PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 17/60 — A1

(11) International Publication Number: WO 00/46724

(43) International Publication Date: 10 August 2000 (10.08.00)

(21) International Application Number: PCT/US00/02935

(22) International Filing Date: 3 February 2000 (03.02.00)

(30) Priority Data:
09/246,019 5 February 1999 (05.02.99) US

(71) Applicant: FUNDSXPRESS, INC. [US/US]; 11950 Jollyville Road, Austin, TX 78759–2309 (US).

(72) Inventors: BURNS, John, A.; 6505 Danwood Drive, Austin, TX 78759 (US). ROCKENBAUGH, Zane, T.; 908 Philco Drive, Austin, TX 78681 (US). ARAMIL, Linda, Scott; 1603 Scenic Loop, Round Rock, TX 78081 (US). BLUMENTHAL, David, S.; 808 Jessie Street, Austin, TX 78704 (US).

(74) Agent: CAYWOOD, Michael; Locke Liddell & Sapp LLP, Suite 300, 100 Congress Avenue, Austin, TX 78701 (US).

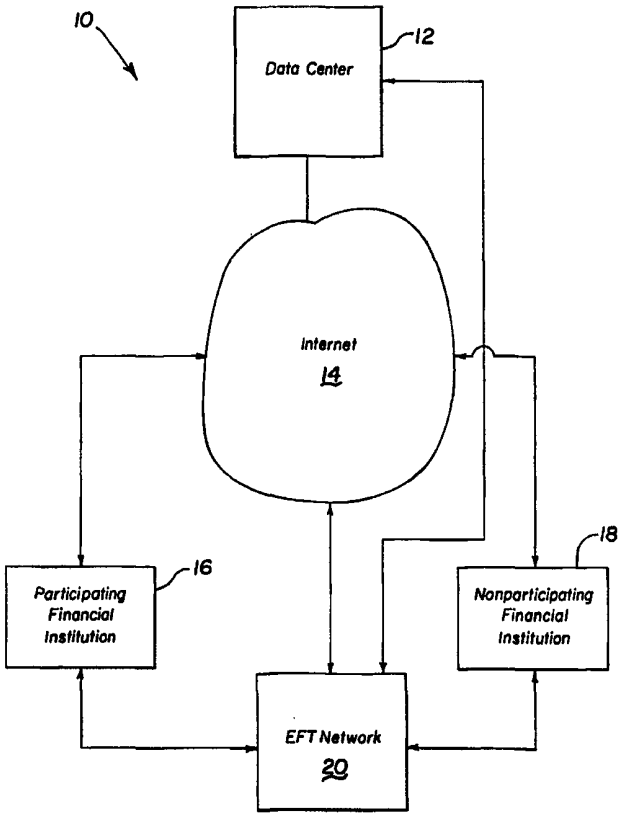
(81) Designated States: AU, CA, JP, MX, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD FOR AUTHORIZING ACCESS TO A SECURE ONLINE FINANCIAL TRANSACTION SYSTEM

(57) Abstract

A method for receiving and approving requests from customers to access a secure online system (10). First, a communication link is established between a user and the online system (10) over a communications network (14) in a secure session. Necessary user information is then gathered over the network (14) and an access ID and password are chosen by the user. The gathered information is stored in the system (10) along with the chosen access ID and password. Next, the stored user information is accessed and evaluated, and approval for access to the system (10) is granted to the user if certain criteria are met.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD FOR AUTHORIZING ACCESS TO A SECURE ONLINE FINANCIAL TRANSACTION SYSTEM

TECHNICAL FIELD

This invention relates to a method for registering customers to use a secure online financial transaction system, and more particularly to an online sign up process for customers of participating financial institutions.

BACKGROUND OF THE INVENTION

Until recently, bank and other financial institutions offered limited online banking capabilities to a small percentage of their banking customers from the customer's computer through proprietary dial up systems. Such proprietary systems gave the customer the ability to conduct basic financial transactions, such as account balance inquiry, transfer of funds between accounts and electronic bill payment, without the assistance of a teller. With the rapid growth in popularity of the Internet, it has become almost a necessity for large banks and other large financial institutions to be able to offer their customers these services through the Internet. These online banking systems permit the bank customer to perform financial transactions at the customer's convenience rather than during normal banking hours. As more and more financial institutions offer such services to their customers, there is increased pressure on small financial institutions such as, for example, community banks, not currently offering online banking services to add them in order to compete effectively in the marketplace. The effort to create a custom online banking system from the ground up is enormous and quite costly, and this effort has prevented many small and medium size financial institutions from being able to offer online banking services to their customers. Furthermore, many banks that would like to offer online banking services to their customers do not currently have a web site set up on the Internet to allow their customers access to online banking. In addition, electronic fund transfer (EFT) systems presently provide limited banking services through automated teller machines ("ATM"s) and point-of-sale ("POS") terminals for participating bank customers holding ATM debit cards. Such ATM cardholders could potentially use an online banking system if one were made available to them. If an online banking system that took advantage of the existing EFT networks to process online financial transactions were in place, there exists a related problem of managing secure access to the online banking system by all interested banking and EFT network users.

Employees in the customer service department of a bank that offers either dial-up or Internet-based online banking to its customers typically have to process a paper application completed by each customer desiring access to the online banking system. The amount of time that passes from when the customer fills out the application until approval to use the online banking system is granted can vary widely and is dependent on many factors. A customer can typically expect to wait several days before being able to access the online banking system, and for banks with many requests, this waiting time can be significantly higher. Further, financial institutions incur the labor costs of hiring and training mailroom and customer service personnel to handle these requests and the attendant phone calls from customers. Some existing systems have tried to reduce the turn-around time by enabling customers to request access to the online banking system via email. However, the bank customer service department still has to review and verify the information submitted in the email application, issue an access ID and a password, and send this information to the customer through regular mail before access can be granted.

Besides the labor cost, an obvious disadvantage of the existing online banking systems described above is that each customer's access ID and password are disclosed to customer service personnel from the time these codes are assigned until the customer receives them and can change the password on the online banking system. There is also a risk of fraud caused by sending the access ID and password to the customer through the mail. Even requiring customers to change their password the first time they log on to the system does not completely eliminate the possibility of access to the customer's accounts by an unscrupulous individual. The authorization process would greatly benefit from automated procedures granting access to the online banking system in a secure manner especially when dealing with large numbers of banking customers and EFT network cardholders.

SUMMARY OF THE INVENTION

The method of the present invention reduces the complexity, implementation time and related cost typically associated with approving and managing access to an online system, such as a financial transaction system, in a secure manner to a large number of potential system users. The method consists of establishing a communication link between a user and the online system over a network in a secure session, gathering necessary user information over the network,

assigning an access ID and password to the user, storing the gathered information along with the access ID and password in the system, accessing the stored information, and approving user access to the system based on an evaluation of the stored information.

The present invention has the added advantage of being designed so that existing financial institution customers can rely on the security and dependability of the method for accurately authorizing access to the online system. Thus, the invention provides a simple way to manage many access requests to a secure online system by institution customers while maintaining the security needed for granting such access.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows the major components in the present secure online system.

FIGS. 2A and 2B are flowcharts depicting the steps for accepting and authorizing customer requests to access the system of FIG. 1.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention is directed to a method for quickly and securely granting access to a secure online banking system for an untold number of banking customers who are existing customers of a financial institution and who want to access their accounts through the online banking system 10 shown in Fig. 1.

One of the significant features of the present invention is its ability to increase the automation of processing requests for access to an online system, such as a financial transaction system. Fig. 1 shows a representative online banking system 10 in which the current invention can be used. System 10 includes a data center 12. Physical access to the system 10 is typically accomplished through the Internet 14 by customers of a participating financial institution 16. While most requesting customers may belong to a financial institution 16 that has contracted to participate in the online banking system 10 shown and has authorized their banking customers to use the system, some potential customers will belong to non-participating financial institutions 18, and such requesting customers may try and access the system 10 through the Internet sites operated by their EFT network 20 or by the data center 12 itself.

Figs. 2A and 2B are a flowchart of the steps in the operation of the present invention to receive and approve customer requests for authorization to access the online banking system 10. The method of the present invention begins when a user 40 accesses the user's financial institution's or EFT network's web site by pointing a browser to the appropriate web site at step 42. Typically, the user 40 will be presented with a number of options for proceeding at step 44. At step 46, if user 40 has been previously authorized to use the online banking system 10, user 40 may securely log into the site using a previously assigned access ID and password and proceed with an online banking transaction at step 48. If user 40 is not yet authorized to use the system, user 40 may select at step 50 an option such as "Enroll now" to request approval. In one embodiment of the present invention, an unauthorized user requesting new access to the system uses an ATM or debit card issued by a financial institution in order to request approval to access the system 10. At step 50, the user may decide to enroll online, or the user may print out an application, filling out and submitting the application through the mail.

If continuing with online enrollment, at step 52 the user enters a secure session within the system 10 before being prompted to enter the first ten digits of the user's debit card. In the preferred embodiment, the secure session is created over the Internet through a Secure Socket Layer (SSL) encrypted session although other encryption methods known in the art may be used. The first ten digits of the debit card are referred to as the Bank Identification Number (BIN) and uniquely identify the financial institution that issued the debit card to the user. If the user does not have a debit card, the user must enter an identifier that allows the system to uniquely identify a financial institution. Assuming a BIN identifier is entered, at step 58 the system will verify that the identifier is valid and decode the identifier to determine the issuing financial institution. In the preferred embodiment, this verification is done through a BIN look-up table maintained by the system 10 although any other decode methods may be used.

If the number is not a valid financial institution identifier, the system 10 will reject the number and may or may not permit the user to try and enter the correct number again. If a valid identifier is entered, the system 10 displays a confirmation page to the user containing information regarding the financial institution name and other identifying information for verification by the user that the correct financial institution has been found. At step 58, the system 10 also checks to

see whether the user's financial institution participates in the system 10 and whether the bank's users can be enrolled online. Participation may result from a contract between an individual financial institution and the system operator, or between an EFT network and the operator of system 10. Either way, all customers of the individual financial institution as well as those customers who use the EFT network can receive authorization to use the system 10 through the online sign-up process of the present invention.

If the user's financial institution is not a pre-existing participant in the system 10, then the user is notified at step 60 that the user is currently unable to bank online using the system 10. In addition, the system 10 may generate various emails or other correspondence at step 60. In particular, e-mail correspondence may be sent to the financial institution informing it of the request for online banking by one of its customers. Likewise, the marketing department of the nearest EFT network may be notified so that it can target the bank to encourage the bank to sign up with the EFT network and thereby be able to offer online banking to its customers. The system may even prompt the user to enter his full name at step 62. If the user's name is provided, it may be used at step 64 in the correspondence described above or in an email to the EFT network's marketing department. The EFT network can then send an email containing the customer's name directly to the customer's financial institution so the financial institution can contact that user once access to the system 10 becomes available.

Returning to step 58, if the user's financial institution participates in the system 10 and the user has confirmed that the bank found based on the entered BIN is the user's bank, the user is presented with a detailed customer information page at step 66 where necessary information is filled in and verified by the system 10. In particular, data such as the additional numbers of the user's debit card number, and the user's name, address and e-mail address may be entered. At this point in the process, the user also specifies by account number the particular accounts the user wants to use within the online banking system 10. Next, the user is presented with a security information entry page wherein the user chooses an access ID, password, and any other security information needed by the user's financial institution. Such additional information may consist of a validation question and secret answer, user's mother's maiden name, or other user unique data. The security information is used by customer service at the user's financial institution to identify

the customer over the telephone if the user should call in with a problem. Once an access ID and password are chosen, the system 10 at step 68 will ensure that the access ID is not already in use by another user. If the access ID is already in use, the system 10 will prompt the user to enter another access ID at step 70. Once a unique access ID is found, the user is presented with a page summarizing all of the information the user entered for verification purposes. This page may also contain other relevant information for the user such as a link to a disclosure page or a signature line. Once the information is verified, the user submits the application at step 72. The system 10 then informs the user through a confirmation page that the user will be notified once the application is approved. Due to the automated nature of the method, the approval process proceeds without any employees of the financial institution or the operators of the system 10 ever seeing the access ID and password combination submitted by each customer.

At this point, the system 10 takes over further processing of the application. As shown in Fig. 2B, the customer's application information is stored within the system 10, and the access ID is reserved across the financial institution and all other financial institutions belonging to that EFT network at step 74. In the preferred embodiment, the application information is stored in a relational database system, such as one licensed by Oracle, used by the system 10. Employees of the financial institution who have the proper authorization can access information stored in new user applications over a secure connection to the system 10. Personnel responsible for reviewing and approving such applications for access to the online system 10 verify the information contained in the application at step 76. Certain financial institutions may choose to add an additional level of security to the process by confirming with the customer via e-mail, a telephone call, or other contact that the user has indeed requested access to the online banking system, thereby implementing the "Know Your Customer" rule requirement of Regulation E of the Board of Governors of the Federal Reserve System. If additional information is needed, the employee can investigate the request further or deny the application at step 78. If everything appears in order, the employee approves the request and authorizes the customer to use the online banking system 10 at step 80, and confirmation is sent to the customer via regular mail.

Thus, it can be seen that the present invention expedites the process of authorizing customers to use an online banking system 10. In fact, the process may be generalized to a variety of

circumstances where a vendor or financial institution needs to authenticate and authorize an applicant before being able to grant access to confidential information over the Internet to that applicant. For example, access to online brokerage or insurance systems could also be authorized using the described method. The method may also be broadened to users without a debit card. This can be done by substituting a credit card number, information from a check (bank routing number and customer account number), or bank routing and transit numbers.

It is intended that the description of the preferred embodiment of the present invention is but one embodiment for implementing the invention. Variations in the description likely to be conceived of by those skilled in the art still fall within the breadth and scope of the disclosure of the present invention. While specific alternatives to components of the invention have been described herein, additional alternatives not specifically disclosed but known in the art are intended to fall within the scope of the invention. It is understood that other applications of the present invention will be apparent to those skilled in the art upon the reading of the preferred embodiment and a consideration of the appended claims and drawings.

We claim:

1. A method for granting approval to access user financial information, maintained by an institution, through a secure online system, the method comprising:

establishing a communications link between the user and the online system over a network in a secure session wherein the online system includes information about the institution;

gathering necessary user information over the network;

assigning an access ID and password to the user;

storing the gathered information along with the access ID and password in the online system;

accessing the stored information;

evaluating the stored information; and

approving user access to the online system based on the evaluation of the stored information.

2. The method of claim 1 wherein the assigning an access ID and password is based on an access ID and password chosen by the user.

3. The method of claim 1 wherein evaluating the stored information is performed by the institution.

4. The method of claim 1 further comprising confirming access to the system with the user after the approval step.

5. The method of claim 1 wherein the online system is a financial transaction system.

6. The method of claim 5 further comprising:
entering a financial institution identifier to select a single financial institution; and
verifying that the selected financial institution participates in the system.

7. The method of claim 6 wherein accessing stored information occurs via a secure session.

8. The method of claim 7 wherein establishing the communications link includes pointing a web browser to an appropriate web site.

9. The method of claim 7 wherein the financial institution identifier is a BIN.

10. The method of claim 7 wherein the financial institution identifier is obtained from a debit card.

11. The method of claim 7 wherein the financial institution identifier is obtained from a credit card number.

12. The method of claim 7 wherein the financial institution identifier is a bank routing number.

13. The method of claim 7 wherein the secure sessions are created over the Internet through a Secure Socket Layer (SSL) session.

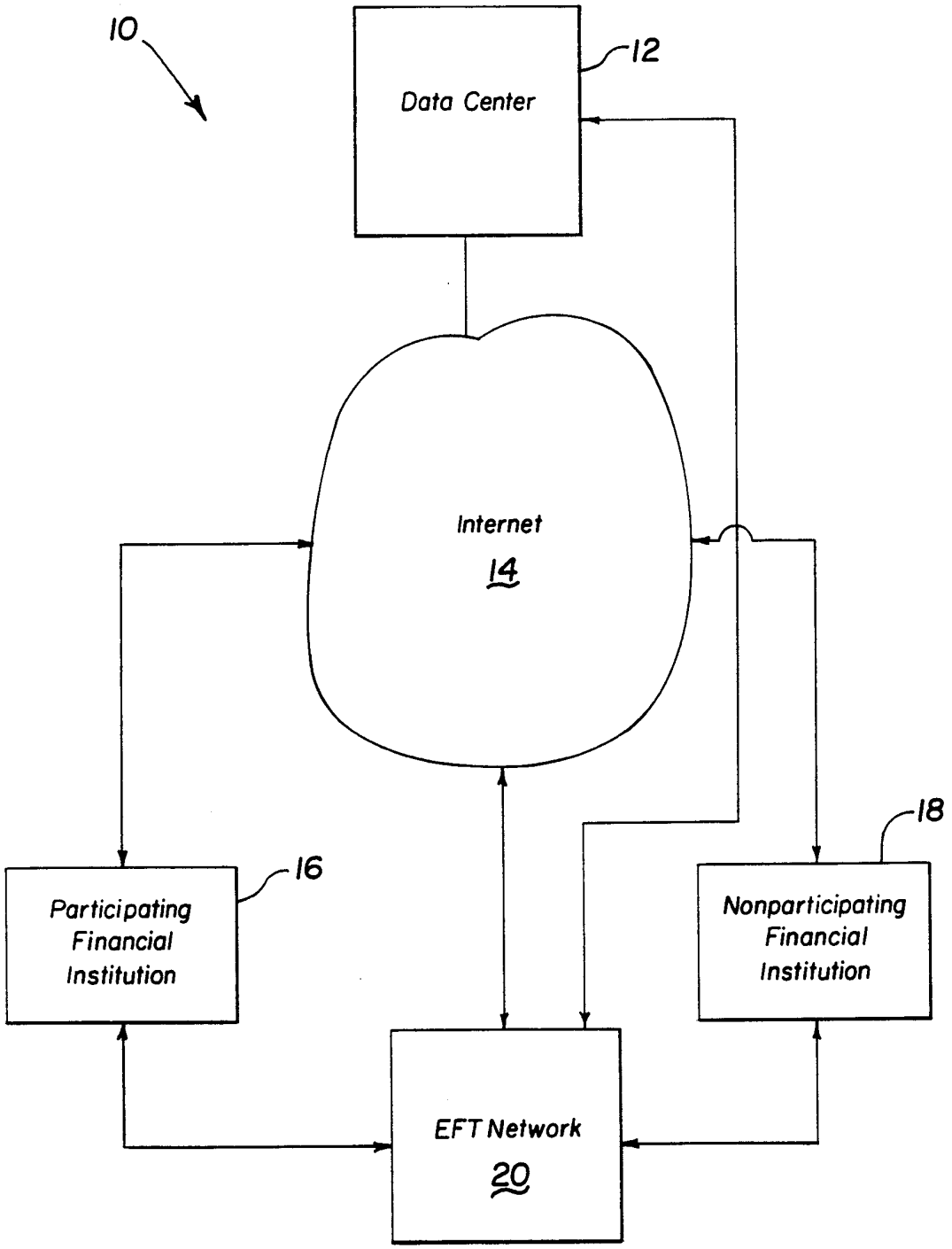

10
Data Center
12
Internet
14
Participating Financial Institution
16
Nonparticipating Financial Institution
18
EFT Network
20

Fig. 1

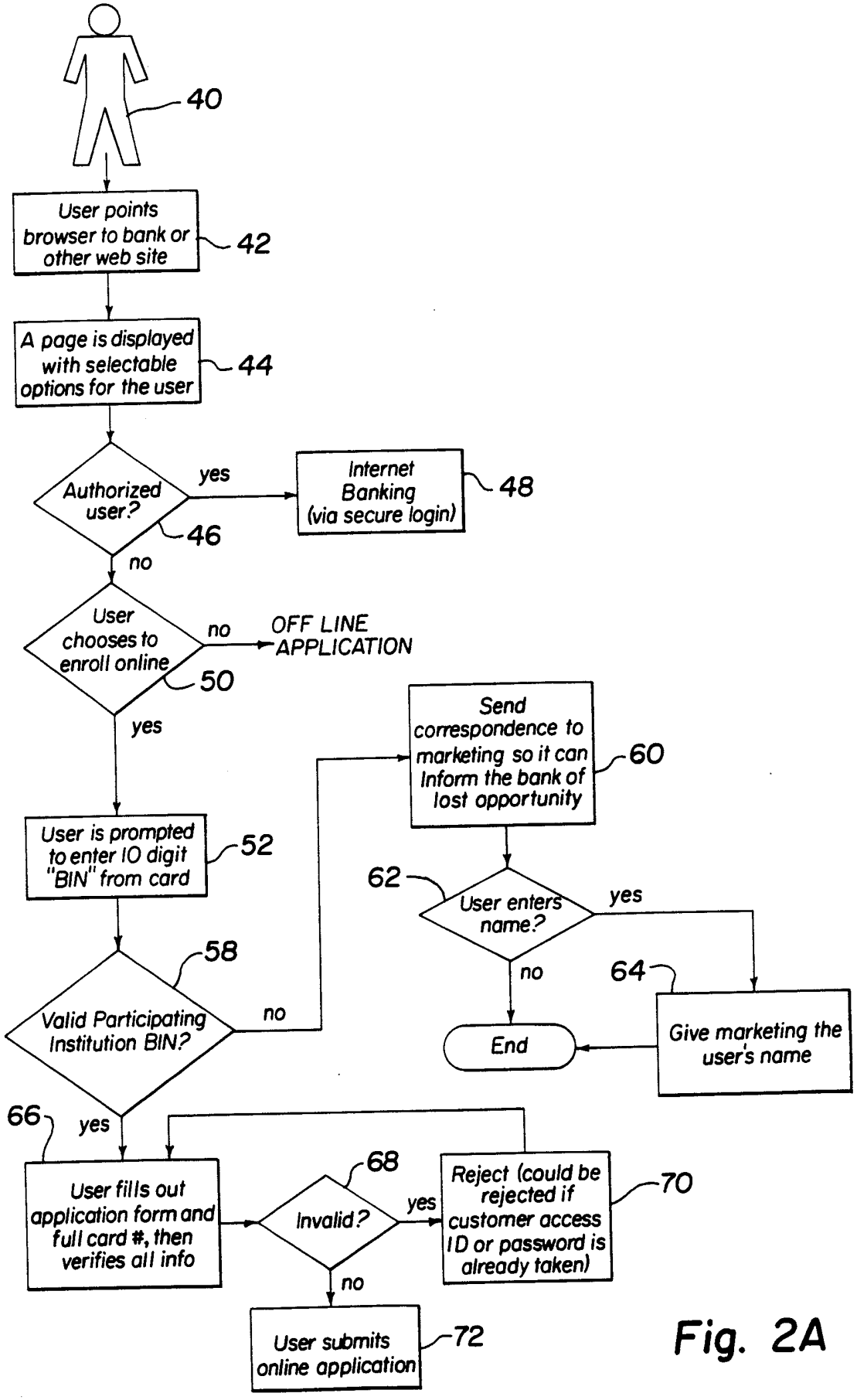

40
User points browser to bank or other web site
42
A page is displayed with selectable options for the user
44
Authorized user?
yes
Internet Banking (via secure login)
48
46
no
User chooses to enroll online
no
OFF LINE APPLICATION
50
yes
User is prompted to enter 10 digit "BIN" from card
52
Send correspondence to marketing so it can inform the bank of lost opportunity
60
62
User enters name?
yes
no
64
Give marketing the user's name
End
58
Valid Participating Institution BIN?
no
66
yes
User fills out application form and full card #, then verifies all info
68
Invalid?
yes
Reject (could be rejected if customer access ID or password is already taken)
70
no
User submits online application
72

Fig. 2A

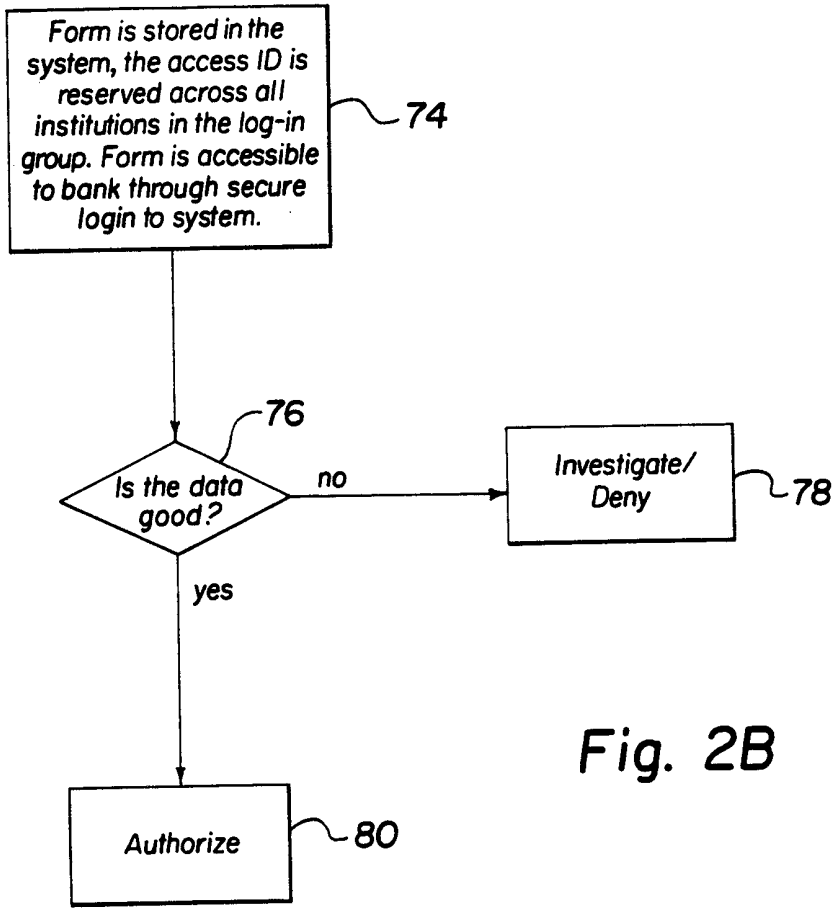

Form is stored in the system, the access ID is reserved across all institutions in the log-in group. Form is accessible to bank through secure login to system.
74
76
Is the data good?
no
Investigate/ Deny
78
yes
Authorize
80

Fig. 2B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/ US00/02935

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/60
US CL : 705/44

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)
U.S. : 705/44

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 practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P	US 5,987,440 A (O'NEIL et al) 16 November 1999 (19.11.1999), column 4, lines 25-29;	1, 3-4
---	column 5, lines 26-31; column 7, lines 53-67; column 8, lines 1-6, 27-31; and column 10,	---------
Y	lines 17-44.	2-13
Y, P	US 5,870,725 A (BELLINGER et al) 09 February 1999 (09.02.1999), column 27, lines 32-47.	2-4
Y	US 5,794,230 A (HORADAN et al) 11 August 1998 (11.08.1998), column 2, lines 1-22; column 3, lines 15-27 and column 8, lines 13-25.	5-13
A	US 5,276,444 A (McNAIR) 04 January 1994 (04.01.1994), entire document	1-13
A	US 5,751,812 A (ANDERSON) 12 May 1998 (12.05.1998), entire document.	1-13
A, P	US 5,890,140 A (CLARK et al) 30 March 1999 (30.03.1999), entire document.	1-13
A, P	US 5,971,272 A (HSIAO) 26 October 1999 (26.10.1999), entire document.	1-13
A, E	US 6,023,684 A (PEARSON) 08 February 2000 (08.02.2000), entire document.	1-13

☐ Further documents are listed in the continuation of Box C. ☐ See patent family 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 application or patent 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
13 April 2000 (13.04.2000)

Date of mailing of the international search report
30 MAY 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703)305-3230

Authorized officer
James P. Trammell

Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)