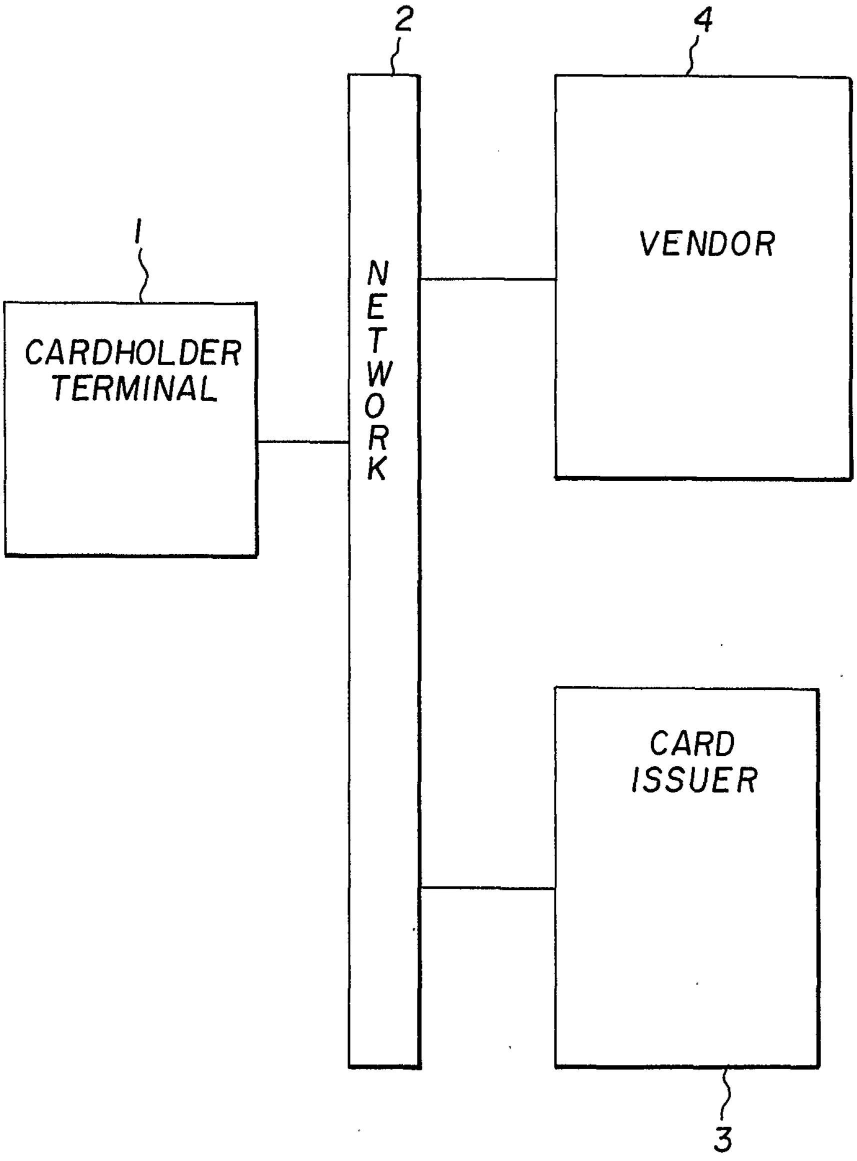


Fig. 1

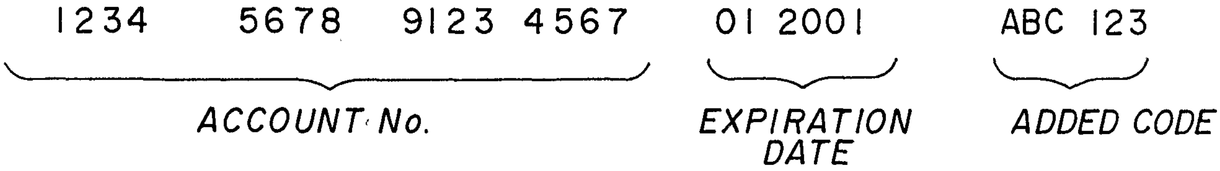

1234 5678 9123 4567
01 2001
ABC 123
ACCOUNT No.
EXPIRATION DATE
ADDED CODE

Fig. 2

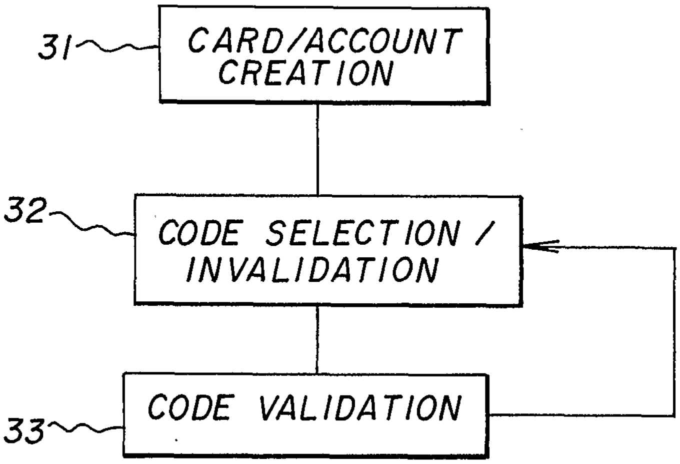

31
CARD/ACCOUNT CREATION
32
CODE SELECTION / INVALIDATION
33
CODE VALIDATION

Fig. 3

INTERNATIONAL SEARCH REPORT

Inter al Application No
PCT/IB 01/00014

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	US 6 000 832 A (D.C. FRANKLIN) 14 December 1999 (1999-12-14) the whole document	1-6,8 7
Y	US 5 239 583 A (L.A. PARILLO) 24 August 1993 (1993-08-24) abstract; figures column 3, line 50 -column 5, line 33	1-6,8
A	US 5 956 699 A (J.Y. WONG) 21 September 1999 (1999-09-21) the whole document	1-8
A	US 5 267 149 A (N. ANADA) 30 November 1993 (1993-11-30) abstract; figures 7,8 column 6, line 33 -column 8, line 23	1,4-6,8
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 31 May 2001	Date of mailing of the international search report 07/06/2001
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Authorized officer David, J

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 883 810 A (D.C. FRANKLIN) 16 March 1999 (1999-03-16) ---	
A	US 5 132 521 A (C.M. SMITH) 21 July 1992 (1992-07-21) -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern al Application No

PCT/IB 01/00014

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6000832 A	14-12-1999	NONE	
US 5239583 A	24-08-1993	WO 9428659 A	08-12-1994
		AU 1313195 A	18-04-1995
US 5956699 A	21-09-1999	US 5913203 A	15-06-1999
		AU 4255597 A	24-04-1998
		EP 1005682 A	07-06-2000
		WO 9814900 A	09-04-1998
		US 5937394 A	10-08-1999
US 5267149 A	30-11-1993	JP 63174172 A	18-07-1988
		JP 63178381 A	22-07-1988
		JP 63049971 A	02-03-1988
		KR 9105350 B	25-07-1991
US 5883810 A	16-03-1999	NONE	
US 5132521 A	21-07-1992	NONE	