PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	2013-08-23
First Named Inventor	Gerry Calabrese et al.
Art Unit	N/A
Examiner Name	N/A
Attorney Docket Number	W-9001D3

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5221838		1993-06-22	Gutman et al.	
	2	5359182		1994-10-25	Schilling	
	3	5521363		1996-05-28	Tannenbaum	
	4	6366893	B2	2002-04-02	Hannula et al.	
	5	6442532	B1	2002-08-27	Kawan	
	6	6494367	B1	2002-12-17	Zacharias	
	7	6726098	B2	2004-04-27	Schilling	
	8	6754636	B1	2004-06-22	Walker et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	W-9001D3

	9	7024396	B2	2006-04-04	Woodward	
	10	7181432	B2	2007-02-20	Wells et al.	
	11	5530438	A	1996-06-25	Bickham et al.	
	12	5615110	A	1997-03-25	Wong	
	13	6064990	A	2000-05-16	Goldsmith	
	14	7096003	B2	2006-08-22	Joao et al.	
	15	7389275	B2	2008-06-17	Kemper et al.	
	16	5708422	A	1998-01-13	Blonder et al.	Corresponds to EP 0745961 A2
	17	5903830	A	1999-05-11	Joao et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	W-9001D3

	1	20020035539	A1	2002-03-21	O'Connell	
	2	20020107755	A1	2002-08-08	Steed et al.	
	3	20020107791	A1	2002-08-08	Nobrega et al.	
	4	20020156689	A1	2002-10-24	Spalding	
	5	20030221125	A1	2003-11-27	Rolfe	
	6	20070027803	A1	2007-02-01	Brandes et al.	Corresponds to EP 1136961 A1

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1136961	EP	A1	2001-09-26	Calvo et al.	Published in the English language and corresponds to US 20070027803 A1	☐
	2	0745961	EP	A2	1996-12-04	Blonder et al.	Published in the English language and corresponds to US 5708422 A	☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	
	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	W-9001D3

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Petitioner Askeladden LLC
Exhibit 1002 - Page 4 of 350

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	
	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	W-9001D3

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Werner H. Stemer/	Date (YYYY-MM-DD)	2013-08-23
Name/Print	Werner H. Stemer	Registration Number	34956

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Petitioner Askeladden LLC
Exhibit 1002 - Page 6 of 350

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 745 961 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
04.12.1996 Bulletin 1996/49

(51) Int Cl.[6]: **G07F 7/08**

(21) Application number: **96303616.5**

(22) Date of filing: **21.05.1996**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **31.05.1995 US 455939**

(71) Applicant: **AT&T IPM Corp.**
Coral Gables, Florida 33134 (US)

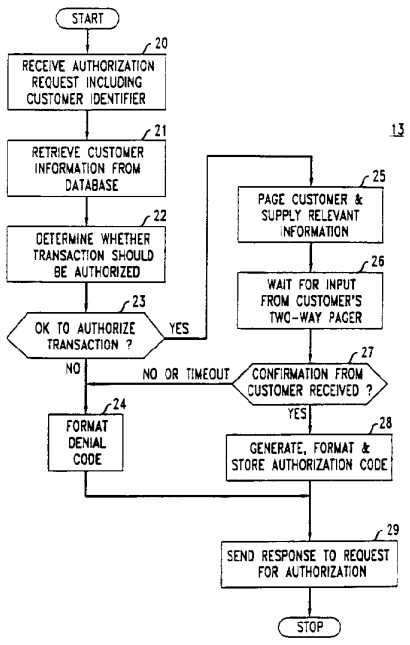
(72) Inventors:
- **Blonder, Greg E.**
  Summit, New Jersey 07901 (US)
- **Greenspan, Steven Lloyd**
  Scotch Plains, New Jersey 07076 (US)
- **Mirville, J. Robert**
  Manalapan, New Jersey 07726 (US)
- **Sugla, Binay**
  Aberdeen, New Jersey 07747 (US)

(74) Representative:
Buckley, Christopher Simon Thirsk et al
Lucent Technologies,
5 Mornington Road
Woodford Green, Essex IG8 0TU (GB)

(54) Transaction authorization and alert system

(57) An automated method for alerting a customer that a transaction is being initiated and for authorizing the transaction based on a confirmation/approval by the customer thereto. In accordance with one illustrative embodiment, a request to authorize the transaction is received, wherein the request includes a customer identifier; a determination is made whether to authorize the transaction based on the customer identifier; if the determination is to authorize the transaction, that fact is communicated to the customer; a confirmation that the transaction should, in fact, be authorized is received back from the customer; and the transaction is authorized in response to the customer's confirmation thereof. In accordance with another illustrative embodiment, a transaction initiated by an agent of the customer (*i.e.*, the principal) is authorized by the principal when one or more threshold parameters that may be pre-defined by the principal are exceeded. A preferred method of alerting the customer and receiving a confirmation to authorize the transaction back from the customer is illustratively afforded by conventional two-way pagers.

FIG. 10



EP 0 745 961 A2

Printed by Jouve, 75001 PARIS (FR)

Petitioner Askeladden LLC
Exhibit 1002 - Page 7 of 350

Description

Field of the Invention

This invention relates to a transaction authorization and alerting system, and more particularly to a method and apparatus for using a communications system to alert an interested party of a recently completed transaction and/or to obtain authorization from the interested party for a pending transaction.

Background of the Invention

The credit card identification numbers assigned to credit card customers are presented to many different people in a variety of circumstances -- when applying for financial services, when concluding purchases in a store, and when making purchases over the telephone, through the mail, or over e-mail (electronic mail). The large number of people that have access to a customer's credit card number has frequently led to fraud. The advantages of using credit cards, however, are substantiaL The customer finds their use advantageous in that he or she need not carry cash or write checks. Credit card purchases also have advantages to the retailer as compared, for example, to payment by check, since the credit card service provider ensures timely payment to the retailer, regardless of when the customer pays the balance on the credit card account. However, credit cards or credit card numbers are often stolen, and credit card numbers are often used over the telephone or through the mail without any secure mechanism for confirming the customer's identity.

Telephone calling card numbers have security problems similar to those of credit cards. These numbers are often spoken aloud or entered through a touch tone keypad, thereby allowing others the opportunity to record them (either electronically or by mere observation), and to then fraudulently use the numbers. Another common source of fraud sterns from authorized usage of a credit card or a telephone calling card followed by a customer denial that he or she made the purchase or placed the call. Thus, simply controlling access to the credit or calling card number without more may be inadequate. Computer access to secure databases is yet another example of a transaction that depends upon private customer identifiers *(i.e.,* passwords) which through legal or illegal channels may become known to others, thereby allowing unauthorized access to these databases.

Prior art mechanisms for handling such security concerns have not taken advantage of advances in communications and computer systems to automate the alerting and approval process. Most techniques which have heretofore attempted to address these security issues tend to significantly increase the complexity of the communication protocol. For example, the customer may be asked additional questions (the answers to which it is expected that only the authorized party would know), or may be required to provide additional information as a part of each transaction such as a (secret) Personal Identification Number (PIN). Moreover, it may be required that such PINs be modified on a routine basis in order to maintain their secrecy. To encourage customers to make use of these types of services *(e.g.,* credit and calling cards), it has become common to limit the liability of the customer while increasing the liability of the service provider *(e.g.,* the credit card vendor or telephone company). Unfortunately, unauthorized uses usually go undetected until a periodic service report is issued -- typically, at the end of a monthly billing cycle and long after the fraud was perpetrated.

In addition to the above-described security issues, one commonly desired class of financial transactions involves a principal who empowers an agent to initiate and complete routine transactions without the principal's knowledge or approval. However, the principal often reserves the right to be alerted to, or even to approve, such transactions, particularly when they are identifiably non-routine or atypical. For example, approval may be required when certain threshold parameters that are associated with the transaction (which may, for example, be pre-defined by the principal) are exceeded.

Prior art mechanisms for handling such agent initiated transactions have also not taken advantage of advances in communications and computer systems to automate the alerting and approval process, thereby limiting the scope of applications of such transactions. For example, a card owner, such as a corporation (parent) that provides an employee (young adult) with a credit/debit card to charge business (personal) expenses, typically places certain restrictions on the use of the card by the cardholder to prevent abuses, excesses or fraud. Those restrictions include, for example, upper limits on either the total amount of money that can be charged to a commercial credit card, or the number of transactions that can be authorized for a credit card number within a predetermined period of time. Those restrictions sometimes operate to deny access to credit to a cardholder who is stranded or facing an emergency situation, when ironically credit is most needed. This clearly defeats the purpose of empowering the employee or young adult. Yet, oversight of the use of those credit cards by the card owners is still needed since the card owners are ultimately financially responsible for the expenses charged to those credit cards. This issue takes particular significance when one considers that merchants concerned about lack of legal competency of minors to complete card transactions have been reluctant to accept debit or credit cards as a means of payment from minors. Hence, another specific problem of the prior art is lack of a flexible restrictiun mechanism for principals to limit monitor, and/or approve use of a card by cardholder for non-routine commercial transactions.

Petitioner Askeladden LLC
Exhibit 1002 - Page 8 of 350

Summary of the Invention

We have recognized that the aforementioned problems result from the inability to quickly and efficiently inform the individual customer *(e.g.,* the account holder or the principal) that his or her customer identifier *(e.g.,* credit/debit/calling card number, PIN, password, *etc.*) is being used in a transaction for a particular purpose, and the inability of the customer to respond thereto in order to confirm or deny its use. Thus, in accordance with certain illustrative embodiments of the present invention, an automated method for authorizing a transaction is provided in which the customer is informed of a pending authorization thereof, and the transaction is then authorized only in response to a customer confirmation. In accordance with certain other illustrative embodiments, the invention provides a method and a system which allow a principal to be automatically alerted to, and/or to promptly authorize, an agent-initiated transaction which may, for example, be deemed atypical based on a pre-stored profile specified by the principal.

In accordance with one illustrative embodiment, a request to authorize a transaction is received, wherein the request includes a customer identifier; a determination is made whether to authorize the transaction based on the customer identifier; if the determination is made to authorize the transaction, the pending authorization is communicated to the customer; a confirmation that the transaction is, in fact, to be authorized is received back from the customer; and the transaction is authorized in response to the customer's confirmation thereof.

One approach to communicating such a determination to authorize the transaction and to receive such a confirmation to authorize from the customer is illustratively afforded by conventional two-way pagers. For example, a computer database, charged with the task of authorizing a transaction, may signal the customer via paging whenever his or her customer identifier is used. Along with this notification, relevant information may be displayed on the pager's alphanumeric (or numeric) display. The customer may then respond (via the two-way pager) by confirming or denying the pending authorization.

According to one aspect of the invention, exception conditions that trigger a customer's alerting or approval process may be stored in a profile specified by the customer. This profile associates those exception conditions to a personal communications address, such as a paging number or a "500" or "700" prefix telephone number at which the customer can be reached. For credit/debit and calling card transactions, exception conditions may be caused, for example, by a request for credit amount (or number of transactions) above threshold parameters pre-imposed by the card owner for the use of the card, or breach of other conditions pre-defined by the card owner for the use of the card. In accordance with the principles of the invention, the card owner may elect to simply receive the alert message or to authorize/deny the charging of the expenses to the card number by transmitting an approval/disapproval message to the card issuer as part of the card validation process.

According to another aspect of the invention, a merchant may request the approval of a parent or guardian to a debit/credit card transaction, such as a stored-value smartcard, presented to the merchant by a minor alleging to act on behalf of the parent or guardian. In that case, the card number, or a proxy thereof, may be used as a search key to retrieve the parent or guardian's profile that identifies a communications address for the parent or guardian. The transaction is approved only if an authorization message is received from the parent or guardian.

Brief Description of the Drawings

FIG. 1 is a telecommunication system arranged in accordance with the invention to allow a card owner to authorize, or to be alerted to transactions charged to the card by a cardholder.

FIG. 2 illustrates an exemplary message that is transmitted by an automatic dialing unit at a merchant's location to a card issuer's validation database.

FIG. 3 shows an illustrative table that associates alerting threshold parameters to card numbers.

FIG. 4 shows an illustrative generic message that is transmitted by an automatic dialing unit at a merchant's location to a card owner's communications device.

FIG. 5 shows specific exemplary messages that may be transmitted by a card validation system to a card owner's communications device.

FIG. 6 is a table that correlates merchant codes to types of commercial establishments.

FIG. 7 shows a flow diagram outlining illustrative programmed instructions executed by different elements of the communications system of FIG. 1 to receive approval for, or to alert a credit card owner to, a credit card transaction initiated by a card holder in accordance with certain illustrative embodiments of the present invention.

FIG. 8 is a flow chart of illustrative programmed instructions executed by various components of the communications system of FIG. 1 to receive approval from a parent or a guardian of a minor initiated debit card transaction in accordance with a first illustrative embodiment of the present invention.

FIG. 9 shows a flow chart of a credit card purchase transaction to which certain illustrative embodiments of the present invention may advantageously be applied.

FIG. 10 shows a flow chart of an authorization process in accordance with a second illustrative embodiment of the present invention.

FIG. 11 shows a flow chart of an authorization process in accordance with a third illustrative embodiment of the present invention.

Petitioner Askeladden LLC
Exhibit 1002 - Page 9 of 350

FIG. 12 shows a flow chart of an authorization process in accordance with a fourth illustrative embodiment of the present invention.

FIG. 13 shows a flow chart of a credit card purchase transaction to which a fifth illustrative embodiment of the present invention may advantageously be applied.

FIG. 14 shows a flow chart of an authorization process in accordance with a fifth illustrative embodiment of the present invention.

Detailed Description

Introduction

Although the principles of the present invention may be applied to many domains, the illustrative embodiments described in detail herein will focus on a credit card or debit card purchase transaction. In these embodiments, a cardholder, who may or may not be the customer of the credit or debit card issuer, uses a credit or debit card (or a credit card number) to instruct a retailer (a provider of a product or service) to charge a purchase to the given credit card account or to debit the amount of the purchase from the given debit card account. The credit or debit card number serves as a customer identifier to the credit card service provider *(e.g.,* the issuer of the credit card).

FIG. 1 shows a communications system arranged in accordance with certain illustrative embodiments of the present invention to implement the principles thereof. The communications system of FIG. 1 includes a communications network 102, a validation database 106 and a paging system network 111. Communications network 102 includes one or a series of interconnected communications switches arranged to relay to validation database 106 (via lines 130-1 to 130-N information received from card reader 101. Specifically, when a credit card holder hands a credit card to a merchant to charge expenses associated with a transaction, the merchant slides the credit card through card reader 101 to read the credit card number, for example, off the magnetic stripe on the back of the credit card. An automatic dialing unit included in card reader 101 dials a telephone number associated with a database 106 of the card issuer to validate the card number. In particular, card reader 101 transmits to validation database 106 a validation request message that is illustratively represented in FIG. 2.

Similarly, when the cardholder wishes to use a debit card such as an Automatic Teller Machine (ATM) card as a means of payment for a commercial transaction, the merchant enters a special code into card reader 101 to initiate the alerting and approval process. Thereafter, card reader 101 retrieves the debit card number, for example, from the magnetic stripe on the back of the debit card before prompting the cardholder for a secret code *(e.g.,* a PIN). Card reader 101 then transmits to validation database 101 a validation request message that is illustrated in FIG. 2.

The message shown in FIG. 2 includes a card number 201, a requested credit amount 202, a merchant code 203, and a validation request 204. When card number 201 is a debit card number, it also includes the PIN entered by the cardholder. Merchant code 203 is a field that identifies the type of business from which the message associated with the transaction, is transmitted. Typically, the merchant code 203 is appended by card reader 101 after the requested credit amount 202 has been entered by the merchant, and the calling card number 201 has been retrieved from the magnetic stripe on the back of the card. The validation request field 204 stores the code entered by a merchant to receive approval from the party authorized to give such approval for a debit card transaction. In the case where the cardholder is a minor, for example, by requesting approval of the transaction from a parent or guardian of the minor *(i.e.,* the authorized party), the merchant and the debit card issuer are assured that the transaction cannot be voided by the minor at a later date on the ground that the minor lacked legal competency to enter into such transaction.

Upon receiving a validation request message, validation database 106 uses card number 201 as a search key to perform a table look-up operation for the purpose of retrieving the profile associated with the card number. When the cardholder is a minor, and the card is a stored-value smartcard, a passphrase or proxy information provided by the minor may be used as search key to retrieve the profile of FIG. 3.

Validation database 106 is a processor-controlled centralized database facility which is a repository of records or profiles for all credit/debit card numbers assigned by a card issuer to its customers. Validation database 106 is designed to authorize transactions charged to card numbers stored therein. Such authorization may be based on a set of pre-defined parameters included in the profiles associated with the card numbers. When a retrieved profile does not include a requirement for alerting or approval, validation of the card number may be performed in a conventional manner. When a profile stores alerting parameters that may require communications with one or more called parties, validation database 106 uses one of the Automatic Dialing Units (ADU) II0-1 to 110-N to dial a telephone number retrieved from a profile associated with a card number.

Shown in FIG. 3 is an illustrative table that associates alerting and approval threshold parameters to credit card numbers. Each record in the table of FIG. 3 is a profile for a credit card number that is used to determine the manner in which transactions charged to that credit card number are processed. The table of FIG. 3 includes a cardholder's name field 301; a card number field 302; alert and authorization flags 303 and 304, respectively; a trigger group of fields; a communications address field 307; a no-answer-credit threshold field 309; and a no-

Petitioner Askeladden LLC
Exhibit 1002 - Page 10 of 350

answer-transaction threshold field 310. Cardholder's name field 301 stores the name of a card holder associated with a particular card number. The cardholder's name field may contain, for example, the first and last name of the cardholder (as shown for the first and third record) or the first name (or nickname) of the cardholder (as shown for the second and fourth record). Credit card number 302 is used as a search key in the table lookup operation mentioned above, to retrieve the profile associated with that card number. The alert flag field 303 indicates that the card owner is to be notified, although possibly only under certain conditions. Such notification may be required, for example, when processing of the transaction would either cause certain conditions predefined for the use of the card to be breached, or a threshold parameter to be exceeded. The approval flag field 304 alerts the card issuer that credit card transactions that violate pre-established conditions need to be authorized by the card owner as part of the card validation process. These pre-established conditions may be pre-selected by the card owner or they may be conditions imposed by the card issuer. The trigger group of fields depicted in FIG. 3 illustratively shows different parameters which cause a card owner to be notified when those parameters exceed certain pre-defined thresholds. The "conditions" field 305 shows restrictions preselected by the card owners for use of their credit cards. For example, the first record indicates that the card owner wishes to be alerted whenever a cardholder charges more than one hundred (100) dollars to the credit card number. The third record illustrates that the card owner wishes to authorize any credit card transaction for more than three hundred dollars. By contrast, the owner of the credit card number associated with the third record wishes to be alerted whenever that card is used at commercial establishments associated with specific merchant codes. Some card issuers assign distinct merchant codes to commercial establishments, such as bars, hotels and liquor stores, thereby allowing credit card transactions at those establishments to be easily identified.

Other restrictions that may be imposed by a card owner may include, for example, the "maximum number of transactions" field 306 which defines an upper limit on the number of transactions that can be charged to a credit card number within a predetermined period of time. For example, the second record indicates that the card owner's approval is required to validate a credit card transaction when more than three credit card transactions have already been processed for that credit card number within a twenty-four (24) hour period. Such a condition may be useful for example, in detecting fraudulent use of a stolen credit card. When a transaction threshold number is used as a parameter for processing a credit card transaction, the transaction counter field 307 is incremented by 1 (one) every time a credit card transaction is processed. The transaction counter field 307 is reset to "0" after the predetermined period *(e.g.,* 24 hours) has expired. It will be appreciated that only a limited number of restrictions and/or authorizations are shown in FIG. 3 for ease of explanation, even though many other restrictions, obvious to those of ordinary skill in the art, may be requested by card owners or card issuers for inclusion in the profile of FIG. 3.

Whenever a card owner is to be notified of a condition-breaching credit card transaction, the communications address field 308 may be used to identify a telephone number or an electronic mail address at which the card owner can be reached. Preferably, the communications address field stores a pager number associated with a communications carrier which provides paging service on a nationwide basis to contact, for example, the card owners associated with the first and the fourth record. Alternatively, a personal telephone number, such as a "500" or a "700" prefix number may be used as a reach number for a card owner, such as the card owner associated with the second and third record shown in FIG. 3. As another alternative, an electronic mail address may be used which, in various illustrative embodiments, may be either an address to which conventional electronic mail may be sent or an electronic address for use in other forms of electronic signaling such as, for example, a direct message communicated to the computer screen of a logged-on user or an interactive electronic two-way communication mechanism *(e.g.,* a "chat" or "talk" program).

Also included in the profile of FIG. 3 is no-answer-credit threshold field 309 and no-answer-transaction threshold field 310. Those fields identify respectively, the maximum amount of credit that can be approved, and the maximum number of permissible transactions within a given period of time, when the card owner cannot be reached by the communications system of FIG. 1. When the card owner does not wish any transactions to be authorized when he or she cannot be reached, then those fields are set to zero.

When the cost associated with the commercial transaction is charged to a debit card, as opposed to a credit card, only the card holder's name field 301, the card number field 302 and the communications address field 308 are of particular relevance since the request for approval is initiated by the merchant and the commercial transaction is not completed when the debit card holder cannot be reached.

Referring back to FIG. 1, when a transaction request message, such as the one illustrated in FIG. 2, is received by validation database 106, the latter uses a) the information included in that message, and b) the retrieved profile associated with the card number in that message to determine whether at least one card owner pre-imposed condition has been breached (or a card owner pre-defined threshold has been exceeded). If so, validation database 106 fetches the communications address of the credit card owner and any other appropriate information to format an authorization request and/or alert message that is transmitted to the card own-

Petitioner Askeladden LLC
Exhibit 1002 - Page 11 of 350

er. One such message is illustrated in FIG. 4 which shows a card holder's name field 401, a display field 402 and a field 403 that is populated by an entry in the table illustrated in FIG. 5. The card holder's name is populated by the name that is included in the profile retrieved by validation database 106. Field 402 is a display field that always contains the two words "Credit Card." Held 403 is populated by one of the entries in the table of FIG. 5.

The table of FIG. 5 shows three separate entries 501, 502 and 503 representing different sections of three different messages. Each entry is comprised mainly of display information and one field that is populated based on the particular condition that has been breached or the specific threshold that has been exceeded. For example, when the requested credit amount for the transaction exceeds the charging limit pre-selected by the card owner, field 505 will be populated by the difference between the maximum charging amount and the requested credit amount. Similarly, when validation of a card number for a transaction would cause the maximum number of transactions per day pre-selected by the card owner to be exceeded, the content of the transaction counter field is moved into field 506. Likewise, when the card holder attempts to charge to a credit card number the expenses related to the purchase of an item from a commercial establishment that is associated with a prohibited merchant code, that code is translated to one of the establishment type entries shown in the table of FIG. 6. That table correlates each merchant code to a particular type of commercial establishment. For example, hypothetical merchant code 1234 is associated with liquor stores, while fictitious merchant code 4567 is mapped to hotels and motels. Thus, once a merchant code is to a commercial establishment type entry, that entry is simply copied to field 507 of FIG. 5.

By populating field 403 of FIG. 4 with one of the entries in FIG. 5, a complete message is formulated for transmission to the card owner. Thereafter, validation database 106 retrieves the communications address in the profile to send to the card owner the message illustrated in FIG. 4 via an idle automatic dialing unit selected from ADU 110-1 to ADU 110-N. The latter are arranged a) to initiate phone calls by dialing telephone numbers received from validation database 106 and, b) to bridge those calls to other communications devices upon detecting a feedback signal from the card owner. ADU 110-1 to 110-N are also designed to terminate the call if no feedback signal is received after a predetermined period of time.

If the communications address is a personal telephone number, such as a "500" or "700" prefix number (shown, for example, in the third record of FIG. 3), then database 106 transmits the message illustrated in FIG. 4 to Interactive Voice Response System (IVRS) 125 before sending the communications address of the card owner to an idle ADU. Upon receiving the number dialed by ADU 110-1, for example, communications network 102 translates the "500" or "700" prefix telephone number to a Plain Old Telephone Service (POTS) telephone number at which the card owner can be reached. When ADU 110-1 detects a feedback signal from the card owner, it bridges the call (via line 140) to Interactive Voice Response System (IVRS) 125 that delivers the message of FIG. 4 in audio form to the card owner at telephone set 145, for example. Specifically, IVRS 125 is a processor that executes text-to-speech synthesis programmed instructions designed to use ASCII input, such as one of the messages shown in FIG. 4, to generate a "read aloud" audio rendition of that ASCII input in a machine synthesized voice. IVRS 125 is also arranged to prompt a card owner to provide some input to approve or disapprove a particular transaction. For example, a card owner may be prompted to enter a "1" on a telephone dialpad to approve a transaction, or a "2" on the dialpad to disapprove the transaction. Also included in IVRS 125 is a means to respond to touch-tone commands from a caller . In particular, IVRS 125 is arranged to translate the Dual Tone Multi-Frequency (DTMF) signal received from the card owner to a machine-readable format, such as ASCII, that is recognizable by validation database 106. Alternatively, IVRS 125 may include a word recognition unit that is arranged to output digitally recorded words, such as the messages in FIG. 5, to prompt a card owner for particular information that is converted to ASCII format for delivery to validation database 106. Furthermore, in order to insure that the person approving the transaction is the card owner, as opposed to an impostor, IVRS 125 may also include a speaker recognition unit that stores templates of pre-recorded digitized voice messages of the card owner that are compared to any input received from the called party to certify that the "real" card owner is the person approving the transaction.

If the communications address is a paging telephone number, then one of the ADUs 110-1 to 110-N dials the paging telephone number to initiate a call to that paging telephone number for the purpose of delivering one of the messages of FIG. 4 to pager device 135 of the card owner. The call is routed over communications network 102 which uses one of the demodulators 120-1 to 120-N to transform the received message into proper signaling format for delivery to paging system network 111 which may be, for example, a satellite-based nationwide paging service network. Alternatively, paging system network 111 may be a cellular communications network or a Personal Communications Services (PCS) network. Paging system network 111 includes a base station (not shown) that receives the dialed number along with the message of FIG. 5. The base station then identifies a particular frequency associated with that paging telephone number to code the received message as a series of pulses represented by a carrier that is modulated on that frequency for delivery to pager 135. The latter converts the pulses into a series of bytes representing the message of FIG. 5. Thereafter, pager

Petitioner Askeladden LLC
Exhibit 1002 - Page 12 of 350

135 emits a loud beep to signal the card owner of an incoming message. Alternatively, pager 135 could be a vibrating pager which silently alerts the card owner of the incoming message through a vibration signal generated therein in response to the reception of a message.

When the incoming message is an alert signal from validation database 106, pager 135 can be any commercially available paging device with a small screen for displaying the message of FIG. 4. However, if an approval/disapproval response is requested by validation database 106, pager 106 may advantageously be a two-way paging device, such as the device available from Mobile Telecommunications Technology Inc. of Jackson, Mississippi. In that case, the card owner transmits an approval/disapproval message by entering a pre-defined code in the two-way pager. The pre-defined code is then transmitted to validation database 106 via paging system network 111. The pre-defined code is received by one of the demodulators I20-1 to 120-N which demodulates the signals associated with the received code for presentation to validation database 106. Alternatively, pager 135 may be a one-way pager. In this case, if an approval/disapproval response is requested by validation database 106, the card owner may communicate an approval/disapproval message to validation database 106 by other means, such as with use of a conventional telephone, for example.

A first illustrative embodiment

FIG. 7 shows a flow diagram in accordance with certain illustrative embodiments of the present invention outlining programmed instructions executed by different elements of the communications system of FIG. 1 to receive an approval from a credit card owner for, or to alert a credit card owner of, a credit card transaction initiated by a card holder. The process shown in FIG. 7 is initiated in step 701 when validation database 106 receives a validation request for a credit card number. As mentioned above, the request for approval may be received in the form of a data message, such as the one illustrated in FIG. 2. Upon receiving the credit card number, validation database 106 uses the received credit card number as a search key in an attempt to retrieve a profile for the credit card number. If no profile is available in the validation database for the credit card number, as determined in step 702, validation database returns an "unauthorized transaction" message to card reader 101 via communications network 102. When validation database 106 is able to retrieve a profile for the card number, the profile is analyzed in step 704 to determine whether the requested credit amount or the type of transaction, for example, triggers any alerting or request for approval conditions. If no such conditions are triggered, validation database 106 proceeds with the validation process in a conventional manner. Otherwise, in step 706, validation database 106 ascertains whether the card owner is only to be alerted when the pre-defined condition is encountered. If so, validation database 106 retrieves from the profile the card owner's communications address to which the alerting message is sent, as indicated in step 707. Thereafter, validation database 106 proceeds with the validation process in a conventional manner.

When the profile retrieved by validation database 106 indicates that the card owner is to approve the credit card transaction (such as the one requested by the card holder) validation database 106 formulates a request for approval message (using appropriate entries in FIG. 4 and FIG. 5) for transmission to the card owner, as indicated in step 708. As mentioned above, the request for approval message may be delivered in the form of a telephone call or a paging message. After the transmission of the message, validation database waits for a response from the card owner. When validation database determines, in step 709, that no response is forthcoming after a pre-defined period of time has expired, validation database 106, in step 711, assesses whether the requested credit amount exceeds the no-answer-credit threshold. As indicated earlier, the no-answer-credit threshold is a field in the profile for a card number which stores the maximum amount of credit that can be approved for a credit card transaction when the credit card owner cannot be reached by the communications system of FIG. 1. If the requested credit amount exceeds the no-answer-credit threshold, as determined in step 711, then validation database 106 returns an "unauthorized transaction" message to card reader 101. If the requested credit amount does not exceed the no-answer-credit threshold, the content of the transaction counter field in the profile is compared to the no-answer-transaction threshold to determine whether this threshold has been exceeded. If so, validation database 106 returns an invalid card message to card reader 101, as indicated in step 705. If neither of the no-answer-thresholds has been exceeded, validation database 106 completes the validation process in a conventional manner, as indicated in step 703.

When validation database 106 receives a response from the card owner within a pre-defined period of time, as determined in step 709, validation database 106 then assesses whether the response indicates approval of the transaction by the card owner. If so, validation database completes the validation process in a conventional manner, as indicated in step 705. Optionally, the cardholder may be required to provide a secret code that matches a similar code included in the response received from the card owner before the transaction is authorized. If a disapproval response is received from the card owner, validation database 106 returns an "unauthorized transaction" message to card reader 101.

FIG. 8 is a flow chart outlining instructions performed by the elements of the illustrative communications system of FIG. 1 to validate a debit card transaction in accordance with a first illustrative embodiment of the present invention. The process depicted in FIG. 8 is in-

Petitioner Askeladden LLC
Exhibit 1002 - Page 13 of 350

itiated in step 801 when validation database 106 receives a debit card number and a password entered by a minor card holder. Validation database 106 launches a query on its storage devices to determine, in step 802, whether a profile can be retrieved for the received card number. If no profile is found, validation database 106 transmits an "unauthorized transaction" message to card reader 101, as indicated in step 803. Upon retrieving a profile for the card number, validation database 106 formulates a message using one of the entries of FIG. 4 for transmission to the card owner. Thereafter, validation database 106 waits a pre-defined amount of time to determine whether a response is received from the card owner. If the pre-defined amount of time expires before a response is received from the card owner, validation database 106 returns an "unauthorized transaction" message to card reader 101, as indicated in step 803. When a response indicative of the card owner's approval of the transaction is received from the card owner, as determined in step 806, validation database 106 proceeds with the validation process in a conventional manner, as indicated in step 807. If the card owner sends a message disapproving the debit card transaction, validation database 106 sends an "unauthorized transaction" message to card issuer 101, as indicated in step 803.

In other illustrative embodiments of the present invention, the authorization of a transaction may need to be approved by more than one party. For example, if the charge account is a corporate account and the amount of the charge is over a certain predefined threshold, it may be required that two authorized parties *(e.g.,* corporate executives) approve the transaction. This is analogous, for example, to the common requirement that corporate checks over a certain amount *(e.g.,* $1,000) include two authorized signatures to be valid. Similarly, if the transaction involves, for example, the dispensing of medications in a hospital (see below), it may be desirable that both the patient's doctor and the hospital's pharmacist approve the treatment. In these cases, step 806 of FIG. 8 is modified to determine whether all parties which are required to approve the transaction have done so.

A second illustrative embodiment

FIG. 9 shows a flow chart of a credit card purchase transaction to which certain illustrative embodiments of the present invention may advantageously be applied. The transaction is initiated by a cardholder *(i.e.,* the customer) who instructs a retailer to charge a purchase to a given credit card account (step 11). This instruction usually takes the form of providing a credit card or a credit card number to the retailer. This transaction may occur with the customer and the retailer co-present and in real-time, while the customer is waiting. In this case, the timeliness with which the authorization process is completed is clearly of great importance, since the relevant parties are awaiting such authorization before they may proceed with other endeavors. (For example, they may be waiting so that the retailer may hand over the goods to the customer or provide a service thereto.) Thus, the communication to the customer and a confirmation or denial of authorization by the customer should advantageously occur quickly. For this reason, the use of two-way pagers is preferred for this type of application of the principals of the present invention.

In alternative applications, the customer may have instructed the retailer (or an agent of the retailer) in person or via some communication mechanism *(e.g.,* a phone, mail, facsimile or electronic mail) at a time prior to the initiation of the transaction. Such instructions might cover an immediate one-time purchase, a future purchase *(e.g.,* the goods or service may not be immediately available) or a series of purchases to occur over a period of time. In cases such as these where the customer and the retailer are not co-present, the parties most typically do not require the authorization to be completed before they may proceed with other endeavors. That is, it may be acceptable in these cases that the authorization process be completed over a longer period of time such as, for example, several hours or even a day. In these cases, therefore, other less immediate communications mechanisms may be used, such as those provided by conventional telephones, e-mail, or, in some circumstances, even physical mail.

In any event, the retailer's typical response to such instructions is to signal a transaction processing center (or a network of such centers) which is associated with the credit card service provider that a particular customer (identified by his or her credit card number) wishes to purchase goods or services of a particular value. Thus, the retailer requests an authorization for the charge from the transaction processing center (step 12). Typically, this request is initiated by swiping the credit card through an automated card reader (such as card reader 101 of FIG. 1) which reads the magnetic stripe on the credit card, dials the transaction processing center, sends the relevant information thereto and receives either an authorization code or a denial in response therefrom. The information transmitted to the transaction processing center typically includes the credit card number, the amount of the contemplated purchase, and the retailer's store identification code *(e.g.,* card number 201, requested credit amount 202, and merchant code 203 of FIG. 2, respectively). The retailer then waits for an authorization from the transaction processing center which represents that the charge will be underwritten *(i.e.,* insured) by the credit card service provider. This authorization is typically sent to the retailer in the form of an authorization code which identifies the transaction and can thereby be used to verify that the authorization process was properly adhered to by the retailer. One typical reason for denial, on the other hand, is that the balance on the customer's account has exceeded (or, if the given purchase were authorized would exceed) a predeter-

Petitioner Askeladden LLC
Exhibit 1002 - Page 14 of 350

mined credit limit associated with the customer's account. In accordance with certain illustrative embodiments of present invention, another reason for denial is the lack of the receipt of an appropriate confirmation (or the receipt of an explicit denial) by the customer whose account is to be charged.

At the transaction processing center, the authorization process is performed automatically by a computer based system comprising, *inter alia,* a database *(e.g.,* validation database 106 of FIG. 1) containing account information for each credit card subscriber (step 13). That is, such a system automatically makes the decision whether to authorize or deny the transaction -- no human intervention is typically required at the transaction processing center. If the transaction is authorized (decision 14), as is typically indicated by the appearance of the authorization code on the display of the retailer's card reader, the retailer is thereby authorized by the credit card issuer to accept the charge for the purchase. Thus, the charge is accepted and the transaction is completed (step 15). If, on the other hand the transaction is denied by the transaction processing center (typically indicated by the appearance of a denial code on the card reader's display), the retailer denies the charge and terminates the transaction (step 16).

FIG. 10 shows a flow chart of an automated authorization process which may be used to implement step 13 of the process of FIG. 9 in accordance with a second illustrative embodiment of the present invention. The process of FIG. 10 is illustratively executed by a computer system at the transaction processing center in response to each received request for the authorization of a transaction. The received authorization request (typically transmitted by an automated card reader at the retailer's location such as card reader 101 of FIG. 1) includes, in particular, a customer identifier *(i.e.,* the credit card number) and may, for example, also include the amount of the proposed purchase and the retailer's store identification code (step 20). Based on the customer identifier, a database (such as validation database 106 of FIG. 1) is consulted to determine whether the transaction should be authorized (steps 21 and 22). For example, the database may include account balance and credit limit information indicating that the customer's account balance is not permitted to exceed a given credit limit. In such a case, the system will determine that the transaction should not be authorized if the sum of the account balance and the amount of the purchase to be authorized exceeds the credit limit. In addition, invalid or (known to be) stolen credit cards obviously should not be authorized.

If it is determined from the analysis of step 22 that the purchase should not be authorized for some reason (decision 23), the system will format a denial code (step 24). If, on the other hand, there is no basis for denying the transaction, the system will, in accordance with the principles of the present invention, make an attempt to have the (tentative) authorization confirmed by the customer. In particular, and in accordance with a second illustrative embodiment thereof, the system will automatically page the customer (using, for example pager 135 of FIG. 1), supplying to him or her any relevant information concerning the purchase (step 25). For example, the system might supply the customer with an identity of the retailer and/or the amount of the purchase, in order to enable the customer to more accurately ensure that the transaction to be authorized is, in fact, the one he or she is presently undertaking, or, alternatively, that the transaction is one being undertaken by an agent and the principal *(i.e.,* the customer) approves thereof. The customer's pager number *(i.e.,* the telephone number which is used to communicate with the pager) may, for example, be stored in the database and associated with the customer's account, as is shown in FIG. 3.

Once the customer has been paged, the system of the second illustrative embodiment waits for a confirmation from the customer which may be supplied with use of the customer's two-way pager (step 26). If the customer responds with an appropriate confirmation (decision 27), the system generates, formats and stores an authorization code which will enable the transaction to be completed. If, on the other hand, the customer does not confirm the transaction *(e.g.,* if no response is received from the customer within a predetermined amount of time), the system formats a denial code (step 24). After either a denial code or an authorization code has been formatted, it is sent to the retailer *(e.g..,* to card reader 101 of FIG. 1) who originally submitted the authorization request (step 29).

A Third Illustrative Embodiment

FIG. 11 shows a flow chart of an automated authorization process which may be used to implement step 13 of the process of FIG. 1 in accordance with a third illustrative embodiment of the present invention. As can be seen from the figure, the illustrative process of FIG. 11 is identical to the illustrative process shown in FIG. 10 except that decision 27, which determined whether a confirmation was received from the customer is replaced by decision 30, which determines whether a denial is received from the customer. Other embodiments of the present invention may combine those shown in FIG. 10 and FIG. 11 by accepting either a confirmation or a denial from the customer. In such a case, the default *(i.e.,* timeout) criterion may be either an assumed confirmation or an assumed denial.

A Fourth Illustrative Embodiment

FIG. 12 shows a flow chart of an authorization process which may be used to implement step 13 of the process of FIG. 9 in accordance with a fourth illustrative embodiment of the present invention. This fourth embodiment may advantageously be employed when the customer has only a one-way (as opposed to a two-way)

Petitioner Askeladden LLC
Exhibit 1002 - Page 15 of 350

pager, since it allows for the customer's confirmation to be communicated indirectly through the retailer. Specifically, the illustrative process of FIG. 12 is identical to that of the illustrative embodiment of FIG. 10 and FIG. 11 except in the mechanism by which the customer confirmation is requested and received.

In particular, when decision 23 determines that it is okay to authorize the transaction, the illustrative system of this fourth embodiment generates a confirmation code and supplies that code to the customer via his or her (one-way) pager (steps 41 and 42). The supplied confirmation code may, for example, be randomly generated so as not to be predictable. In this manner, the confirmation code will be known only to the customer (and not, for example, to a fraudulent user of the customer's credit card number who is not in possession of the customer's pager). The confirmation code may then be used to indirectly confirm the authorization. For example, where the customer is making a face-to-face purchase in a store, the customer may provide the confirmation code supplied by the transaction processing center to the retailer, who may, in turn, provide that confirmation code back to the transaction processing center. This latter step may be performed, for example, with use of the automated card reader which is already in communication with the transaction processing center.

Thus, after the illustrative process of FIG. 12 has supplied the confirmation code to the customer, step 43 waits for a responsive input which includes a (return) confirmation code *(e.g.,* from the automated card reader). Then, the confirmation code which was supplied for the given transaction is compared to the confirmation code that was received (decision 44) to ensure that the customer is, in fact, providing a proper confirmation of the authorization. If the supplied confirmation code matches the received confirmation code, the system authorizes the transaction (steps 28 and 29). If they do not match, or if the system receives no responsive confirmation code after a predetermined amount of time has elapsed, the transaction is denied (steps 24 and 29).

A Fifth Illustrative Embodiment

FIG. 13 shows a flow chart of a credit card purchase transaction to which a fifth illustrative embodiment of the present invention may advantageously be applied. This fifth embodiment eliminates the need for performing multiple communications at the time of purchase. That is, the extra time that may otherwise be required to page the customer and receive a confirmation or denial of the pending authorization are not needed when this fifth illustrative embodiment is employed.

Prior to the initiation of the transaction itself, the customer requests and receives a confirmation code for use in a specifically identified subsequent transaction (steps 51 and 52). This confirmation code, which may, for example, be randomly generated, will be known only to the customer who intends to execute the specific transaction *(e.g.,* make a particular purchase), or, alternatively, to an agent of the customer *(i.e.,* the principal) to whom the customer has communicated the given confirmation code. The specific transaction may, for example, be identified based on the retailer's store identification code (such as merchant code 203 of FIG. 2) or other identifying indicia of the retailer. Then, when the purchase is initiated, the customer (or the principal's informed agent) provides the previously received confirmation code to the retailer, who, in turn, provides the confirmation code to the transaction processing center which performs the automated authorization process (steps 53-55). The automated authorization system can then use the received confirmation code in a manner similar to that of the fourth illustrative embodiment shown in FIG. 12 for purposes of confirming an authorization of the transaction. Note that since the two-way communication process of steps 51 and 52 need not occur at the time (or at the location) of the purchase but, rather, may precede the transaction by a substantial amount of time, a wide variety of communications devices (in addition to one-way or two-way pagers) may advantageously be used in realizing the fifth illustrative embodiment.

FIG. 14 shows a flow chart of an automated authorization process which may be used to implement step 55 of the process of FIG. 13 in accordance with the fifth illustrative embodiment of the present invention. As described above, upon the receipt of a customer's request for a confirmation code to be used in executing a specific (future) transaction, the illustrative authorization system generates and supplies a confirmation code to the customer. In addition to its being supplied to the customer, however, this confirmation code is associated with the customer identifier and, for example, the retailer store identification code, and this data is then stored in the transaction processing center database *(e.g.,* validation database 106 of FIG. 1) for later retrieval -- that is, when the identified transaction is actually executed. Thus, upon a request for authorization of the given transaction, the illustrative process of FIG. 14 retrieves the previously supplied confirmation code from the database based on the customer identifier and the retailer store identification code (steps 61 and 62). Then, after it is determined that the transaction should (otherwise) be authorized, the system verifies that the confirmation code received with the request for authorization matches the confirmation code previously supplied to the customer (decision 63). If they do in fact match, the authorization may be confirmed (steps 28 and 29).

A Sixth Illustrative Embodiment

In accordance with a sixth illustrative embodiment of the present invention, a confirmation code may be provided to a customer without the customer making a specific request therefor. This embodiment may be advantageously applied to a credit card purchase transaction in a similar manner to the fifth illustrative embodi-

Petitioner Askeladden LLC
Exhibit 1002 - Page 16 of 350

ment described above. In particular, the flow chart shown in FIG. 13 may be modified by removing step 51 therefrom Then, instead of the customer requesting and receiving a confirmation code for use in a specifically identified subsequent transaction, the customer (automatically) receives a new confirmation after each transaction and/or periodically *(e.g.,* each morning) for use in his or her next transaction. By limiting the use of the given confirmation code to, for example, a single transaction, the advantages of the present invention in protecting against fraudulent transactions is obtained, while no direct communication from the customer to the transaction processing center is required. Thus, for example, as in the case of the fourth and fifth illustrative embodiments, one-way pagers may advantageously be used. Moreover, the use of a confirmation code which does not match the last previously supplied confirmation code but, rather, matches one used in a previous transaction may well be indicative of fraud.

Although a number of specific embodiments of this invention have been shown and described herein, it is to be understood that these embodiments are merely illustrative of the many possible specific arrangements which can be devised in application of the principles of the invention. Numerous and varied other arrangements can be devised in accordance with these principles by those of ordinary skill in the art without departing from the spirit and scope of the invention. For example, although the embodiments described above have focused on a credit card purchase transaction, it will be obvious to those of ordinary skill in the art that the principles of the present invention may be applied to a wide variety of transactions including, but not limited to, telephone calling card transactions, banking transactions including those using PINs, stock and commodity trading transactions, and secure access transactions such as computer access transactions based on computer passwords. In addition, the principals of the present invention may be applied to numerous other types of secure access transactions such as physical access *(i.e.,* entry) transactions including those used for purposes of inventory control. For example, an entry door to a secure room *(e.g.,* a hospital's medication room) or to a secure facility may be locked by an electronic locking system *(e.g.,* combination keypad or card access entry) which is electronically linked to a central facility such as the transaction processing center described above. Then, any attempt to enter the room or facility may be made subject to confirmation in accordance with the principals of the present invention.

In addition, although the above embodiments focused primarily on communication via wireless paging devices *(e.g.,* one-way or two-way pagers), it will be obvious to those skilled in the art that many other communications mechanisms may be used instead of, or in addition to, wireless paging devices. These mechanisms include, for example, cellular telephones, conventional wired telephones, personal computers, *etc.*

Claims

1. An automated method for authorizing a transaction, said transaction based on a customer identifier associated with a customer, the method comprising the steps of:

   receiving a request to authorize said transaction, said request including said customer identifier;
   determining, in response to said request and based on said customer identifier, whether to authorize said transaction;
   if said determining step determines that said transaction is to be authorized, communicating said determination to said customer;
   receiving a communication from said customer confirming that said customer consents to said transaction being authorized; and
   authorizing said transaction in response to said communication received from said customer.

2. An automated method for authorizing a transaction, said transaction based on a customer identifier associated with a customer, the method comprising the steps of:

   receiving a request to authorize said transaction, said request including said customer identifier;
   determining, in response to said request and based on said customer identifier, whether to authorize said transaction;
   if said determining step determines that said transaction is to be authorized, communicating said determination to said customer; and determining whether a communication indicating that said transaction is not to be authorized is received within a given amount of time from said customer; and
   authorizing said transaction if said communication from said customer is not received within said given amount of time.

3. The method of claim I or 2 wherein said step of communicating said determination to said customer comprises transmitting signals representative of said determination to a wireless telecommunications receiver.

4. The method of claim 3 wherein said wireless telecommunications receiver comprises a display and wherein said step of communicating said determination to said customer comprises communicating said customer identifier to said customer.

5. The method of claim 3 wherein said wireless telecommunications receiver comprises a display and

Petitioner Askeladden LLC
Exhibit 1002 - Page 17 of 350

wherein said step of communicating said determination to said customer comprises communicating an identity of said provider to said customer.

6. The method of claim 3 wherein said wireless telecommunications receiver comprises a two-way pager and wherein said communication from said customer confirming that said customer consents to said transaction being authorized is transmitted by said customer with use of said two-way pager.

7. An automated method for authorizing a transaction, said transaction based on a customer identifier associated with a customer, the method comprising the steps of:

communicating to said customer a confirmation code for use in executing said transaction;
receiving a request to authorize said transaction, said request including said customer identifier and said confirmation code;
determining, in response to said request, based on said customer identifier, and based on whether said received confirmation code matches said confirmation code communicated to said customer, whether to authorize said transaction;
authorizing said transaction if said determining step determines that said transaction is to be authorized.

8. The method of claim 7 wherein said step of communicating to said customer a confirmation code for use in executing said transaction is performed in response to receiving a communication from said customer indicating that said customer desires to execute said transaction.

9. The method of claim 7 further comprising the step of communicating a second confirmation code to said customer after authorizing said transaction, said second confirmation code for use in executing a second transaction subsequent to said transaction and being different from said confirmation code.

10. An automated method for authorizing a transaction, said transaction based on a customer identifier associated with a customer, the method comprising the steps of:

receiving a request to authorize said transaction, said request including said customer identifier;
determining, in response to said request and based on said customer identifier, whether to authorize said transaction;
if said determining step determines that said transaction is to be authorized, communicating to said customer a confirmation code for use in completing execution of said transaction;
receiving a communication comprising said confirmation code; and
authorizing said transaction in response to said received confirmation code matching said confirmation code communicated to said customer.

11. The method of claim 7 or 10 wherein said step of communicating to said customer said confirmation code comprises encoding said confirmation code to provide a secure communication thereof.

12. The method of claim 1, 2, 7 or 10 wherein said transaction comprises a sales transaction and wherein said customer identifier comprises a credit card number.

13. The method of claim 1, 2, 7 or 10 wherein said transaction comprises placing a telephone call and wherein said customer identifier comprises a telephone calling card number.

14. The method of claim 1, 2, 7 or 10 wherein said transaction comprises a banking transaction and wherein said customer identifier comprises a bank card number.

15. The method of claim 1, 2, 7 or 10 wherein said customer identifier comprises a Personal Identification Number.

16. The method of claim 7 or 10 wherein said step of communicating said confirmation code to said customer comprises transmitting a signal representative of said confirmation code to a wireless telecommunications receiver.

17. The method of claim 3 or 16 wherein said wireless telecommunications receiver comprises a pager.

18. An automated system for use in authorizing a transaction, said transaction based on a customer identifier associated with a customer, the system comprising:

a receiver adapted to receive a request to authorize said transaction, said request including said customer identifier;
means for determining, in response to said request and based on said customer identifier, whether to authorize said transaction;
a transmitter adapted to communicate said determination to said customer if said means for determining determines that said transaction is to be authorized;
a receiver adapted to receive a communication from said customer confirming that said cus-

Petitioner Askeladden LLC
Exhibit 1002 - Page 18 of 350

tomer consents to said transaction being authorized; and
means for authorizing said transaction in response to said communication received from said customer.

19. An automated system for use in authorizing a transaction, said transaction based on a customer identifier associated with a customer, the system comprising:

a receiver adapted to receive a request to authorize said transaction, said request including said customer identifier;
means for determining, in response to said request and based on said customer identifier, whether to authorize said transaction;
a transmitter adapted to communicate said determination to said customer if said means for determining determines that said transaction is to be authorized;
a timer adapted to determine whether a communication indicating that said transaction is not to be authorized is received within a given amount of time from said customer; and
means for authorizing said transaction if said communication from said customer is not received within said given amount of time.

20. An automated system for use in authorizing a transaction, said transaction based on a customer identifier associated with a customer, the system comprising:

a receiver adapted to receive a communication from said customer indicating that said customer desires to execute said transaction;
a transmitter adapted to communicate to said customer a confirmation code for use in executing said transaction;
a receiver adapted to receive a request to authorize said transaction, said request including said customer identifier and said confirmation code;
means for determining, in response to said request, based on said customer identifier, and based on whether said received confirmation code matches said confirmation code communicated to said customer, whether to authorize said transaction; and
means for authorizing said transaction if said means for determining determines that said transaction is to be authorized.

21. An automated system for use in authorizing a transaction, said transaction based on a customer identifier associated with a customer, the system comprising:

a receiver adapted to receive a request to authorize said transaction, said request including said customer identifier;
means for determining, in response to said request and based on said customer identifier, whether to authorize said transaction;
a transmitter adapted to communicate to said customer a confirmation code for use in completing execution of said transaction if said means for determining determines that said transaction is to be authorized;
a receiver adapted to receive a communication comprising said confirmation code; and
means for authorizing said transaction in response to said received confirmation code matching said confirmation code communicated to said customer.

22. A method of processing a transaction, the method comprising the steps of:

receiving information associated with a transaction initiated by an agent of a principal;
retrieving a profile based on said information associated with said transaction;
comparing at least a portion of said information to data included in said profile; and
in response to said comparison, notifying said principal of said transaction.

23. The method of claim 22 wherein said notifying step further includes the step of transmitting a message to said principal to request approval for the transaction.

24. The method of claim 23 further comprising the steps of:

receiving an approval signal from said principal; and
in response to receiving said approval signal, authorizing said transaction.

25. The method of claim 24 wherein the approval signal from the principal is transmitted from a paging device which received the notification in response to the comparison.

26. The method of claim 23 further comprising thc steps of:

receiving a disapproval signal from said principal; and
in response to receiving said disapproval signal, invalidating said transaction.

27. The method of claim 23 further comprising the step of invalidating said transaction when no signal is re-

Petitioner Askeladden LLC
Exhibit 1002 - Page 19 of 350

ceived from said principal in response to said request for approval message.

28. The method of claim 22 wherein said comparing step further includes the step of determining whether parameters included in said second subset of information exceed threshold values represented by said data included in said profile.

29. A system for processing a transaction. the system comprising:

a database which receives information associated with a transaction initiated by an agent of a principal and which stores a profile defined by said principal;
a processor which a) retrieves said profile from said database based on said information associated with said transaction, and b) compares at least a portion of said information to data included in said profile; and
a network over which a notification signal is transmitted to said principal in response to said comparison.

30. The system of claim 29 wherein said notification signal includes a message requesting approval of the transaction.

31. The system of claim 30 further comprising:

an end-user device from which an approval signal is transmitted by said principal to said database; and
means responsive to receiving said approval signal at said database, for authorizing said transaction.

32. The system of claim 31 further comprising a paging device which a) receives the notification signal in response to the comparison, and b) transmits the approval signal from the principal.

33. The system of claim 30 further comprising:

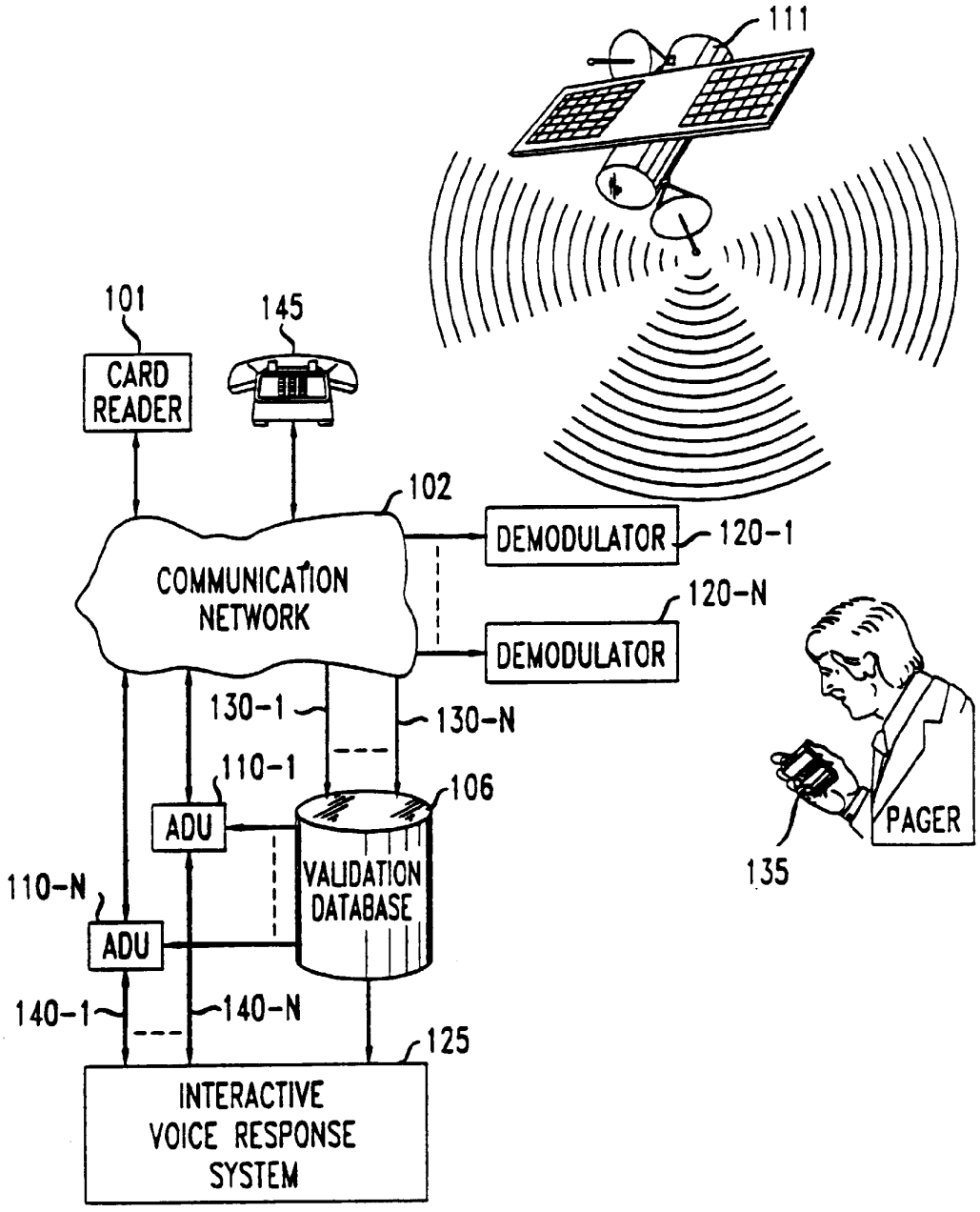
an end-user device from which a disapproval signal is transmitted by said principal to said database; and
means responsive to receiving said disapproval signal at said database. for invalidating said transaction.

34. The system of claim 30 further comprising means for invalidating said transaction when no signal is received from said principal in response to said request for approval message.

35. The system of claim 29 wherein said processor further includes means for determining whether parameters included in said second subset of information exceed threshold values represented by said data included in said profile.

Petitioner Askeladden LLC
Exhibit 1002 - Page 20 of 350

FIG. 1



Petitioner Askeladden LLC
Exhibit 1002 - Page 21 of 350

FIG. 2

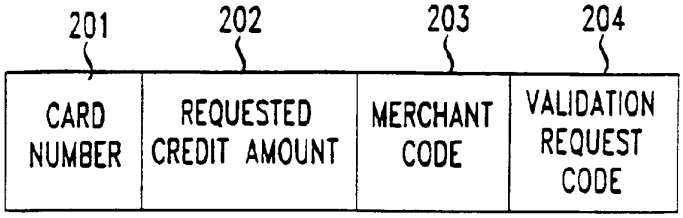


FIG. 4

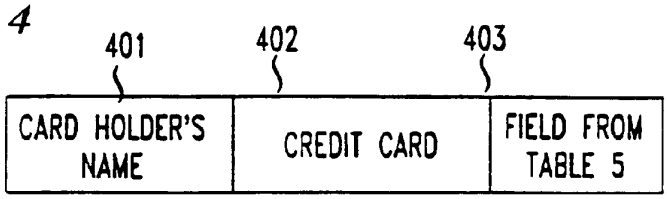


FIG. 5

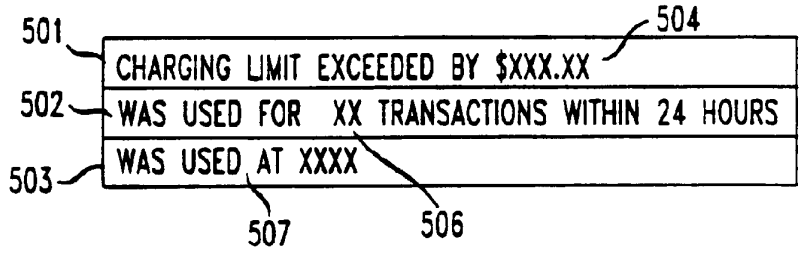
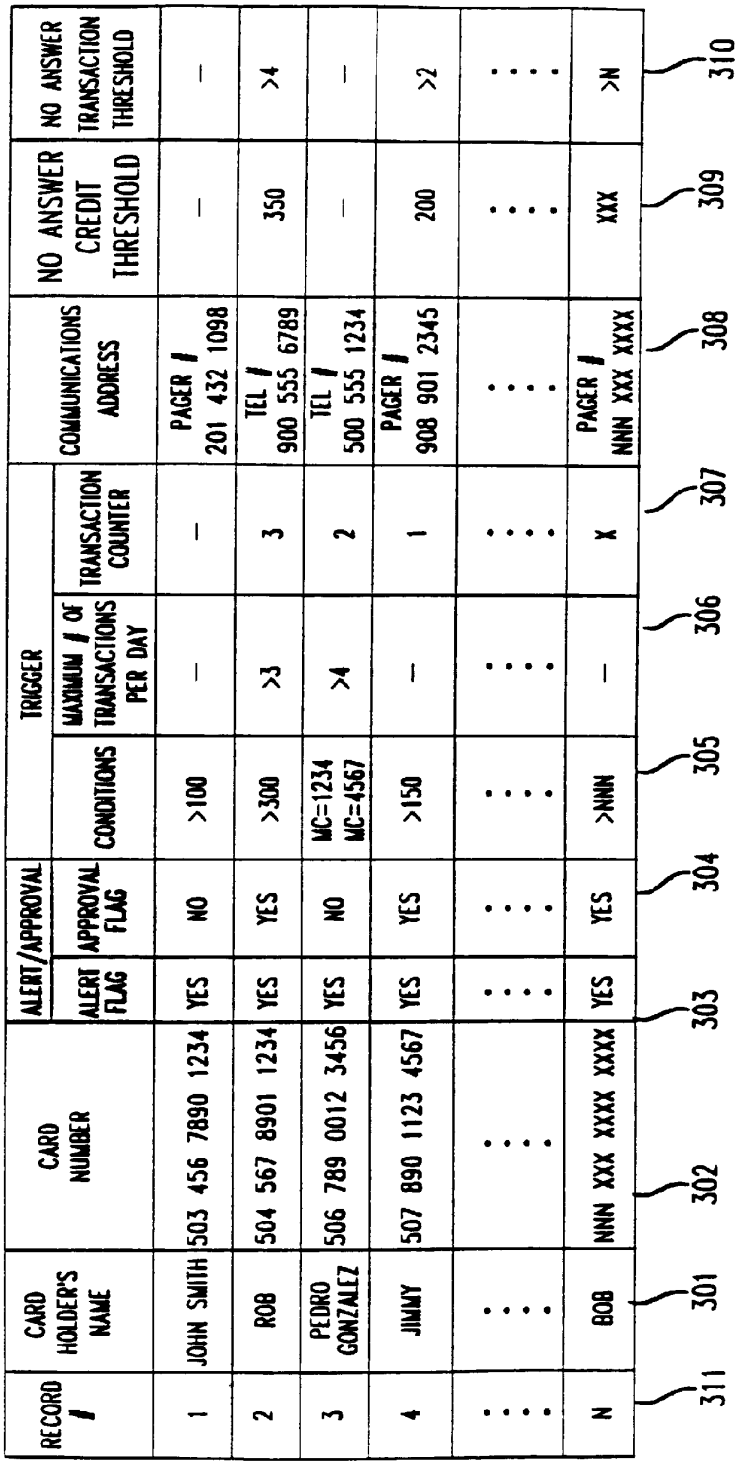


FIG. 6

MERCHANT CODE	ESTABLISHMENT TYPE
1234	LIQUOR STORE
4567	HOTEL
5678	RACE TRACK

Petitioner Askeladden LLC
Exhibit 1002 - Page 22 of 350

FIG. 3

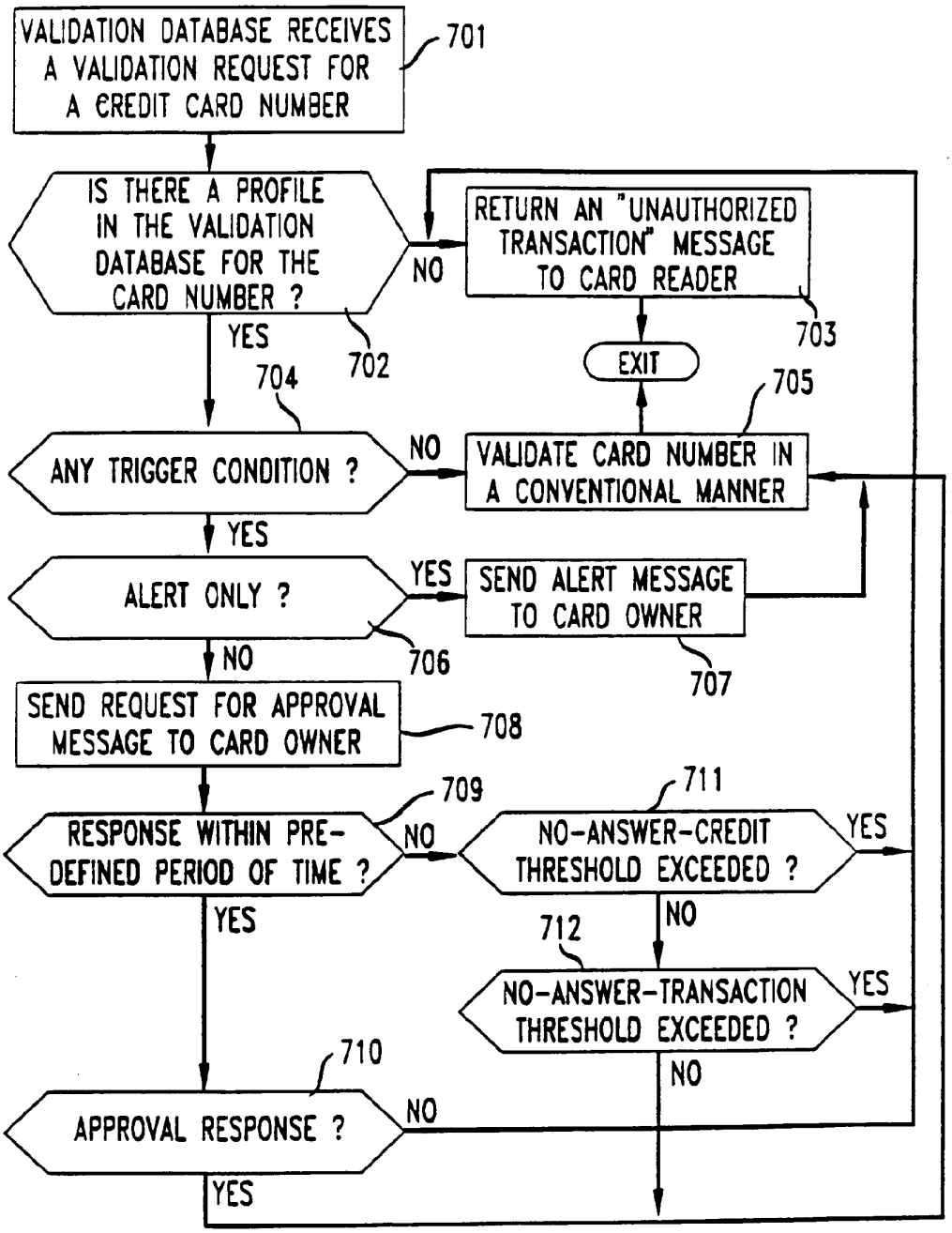


RECORD #	CARD HOLDER'S NAME	CARD NUMBER	ALERT/APPROVAL		TRIGGER			COMMUNICATIONS ADDRESS	NO ANSWER CREDIT THRESHOLD	NO ANSWER TRANSACTION THRESHOLD
			ALERT FLAG	APPROVAL FLAG	CONDITIONS	MAXIMUM # OF TRANSACTIONS PER DAY	TRANSACTION COUNTER			
1	JOHN SMITH	503 456 7890 1234	YES	NO	>100	—	—	PAGER # 201 432 1098	—	—
2	ROB	504 567 8901 1234	YES	YES	>300	>3	3	TEL # 900 555 6789	350	>4
3	PEDRO GONZALEZ	506 789 0012 3456	YES	NO	MC=1234 MC=4567	>4	2	TEL # 500 555 1234	—	—
4	JIMMY	507 890 1123 4567	YES	YES	>150	—	1	PAGER # 908 901 2345	200	>2
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
N	BOB	NNN XXX XXXX XXXX	YES	YES	>NNN	—	X	PAGER # NNN XXX XXXX	XXX	>N

311 301 302 303 304 305 306 307 308 309 310

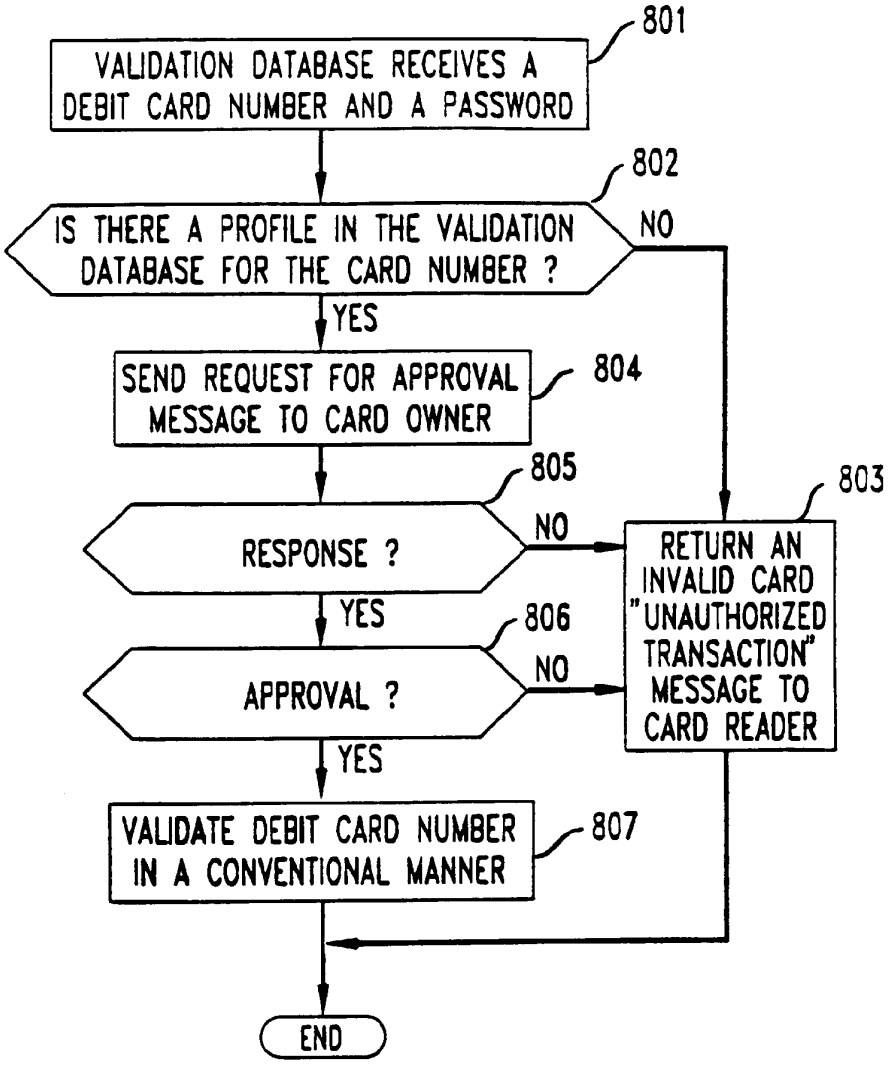
Petitioner Askeladden LLC
Exhibit 1002 - Page 23 of 350

FIG. 7



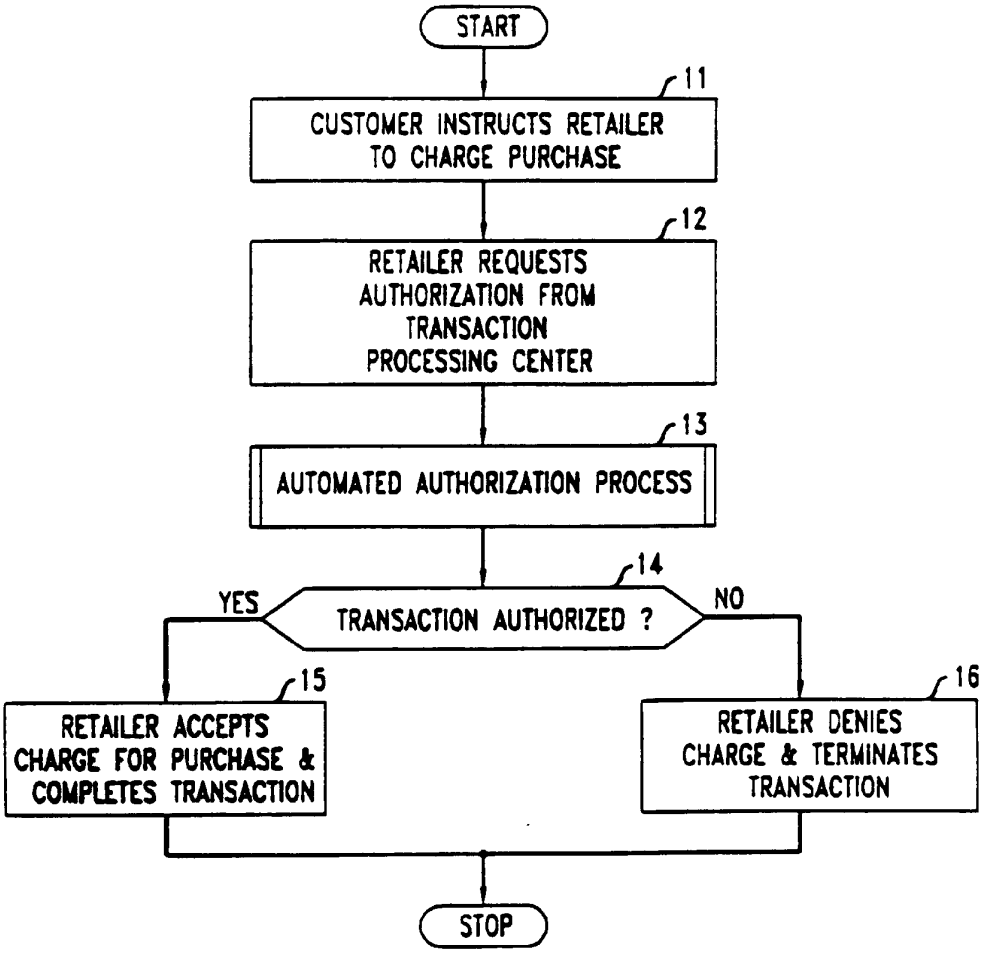
Petitioner Askeladden LLC
Exhibit 1002 - Page 24 of 350

FIG. 8



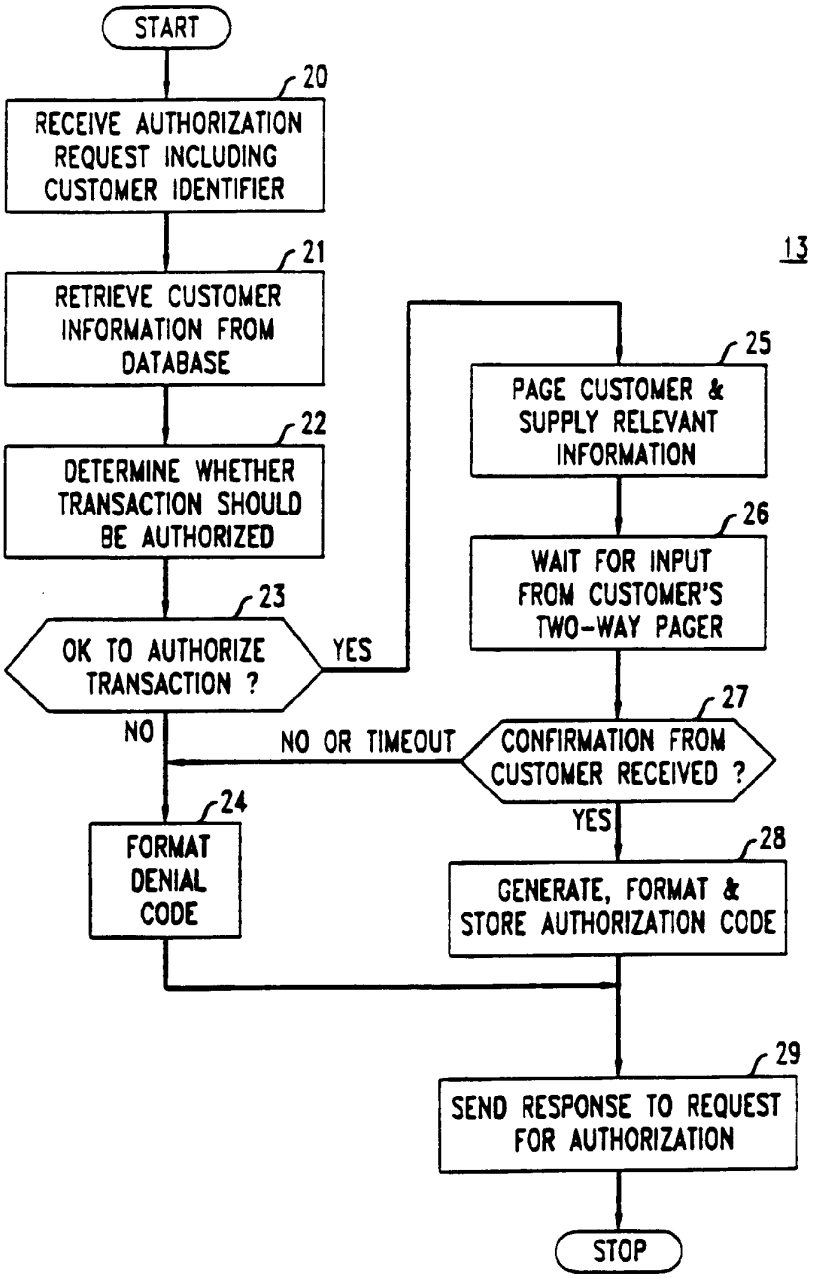
Petitioner Askeladden LLC
Exhibit 1002 - Page 25 of 350

FIG. 9



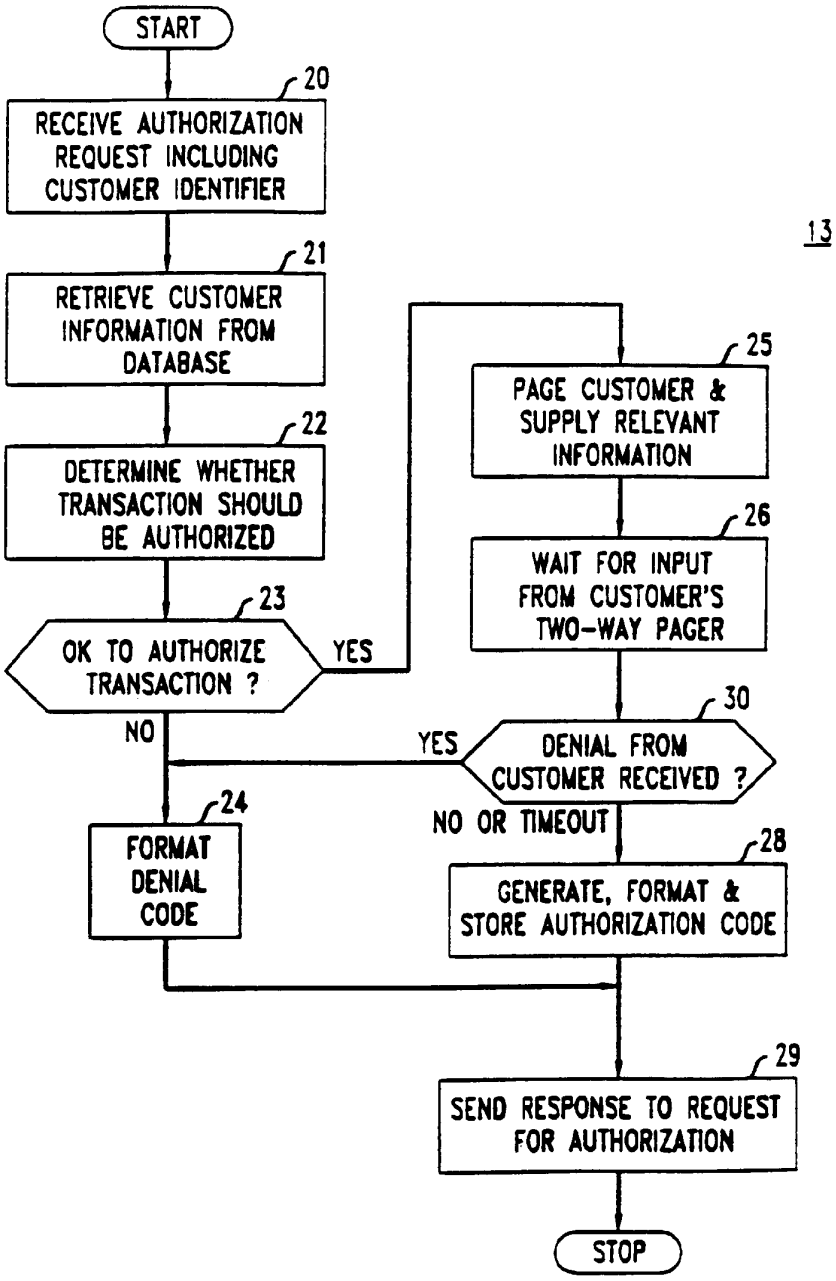
Petitioner Askeladden LLC
Exhibit 1002 - Page 26 of 350

FIG. 10



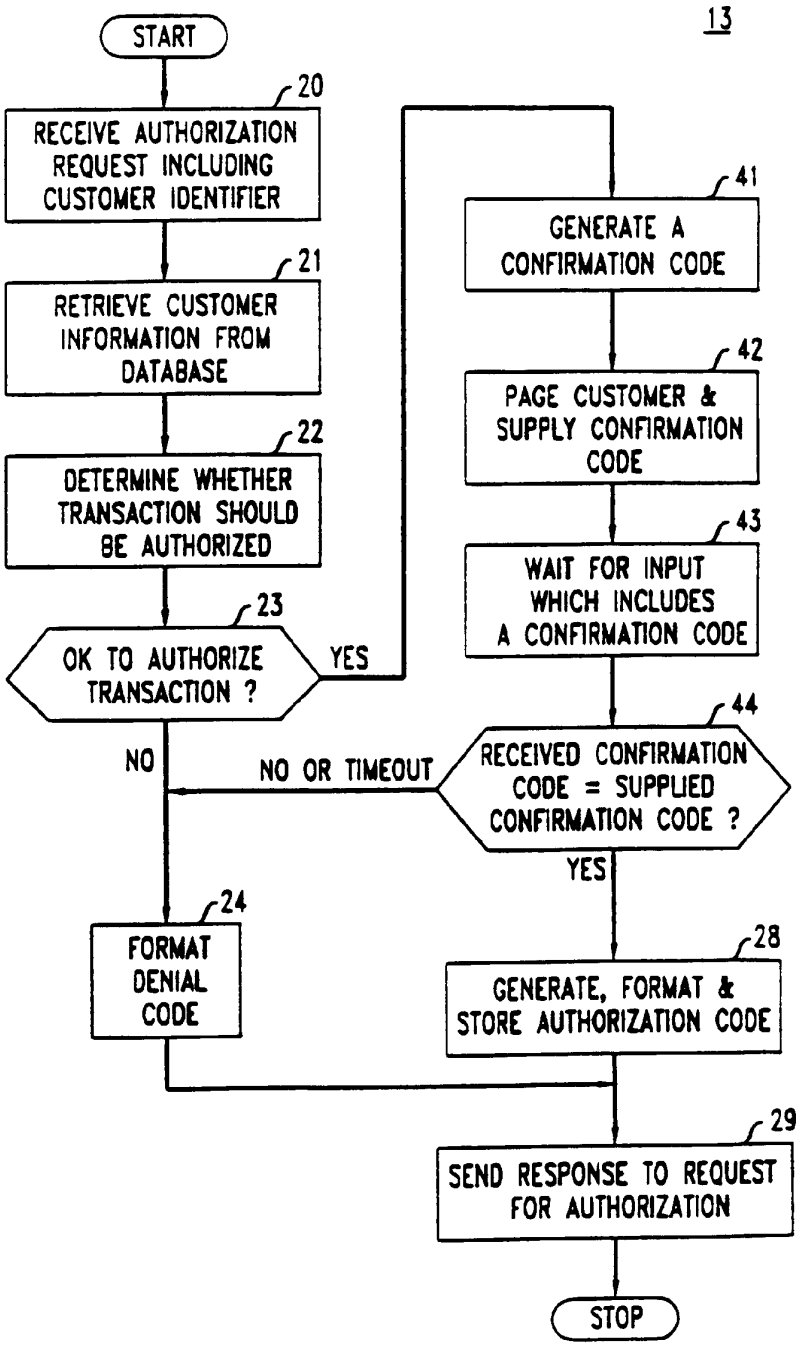
Petitioner Askeladden LLC
Exhibit 1002 - Page 27 of 350

FIG. 11



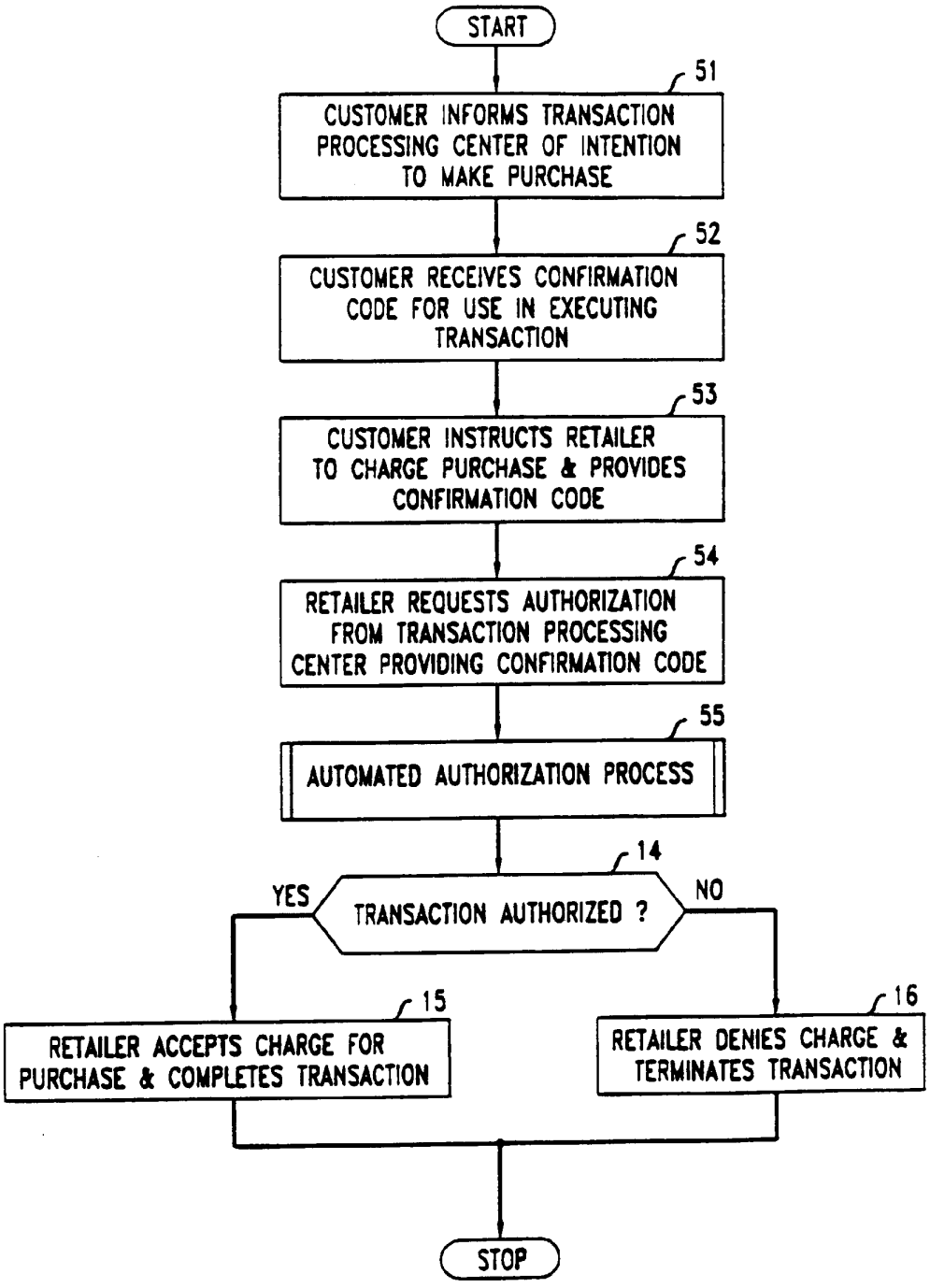
Petitioner Askeladden LLC
Exhibit 1002 - Page 28 of 350

FIG. 12



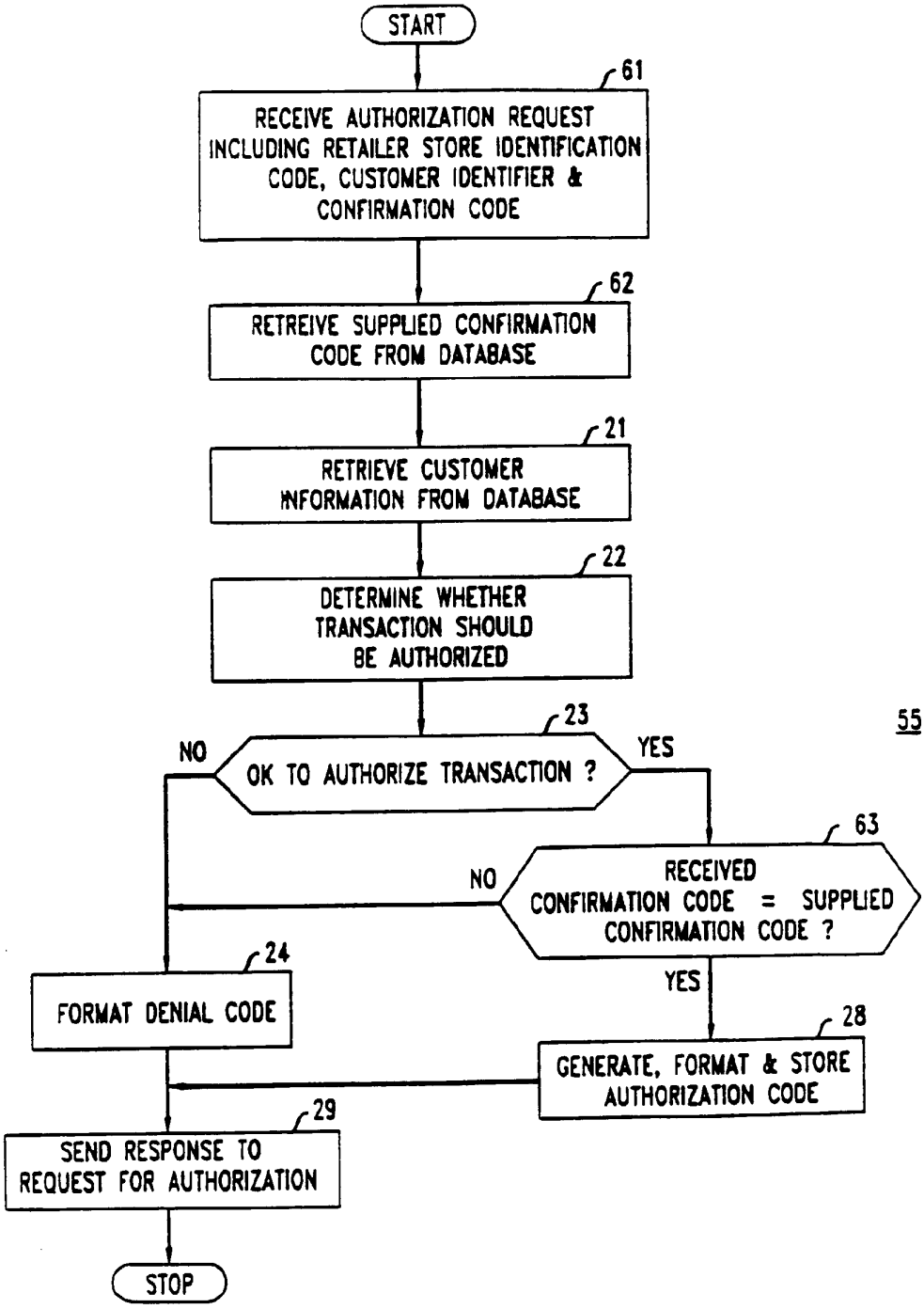
Petitioner Askeladden LLC
Exhibit 1002 - Page 29 of 350

FIG. 13



Petitioner Askeladden LLC
Exhibit 1002 - Page 30 of 350

FIG. 14



Petitioner Askeladden LLC
Exhibit 1002 - Page 31 of 350

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 136 961 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
26.09.2001 Bulletin 2001/39

(51) Int Cl.[7]: **G07F 7/10**
// G07F19/00

(21) Application number: **00202720.9**

(22) Date of filing: **31.07.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **24.03.2000 ES 200000724**
23.06.2000 ES 200001573
23.06.2000 ES 200001574

(71) Applicants:
- **Banco Bilbao Vizcaya Argentaria S.A.**
  48005 Bilbao (ES)
- **Telefonica Servicios Moviles S.A.**
  28013 Madrid (ES)

(72) Inventors:
- **Calvo Pesquera, Alicia Lucia**
  28220 Majadahonda, Madrid (ES)
- **Vacas Cid, José Luis**
  28806 Alcala de Henares, Madrid (ES)
- **De Casso Basterrechea, Pablo**
  28020 Madrid (ES)
- **Moreno Camacho, Jorge Miguel**
  28224 Pozuelo, Madrid (ES)
- **Martinez Hernandez, Pedro**
  48005 Bilbao (Vizcaya) (ES)
- **Gomez-Acebo Dennes, Gonzalo**
  28034 Madrid (ES)
- **De La Cruz Vega, José Manuel**
  48005 Bilbao (Vizcaya) (ES)
- **Diaz Martin, Javier**
  48005 Bilbao (Vizcaya) (ES)
- **Cantero Brandes, Mario**
  48005 Bilbao (Vizcaya) (ES)
- **Clemente Simon, Ivan**
  48005 Bilbao (Vizcaya) (ES)

(74) Representative: **Ungria Lopez, Javier et al**
Avda. Ramon y Cajal, 78
28043 Madrid (ES)

(54) System and process for remote payments and transactions in real time by mobile telephone

(57) A system and a process for processing payments and transactions between payers (13) and payees (27, 29, 14, 14a, 13a, 46) associated to the system, using a first server (20) interconnected with telecommunication means (18, 19, 28, 47) with

first data storage means (22) containing information on each associated payer (13) consisting of at least an admissible telephone number, at least a authorization criterion for authorizing a transaction, and a safety criterion associated to the admissible telephone number, as well as an admissible identification code of each payee;

- second data storage means (21) that contain a second information referring to the type of digital mobile telephone (16, 41) belonging to each telephone number;
- selecting means (20h) for verifying one of the telecommunication equipments (18, 19) that communicates with the digital mobile telephone (16, 41) identified by the admissible telephone number by means of a telecommunication service being compatible with the type of digital mobile telephone (16, 41) as identified.

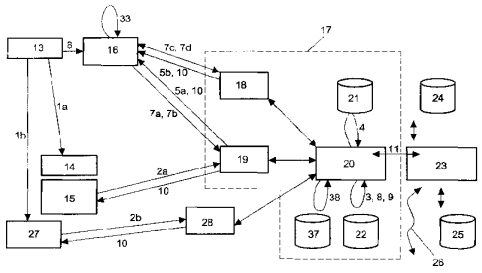


FIG. 1

EP 1 136 961 A1

Petitioner Askeladden LLC
Exhibit 1002 - Page 32 of 350

Description

TECHNICAL FIELD OF THE INVENTION

[0001] The present invention is applicable to the industrial field of electronic transactions related to businesses and means of payment and in the field of mobile telephones.

BACKGROUND OF THE INVENTION

[0002] In prior art there is known the use of payment processes and systems by means of a mobile telephone which are based on the use of a point of sale terminal, to which a mobile telephone is added in order to carry out the transactions.

[0003] In this sense, European patent application EP-A-0940783 or U.S. Patent US-A-5754655 can be cited.

[0004] Furthermore, systems are known in which a mobile telephone does not form part only of a point of sale terminal, but also payment is made by means of a mobile telephone, for which purpose the mobile telephone has to be modified so that safe transactions can be carried out. In this sense we can cite European patent application EP-A-0785534.

[0005] Other systems are based on transmitting the number of the payer's bank account to a payment collector by means of a connection from the collector's mobile telephone to a bank, such as the case of patent application WO-A-96/13814 or patent application WO-A-97/45814.

[0006] These systems have the inconvenience that the user must inform a person that he might not know, on his bank account number, which represents a very high risk.

[0007] French patent application FR-A-2779896 which describes a process wherein payment is carried out by means of the identification of the buyer should also be pointed out which process consists of ensuring that said buyer is a subscriber normally subscribed to a list of subscribers of the communication network.

[0008] This process has the inconvenience that the confirmation of the transaction is first made from the payment server to the businesses server and then from the store's server to the buyer, whereby the payment server cannot certify that the confirmation of the transaction has been transmitted to the buyer. Furthermore after the buyer decides to make a purchase, communications can only be held between the server of the means of payment and the store's server, which implies that the buyer and the seller are customers of the server of the means of payment so that this latter server can compensate his account.

[0009] Another document is European patent application EP-A-0986275 that refers to a method to carry out a transaction between a buyer, who has a mobile telephone, and a seller, both being subscribed to a validation platform. In order to carry out the transaction, a contact is established between the buyer and the seller, and a purchase agreement is reached; then, the buyer transmits a confirmation message that includes the buyer's identification. A copy of the purchase confirmation is transmitted, automatically, to the validation platform, from the buyer or from the seller.

[0010] Mention can also be made of PCT application WO-A-98/54678 which refers to a system in order to activate a petrol pump by means of a mobile telephone. In order to fill up the tank, the buyer makes a telephone call from his mobile telephone to a unit, and introduces a first secret code. The unit verifies the buyer's telephone number and the first secret code, it verifies that the code corresponds to the telephone number and it verifies whether the buyer thus verified is on a "black list". If the verified buyer is not on the "black list", he is granted access to the system and the buyer can enter the code identifying a specific petrol pump in question and can fill up the tank.

[0011] European patent application EP-A-0950968 describes an electronic trading system that includes a mobile terminal which can be provided with means for carrying out a wide range of operations (payment card, telephone card, electronic ticket for shows, etc.)

[0012] PCT application WO-A-98/47116 that refers to a payment system using a mobile telephone can also be cited. In this case the payer transmits information that identifies him/her, and information regarding the amount of the transaction and an identifier of the seller, to the transaction center.

[0013] The abstract of the publication of Japanese application JP-A-08/249530 that describes a way of operating a vending machine by means of a mobile telephone can also be cited.

[0014] French patent application FR-A-2780800 refers to a mobile telephone payment system that includes the transmission of data that identify a seller from a payer's mobile telephone.

[0015] German patent application DE-A-19806557 describes a system for indicating expenses.

[0016] PCT application WO-A-98/06214 refers to a system for alerting the holder of a credit card, payment card, mobile telephone or the like, about fraudulent use thereof. For example, when an attempt is made to carry out a transaction using a credit card in a terminal of a point of sale, the system detects that an attempt to use the credit card is being made and a warning is sent to a telecommunications device, such as a mobile telephone, of the holder of the card, so that the holder thereof can authorize or refuse the transaction, or simply so that the holder thereof may be informed about the transactions carried out.

[0017] None of the cited documents permits selection of a specifically suitable communication equipment, by selecting the suitable communication channel depending on the user's type of mobile telephone, in such a way that payment can be made by a plurality of types of mobile telephones, without changing the structure or parts

Petitioner Askeladden LLC
Exhibit 1002 - Page 33 of 350

thereof.

[0018] On the other hand, none of the cited documents consider the possibility of carrying out the certification of the purchase of Intellectual Property, nor the inclusion of an electronic delivery note, nor the purchase from vending machines.

OBJECT OF THE INVENTION

[0019] The invention in question has the purpose of solving the inconveniences of prior art by means of a system and a process, which allows the use of any mobile telephone as a means of payment: purchases in person, i.e. when the user goes directly to the store; purchases by Internet of goods as well as of Intellectual Property, for example information, music or video games; purchases from vending machines; purchases and reservations in advance; purchases by catalogue; purchases in response to any type of commercials or advertisements, such as for example, television commercials or written advertisements; pay per view; and to allow transactions between users, and all of this irrespective of the type of mobile telephone that the users have. Due to the design of the system, it is applicable for any other type of purchase. Transactions are carried out in real time.

[0020] The invention permits payment to be made from any type of digital mobile telephone, hereinafter referred to as "mobile telephone", without the mobile telephone having to be modified which permits any user who has a mobile telephone to hire the group of payment functions and services; and all of this without the use of credit cards, and without the need of the user having to be necessarily a client of a bank. For this purpose a transaction and payment center is provided for and this center is provided with the different mobile communication capacities with the corresponding equipment and means for identifying from what type of mobile telephone payment is being requested or made, and thus allow the transaction and payment center to make the communication with any mobile telephone by means of the corresponding mobile telephone equipment.

[0021] It should be emphasized that the invention also permits a purchase receipt to be obtained, even in the case of the purchase of Intellectual Property by Internet. Furthermore, confirmation of delivery of previously purchased goods, certifying the delivery without the need of the seller to hand over a delivery note is achieved by means of the invention.

[0022] The invention may be implemented in all countries having a mobile telephony network, and especially in those countries where a nationwide management company has been established. This company will agree with the country's mobile telephone operators on the conditions of providing and operating the service, and payment will be carried out by means of any type of mobile telephone without the need of making variations thereof.

DESCRIPTION OF THE INVENTION

[0023] To achieve the aforementioned objects, the invention provides a system for processing payments and transactions between payers and payees being associated to the system, using at least one communication by digital mobile telephony, the system comprising:

- a first server interconnected with telecommunication means with first data storage means and including account management means that process first data of an account of each associated payer and second data of an account of each associated payee; wherein
- the first telecommunication means selectively communicate the first server with a digital mobile telephone unit identified by an admissible telephone number of an associated payer and with a telecommunication terminal identified by an admissible identification code of an associated payee; the telecommunication means comprising a plurality of telecommunication equipments;
- the first data storage means contain first information on each associated payer, said first information comprising at least the admissible telephone number, at least a pre-established authorization criterion for authorizing at least one transaction that requires a payment from the associated payer's account and at least a safety criterion associated univocally to the associated payer's telephone number, as well as some second information on each associated payee that comprises at least the admissible identification code; the first server comprising
- first verifying means for verifying in the data storage means whether a first message received through the telecommunication means contains an admissible telephone number of an associated payer and an admissible identification code of an associated payee, said first verifying means generating a first acceptance message when they detect an admissible identification code and an admissible telephone number;
- second verifying means for verifying in the data storage means whether a transaction authorization request received through the telecommunication means in addition to the admissible telephone number detected by the first verifying means, satisfies said pre-established authorization criterion, said second verifying means generating a second acceptance message when the authorization request satisfies said authorization criterion;
- third verifying means for verifying in the first data storage means whether a safety parameter received through the telecommunication means satisfies the safety criterion associated to the admissible telephone number detected by the first verifying means, said third verifying means generating a third acceptance message when they detect that the

Petitioner Askeladden LLC
Exhibit 1002 - Page 34 of 350

safety parameter satisfies the safety criterion associated to the admissible telephone number;

- authorization means for authorizing the account management means on the basis of the authorization request, to process a debit in the associated payer's account and to process a corresponding credit in the associated payee's account as long as the first, second and third acceptance messages have been generated;
- rejection message generating means for generating a rejection message when at least one of the acceptance messages has not been generated, and for transmitting the rejection message to the telecommunication means;
- confirmation message generating means for generating at least a confirmation message when at least one of the acceptance messages has been generated, and for transmitting said confirmation message to the telecommunication means, and for selective transmission of the confirmation message to the mobile telephone identified by the admissible telephone number in said first message, and to the telecommunication terminal identified by the admissible identification code;
- second data storage means that contain at least first information referring to the admissible telephone number of each payer, and at least second information referring to the type of digital mobile telephone belonging to each telephone number;
- selecting means for verifying in said second data storage means, the second information corresponding to the digital mobile telephone unit identified by the admissible telephone number and for selecting one of the telecommunication equipments that communicates with a digital mobile telephone identified by the admissible telephone number by means of a telecommunication service being compatible with the type of digital mobile telephone identified in said second information.

[0024] In an embodiment of the invention, each second information contained in the second data storage means and referring to the type of digital mobile telephone corresponding to each admissible telephone number of each associated payer and each admissible identification code of each payee when the latter is a number of a digital mobile telephone, is a first identifying code being representative of the International Mobile Equipment Identifier (IMEI).

[0025] The incorporation of the IMEI codes on the basis of which, according to this embodiment, the types of mobile telephones corresponding to each of the admissible telephone numbers are identified, may be made by loading data from a source being alien to the system or, alternatively or complementarily, by inquiry and updating means being present in the system. This, the first server may comprise first inquiry means for inquiring in at least one Visitor Location Register (VLR) comprising a first register relating telephone numbers with an IMEI code, the IMEI code corresponding to each of the admissible telephone numbers, and updating means for updating said second information in the second data storage means by comparing each IMEI code inquired by the first inquiry means with each code being representative of the IMEI code associated to each admissible telephone number as contained in the second data storage means.

[0026] Alternatively or complementarily, the first inquiry means may also extract the IMEI codes associated to each admissible telephone number,

* from an Equipment Identifier Register (EIR) that contains an association between each admissible telephone number and the IMEI code corresponding to each admissible telephone number, and which receive said association from each Visitor Location Register as updated by said Visitor Location Register;
* from an Unstructured Supplementary Service Data (USSD) frame into which each Visitor Location Register associated to each Mobile Switching Center (MSC) which has issued said frame, has inserted the IMEI code associated to the admissible telephone number corresponding to the user who has originated said frame;
* through an interface between the Visitor Location Register and said inquiry means; and/or
* by third inquiry means for inquiring in a data bank of a mobile telephony network operator, registers that each Mobile Switching Center (MSC) transfers immediately each time a USSD frame or a voice call is addressed to a specific telephone number, said registers containing a relation of each telephone number from which a call was made or originated the USSD frame with an IMEI code of the terminal from which said call or frame originated, in respect of the IMEI codes corresponding to each admissible telephone number, and by third updating means for updating said second information in said second data storage means on the basis of a comparison of each inquired IMEI code inquired by the third inquiry means with each code being representative of the IMEI code associated to each admissible telephone number contained in the second data storage means.

[0027] Also alternatively or complementarily, the first server may comprise second inquiry means for inquiring the IMEI code corresponding to each admissible telephone number, in Call Data Registers (CDR) of a data bank of a mobile telephony network operator, that contain a relation of each telephone number which, on the grounds of a call, has originated a Call Data Register with an IMEI code of the terminal from which said call originated, and by second updating means for updating said second information in the second data storage

Petitioner Askeladden LLC
Exhibit 1002 - Page 35 of 350

means on he basis of a comparison of each IMEI code inquired by the second inquiry means with each code being representative of the IMEI code associated to each admissible telephone number, contained in the second data storage means.

[0028] On the other hand, the information on the type of mobile telephone corresponding to each admissible telephone number stored in the second data storage means, may also be complemented with other data, as for example, at least one datum being indicative of a communication capacity selected from a capacity of managing sessions according to Wireless Application Protocols (WAP), a capacity of managing sessions of Unstructured Supplementary Service Data (USSD), and combinations thereof, of each digital mobile telephone identified by an IMEI code and associated to an admissible telephone number.

[0029] The presence of the second data storage means has the advantage that the system, on the basis of comprising information o the types of mobile telephones of the associated payers and, in some cases, of associated payees, is capable of selecting the communication channel being the most efficient and quick one for communicating with a payer, this being especially important when the first message, i.e. the first communication regarding a transaction, has not been established from the mobile telephone of an associated payer, because thus a fast and efficient communication may be established without the mobile telephones of the users needing to be modified.

[0030] The admissible identification code of each payee may be selected among a telephone number, a number related to a telephone number, an Internet code, a code representative of an Internet code, an e-mail address, and a code based on an e-mail address. The admissible identification code of a payee may also be that of a digital mobile telephone the admissible telephone number and type of which are comprised in the second data storage means. In this latter case, the first server further comprises complementary verifying means being associated to the selecting means, for verifying if the admissible identification code that has been verified by the first verifying means in said first message received from a payer identified by a first admissible telephone number and containing a transaction request that has been verified by the second verifying means, corresponds to a second admissible telephone number from among the admissible telephone numbers of a digital mobile telephone comprised within the first information contained in the first data storage means. Thus, when said verifying means detect that the first message identifies the second admissible telephone number as identification of a payee, the complementary verifying means generate a fourth acceptance message being processable by the confirmation message generating means. On the other hand, the rejection message generating means generate a rejection message when the fourth message has not been generated.

[0031] Also, the admissible telephone numbers of each or of at least a part of the payers, may be contained in the first and/or second data storage means as such and/or in the form of a code being representative of said numbers, such as for example as MSISDN associated to an admissible telephone number, such the first verifying means verify the payer's admissible telephone number from said code representative of said admissible telephone number and contained in the first data storage means, as received through the telecommunication means. In accordance with the invention, the second acceptance message may be designed such that emission thereof generates an order to the telecommunication means, to transmit to the mobile telephone of a payer identified by the admissible telephone number, a first confirmation message that contains a request to transmit the safety parameter that is to be verified by the third verifying means against the safety criterion. This embodiment is applicable when the first message does not contain a safety parameter which is always the case when the first communication regarding a transaction has been established by a payee, and in those cases where a payer, in his/her first communication, has not yet transmitted a safety parameter. Thus, when the first message verified by the first verifying means is a message received from the telecommunication terminal of a payee, the second acceptance message generates an order to the telecommunication means to establish communication with the mobile telephone for requesting the payer identified by the admissible telephone number to transmit the safety parameter. On the other hand, when the first message verified by the first verifying means is a message received without a safety parameter from the mobile telephone of a payer, the second acceptance message generates an order to the telecommunication means, to transmit a message to said mobile telephone requesting the payer identified by the admissible telephone number to transmit the safety parameter.

The second message may be also designed to further generate an order to the telecommunication means to communicate with the telecommunication terminal identified by the admissible identification code detected by the first verifying means, to transmit a second confirmation message that confirms the generation of the first acceptance message.

On the other hand, the third acceptance message generates an order to the telecommunication means to communicate with the telecommunication terminal identified by the admissible identification code detected by the first verifying means to transmit a third confirmation message that confirms the generation of the third acceptance message.

[0032] The third acceptance message generated by the third verifying means may be further designed to generate an order to the telecommunication means, to communicate with the mobile telephone identified by the admissible telephone number detected by the first verifying means, and to transmit a fourth confirmation mes-

Petitioner Askeladden LLC
Exhibit 1002 - Page 36 of 350

sage that confirms the generation of the third acceptance message, such that the payer receives a confirmation that the transaction has been authorized.

[0033] In an advantageous embodiment of the invention, the third acceptance message generated by the third verifying means generates a command to the account management means to process the debit in the payer's account and to process the corresponding credit in the payee's account.

[0034] At their end, the account management means control at least a first intermediate account of each payee contained in the first data storage means and in which each credit is made, and, in an advantageous embodiment of the invention, the account management means comprise first transmission means for transmitting said credit to an administration and management server that comprises a payees' data bank in which all credits made in favor of each payee are stored, the administration and management server transferring the credits contained in the data bank to financial entities that manage each payee's financial accounts.

On the other hand, the account management means advantageously may also be designed to control second intermediate accounts selected from prepayment accounts, such as accounts based on an electronic purse previously created in the first data storage means for each payer who has previously "loaded" this purse by means of a payment in an analogous manner to how conventionally electronic purses are loaded, for example, in payment cards or telephone cards, real time debit accounts having a performance being analogous to that of debits charged by banks on the grounds of payments made with debit cards, and post-payment accounts being analogous to bank accounts which are charged with payments made with credit cards. Each intermediate account of each payer is associated to a pre-established authorization criterion which is verified by the second authorization means. The authorization criterion may be, for example, an available balance in an intermediate account, a maximum credit limit and combinations thereof.

[0035] On the other hand, in an advantageous embodiment of the invention, the account management means comprise second transmission means for transmitting said debit to an administration and management server that comprises a payers' data bank wherein all debits made against each payer are stored, the administration and management server transferring the credits contained in the payers' data bank to financial entities that manage each payer's financial accounts., so as to make all required final transactions from the account of each payer to the account of each payee.

[0036] The safety criterion associated to each admissible telephone number and known to the payer identified by the admissible telephone number, may be a secret identification code, such as an alphanumeric code as for example a PIN code, stored in the first data storage means. In this case, the third identification means are designed to verify, in a manner known *per se*, if a safety parameter received from a digital mobile telephone of a payer involved in an transaction, corresponds to said code, by means of one of the following verification methods which are applied according to the kind of safety criterion associated to said admissible telephone number:

* Direct verification of whether the safety parameter contains the secret identification code;
* Verification of whether the safety parameter contains an encrypted result of a self-verification carried out locally in the mobile telephone after direct entry of the secret identification code into the mobile telephone by the payer, by means of decryption means for decrypting the encrypted result, on the basis of the secret identification code stored in the first data storage means.

[0037] In addition to the criteria ad information already described herein before, the first data storage means may further contain, at least in respect of certain payees, complementary information i.e. fourth information associated to said second information and which comprise reference code identifying products or services of a payee as well as a price associated to each product or service. This fourth information is useful in the applications of the system of the invention which will be described hereafter.

[0038] On the one hand the fourth information may be used to calculate the value of a requested transaction and for transmitting to the associated payers information and the products and/or services and/or total prices and/or partial prices of transactions the authorization of which is being or could be or is to be processed, and to thereby request the payer's conformity. Thus, in an embodiment of the invention, the second acceptance message further generates an order to the telecommunication means to transmit at least the value of the transaction, or the total value and a specification of products and/or services, corresponding to the transaction, together with an identification of the payee, which are transmitted together with the message requesting the safety criterion, to the mobile telephone of the payer identified by the admissible telephone number involved in the transaction.

[0039] On the other hand, the fourth information may furthermore comprise a first selectable telephone number, comprised of one of the aforementioned reference codes and an identification code of the corresponding payee, which selectable phone number constitutes the admissible identification, such that purchase of a product or service is enabled by means of the admissible identification codes, such as for example telephone numbers which each univocally identify each product or service, or each group of products or services of a certain payee.

[0040] On the other hand, the fourth information may

Petitioner Askeladden LLC
Exhibit 1002 - Page 37 of 350

further comprise the admissible identification code in the form of an access telephone number to the payee which access telephone number is associated to at least a first menu comprised of the reference codes, the products or services, identified respectively by each one of said reference codes and the price of said products or services.

[0041] In another embodiment of the invention, the first data storage means may group payees who, for example, offer similar products or services, under one same admissible identification code, particularly an admissible access telephone number which, when dialed, provides access to a menu of options wherein the payees grouped under the admissible access telephone number are specified, from which menu the payer may elect at least one payee being in turn identified by an admissible telephone. The menu may be designed in such a manner that, starting from the same, the payer may directly access the elected payee to know the payee's products and/or services, making his/her selection in the menu, or in such a way that election of a certain payee provides access to the payer, to fifth information associated to said second information and analogous to fourth information. This fifth information advantageously comprises reference codes that identify products or services of each one of the payee as well as a price associated to each product or service.

[0042] The system of the present invention is suitable to be used in and adapted to, a plurality of different transactions, such as purchases in person where the payer is staying in the premises, as for example a store, of a payee, purchase of software files by Internet, purchase of products or services with advance payment, delivery of products or services with a delivery receipt, and payment from one person to another.

[0043] Thus, in an embodiment applicable to when a payer wishes to acquire software files such as computer programs, computer games, music, videos etc., the system is designed in such a way that it may process a first message which, in addition to the payer's admissible telephone number, the payees admissible identification code of the payee who, in this case, is a software provider, contains a recipient e-mail address to which the payer wishes the software file to be transmitted by the payee. In this case, the system, in addition to performing the steps which have already been described herein before, operates with confirmation message generating means which additionally generate a further confirmation message that contains a decryption code of the software file, received from the payee in the first server, said further confirmation message being transmitted to the payer's mobile telephone so that the payer may decrypt the software file received at said recipient e-mail address.

[0044] On the other hand, when the system is used for making a purchase with advance payment, the system may be designed in such a way that the first server additionally comprises first detecting means for detecting a first instruction to make a purchase with advance payment and collection code generating means. In this embodiment, the confirmation message generating means further generate a complementary confirmation message that contains the collection code, said complementary confirmation message being transmitted to the payer's mobile telephone and to the payee's telecommunication terminal. Thereby, the payer or a person in which the payer has delegated, may receive the acquired product or service from the payee, by indicating to the payer the collection code.

[0045] In an embodiment of the system being applicable to transactions where issuance of a delivery receipt is required, the first data storage means further comprise, with respect to each payee, third information associated with said second information and that comprises data regarding products or services corresponding to each authorized transaction, and the first server further comprises second detecting means for detecting a second instruction to manage a delivery in person corresponding to an authorized transaction and received from the telecommunication terminal being a payee's mobile telephone, delivery code generating means for generating a delivery code identifying at least a product or service to be delivered, and identification message generating means identifying said product or service. In this embodiment, the confirmation message generating means further generate an additional message that contains the delivery code, said additional message being transmitted to the payer's mobile telephone and to the payee's mobile telephone and the identifying message being transmitted at least to the payer's mobile telephone along with a request to transmit the safety parameter. For managing the delivery, the system comprises delivery management processing means that, when the third verifying means have verified that the safety parameter satisfies the safety criterion associated to the payer's mobile telephone, generate an entry in a delivery note data, which, preferably, is inquirable by the payees for which such delivery notes have been generated.

In an embodiment of the invention applicable to transactions relating to purchases of associated payers in vending machines, the second information in the first data storage means comprises identification codes of a plurality of vending machines each one of which includes a digital mobile telephone as a telecommunication terminal, identified by a mobile telephone number as an admissible identification code, an authorization code associated to the admissible identification code of each vending machine and an activation code for activating the vending machine, associated to each authorization code that activates the vending machine for receiving a request from the payer identified by the admissible telephone number. In this embodiment, the confirmation message generating means generate, when the first, second and third verifying means have respectively generated the first, second and third acceptance mes-

Petitioner Askeladden LLC
Exhibit 1002 - Page 38 of 350

sage, and transmit the confirmation message that comprises at least the code for activating the vending machine and the admissible telephone number of the payer's mobile telephone. So that the payer may select and extract a product which he/she wishes to acquire at the vending machine, this embodiment may. depending on the pre-established conditions stored in the first data storage means, adopt one or both of the following configurations:

[0046] In accordance with the first of these configurations, the confirmation message generating means establish a communication between the payer's mobile telephone and the vending machine, for a pre-established period of time during which the payer can transmit, through the first server, a selection message to the vending machine. In this configuration, the server further comprises deactivation detecting means for detecting deactivation of the vending machine.

[0047] In accordance with the second configuration, the confirmation message generating means in the first server, close the communication with the vending machine after having transmitted the confirmation message, so that the payer may make his selection directly by means of the selection display or a keyboard of the vending machine.

[0048] In view that in the great majority of the cases the products dispensed by vending machines have only low prices, in this embodiment the authorization criterion associated to the admissible telephone number of each vending machine is a direct authorization code that establishes a maximum limit selected from an economic value and a number of dispensing requests, admitted in a specific period of time in respect of requests made from the same mobile telephone, such that the confirmation message generating means generate the confirmation message when the direct authorization code has been detected. Thereby, the need of the second verification means having to access the first data storage means for verifying the authorization criterion being specifically assigned to the payer is avoided and, thus, a greater speed and a lower cost of the transaction is achieved.

[0049] In this embodiment, the first server preferably further comprises recording means associated to the authorization means, for recording transactions recorded in each vending machine.

The system of the invention may be also adapted for enabling payment transactions from one associated user to another, for which purpose the system may be designed in such a manner that the confirmation message generating means generate, when detecting the first, second, third and fourth acceptance message, a first confirmation message containing an identification of the payer, an identification of the transaction and a petition for conformity to the payee identified in the first message. Said petition for conformity further comprises a request of transmission of the safety parameter which said confirmation message transmit to the mobile telephone of the payee identified by the second admissible telephone number through the telecommunication means selected by said selecting means. In turn, the third verifying means furthermore verify if the safety parameter transmitted from the mobile telephone in response to the petition for conformity, satisfies the safety criterion associated to the second admissible telephone number, and generate a fifth acceptance message when said parameter satisfies said safety criterion, whilst the authorization means authorize the account management means when said fifth acceptance message has been generated, whereafter the confirmation message generating means generate and transmit a second confirmation message to the mobile telephone of the payer and to the mobile telephone of the payee.

[0050] Preferably, at least the first server with the before describe means, is integral with a transaction and payment center.

[0051] On the other hand, the present invention also relates to a process for processing payments and transactions between payers and payees associated to the hereinabove described system, by using at least one mobile telephony communication, which process particularly comprises the steps of

- selectively receiving, through telecommunication means, in a payment and transaction center, a first message a first message comprising the number of a mobile telephone of a payer or an identification code of a payee, and, furthermore,
- receiving the amount of a purchase or of a code identifying a product or service, in the payment ad transaction center,
- verifying if the first message originates from a payer identified by an admissible telephone number or an admissible identification code of a payee;
- verifying if conditions of a transaction requested in the first message, satisfy transaction criteria stored in first data storing means;
- verifying the type of digital mobile telephone associated to the admissible telephone number, in second data storage means, and selecting one telecommunications equipment for communicating with the digital mobile telephone identified by the admissible telephone number, through a telecommunications service being compatible with the type of digital mobile telephone identified by the admissible telephone number;
- checking "on line", in the first data storage means, if the payer has a disposable balance in a previously created electronic purse in said transaction and payment center;
- requesting the payer identified in the first message, when the transaction condition is satisfied and there is a sufficient disposable balance for authorizing the transaction, to introduce into the mobile telephone identified in the first message, and to transmit, a safety parameter;

Petitioner Askeladden LLC
Exhibit 1002 - Page 39 of 350

- verifying in the first data storage means, if the safety parameter introduced into and transmitted by, the mobile telephone of the payer, satisfies a safety criterion univocally assigned to said mobile telephone;
- authorizing and carrying out the transaction as requested when the safety parameter satisfies the safety criterion; and
- sending a confirmation that the transaction has been carried out, to the mobile telephone of the payer and to the payee.

[0052] All these steps are common for the different embodiments of the invention and in the event that the buyer makes a purchase in person, in other words, directly at the seller's store, the seller is the one who starts the transaction, and the identification of the buyer is done_by means of the seller transmitting the buyer's mobile telephone number to the transaction and payment center.

[0053] In this case the identification of the seller is done implicitly by means of the communication that is established with the transaction and payment center in order to transmit the buyer's mobile telephone number along with the amount of the purchase or identification code of the product that is being purchased. This communication is carried out by means of a connection between a seller's mobile telephone and the transaction and payment center.

[0054] Therefore, the process of the invention comprises a step in which the buyer provides his telephone number to the seller. This step is carried out directly, by the buyer verbally informing the seller of his telephone number, or by means of reading a support that contains the buyer's telephone number. Obviously the buyer can communicate his mobile telephone number by any process and conventional device with an equivalent function.

[0055] After having verified the identity of the buyer and of the seller, verifying that both have been subscribed to the transaction and payment center, the process of the invention comprises the step of transmitting, to the buyer's mobile telephone by means of a connection from the transaction and payment center, a confirmation re-quest that he agrees with the collection order or re-quested transaction, that was carried out by means of the prior transmission of the amount of the purchase or identification code of the product that is being purchased. The data of the transaction are included in this request.

[0056] Then the buyer confirms the collection order by means of entering and transmitting his secret identification code, by means of his mobile telephone, to the transaction and payment center, wherein it is verified.

[0057] In order to carry out the communication between the transaction and payment center and the buyer's mobile telephone, it has been provided for that the process comprises a consultation step, on the part of the transaction and payment center, of a data base provided therein, a data base that contains the characteristics of each buyer's mobile telephone and from this consultation mobile telephone communication equipment is selected from among the following, equipment that are included in the transaction and payment center itself:

- Short Message Centers (SMC), from which the Short Message Service (SMS) defined in the ETSI specifications 03.38, 03.40, 04.11, 09.02, is permitted/carried out. By means of this system it is possible to exchange messages of up to 160 characters between mobile telephones or between mobile telephones and applications. Common short message centers, as well as specifically designed message centers will be used for the present transaction and payment system in order to permit synchronous communication between mobile telephones and the transaction and payment center. Said centers will be used in all short message communications ended in a mobile telephone.
- Unstructured Supplementary Service Data (USSD) Centers defined in the ETSI specifications GSM 02.90, 03.90, 04.80 and 04.90, by means of which it is possible to establish continuous and interactive text dialogues between a mobile telephone and an application, started by the user of the mobile telephone (MAP step 1 and 2) as well as by the application (telephones MAP step 2), by means of the use of the so-called USSD operations.

[0058] The above-mentioned USSD operations as well as the short message service make use of the Stand-alone Dedicated Control Channel (SDCCH) in the interface between the mobile telephone and the base station, of the Direct Transfer Application Part (DTAP) operations from the base station to the Mobile Network Switching Center (MSC), and of the Mobile User Application Part (MAP) operations between the MSC and the USSD centers and short message centers respectively.

[0059] - By means of Wireless Application Protocol (WAP) that permits communication between mobile telephones provided with suitable software and resident applications in Internet nodes, according to the specifications of the WAP Forum (http://www.wap-fprum.org), using the short message or data services as transport in the cases of GSM networks.

[0060] Therefore, the invention permits the exchange of information between the transaction and payment center and the different types of mobile telephones, without the mobile telephones having to be modified, in such a way that payment can be made by any type of mobile telephone.

[0061] The updating of the data base which includes the characteristics of each buyer's mobile telephone is done automatically for which purpose the transaction and payment center consults the nodes of the mobile telephone network.

Petitioner Askeladden LLC
Exhibit 1002 - Page 40 of 350

[0062] In the secret identification code verification process, some of the following mechanisms intervene:

- Authentication and GSM ciphering that is based on the authentication center of the GSM network in which a Ki secret authentication code of each user resides. This same code resides inaccessibly in the user's Subscriber Identification Module (SIM). For access to the GSM network, the authentication center generates a RAND random number of 128 bits, a number which entered in the non-standard algorithms A3 and A8, together with Ki code, respectively produce a SRES parameter and a Kc session code. These parameters are stored in a Visitor Location Register (VLR) of the authentication center transmitting the RAND random number to the SIM where the same process is carried out: the SRES parameter is returned to the network, which authenticates the user, and the Kc session code is stored in the mobile terminal. From this moment the communication of the mobile telephone with the Base Station Controller (BSC) is ciphered using the algorithm A5 with the Kc code.
- Authentication and ciphering by means of software included in the SIM Toolkit Card, which is a programming model of the SIM cards, described in the ETSI specifications GSM 11.11 and 11.14. Irrespective of the application of GSM ciphering that all the SIM cards carry out, SIM applications that carry out the same management of digital certificates that is presently carried out in personal computer applications, can be developed.
- Authentication and ciphering by means of software in the mobile telephone, in the event that the mobile telephone has the necessary processing capacities, the above-mentioned management of digital certificates can be carried out in the mobile telephone itself.

[0063] The result of the local verification, just as it has already been indicated, is sent to the transaction and payment center in these last two cases.

[0064] Furthermore for a purchase in person, after verification, in the transaction and payment center, that the secret code is correct, the process comprises a step of subtracting the amount of the transaction from the buyer's purse, and once the confirmation of the transaction has been made to the buyer and to the seller, and after a certain amount of time, there is a step for updating the data of the transaction carried out, which leads to credit to the stores and debit to the buyers, in terms of the type of payment chosen. Two types of payment have been defined by means of which the user of the service will be able to pay the amount of his purchases:

- Prepayment: The buyer previously charges an amount of money in his purse previously open in the transaction and payment center. Once the purchases are made, the amount thereof is subtracted from this account in real time.
- Post-payment: The amount of purchases made during a month are entered in the user's purse and the total thereof will be billed monthly in the current account indicated by the user.

[0065] In both cases secondary accounts may be associated to a main account, in such a way that several users, each one provided with his own mobile telephone and each one associated to a secondary purse, may use the service, in which a single holder appears.

[0066] By means of the process of the invention, there is also the possibility of making a purchase in advance, in which case the process is identical to the one described for the purchase in person, with the difference that the buyer provides his telephone number to the seller by means of a connection of the buyer with the seller's service center or automatic sale system, from which the seller transmits the amount of the purchase or identification code of the product that is being purchased to the transaction and payment center.

[0067] Then the transaction and payment center transmits to the seller, a collection code along with the amount of the purchase or identification code of the product that is being purchased.

[0068] Furthermore, after subtracting the amount of the purchase from the buyer's purse, the confirmation is transmitted to the buyer so that the order collection code is transmitted to the buyer, and the stipulated delivery time of the purchase that is being made is also transmitted.

[0069] In this way, when the buyer is going to collect the purchased product, the collection code constitutes the receipt code, that guarantees that payment has been made and furthermore it represents the product that is going_to be delivered to the buyer.

[0070] The invention also permits purchases to be made by Internet, in which case the store is a conventional virtual store that is communicated by Internet or by any type of network, with the transaction and payment center.

[0071] In this case the process is exactly the same as the one described for a purchase in person, but with the difference that the buyer transmits his telephone number to the virtual store by Internet.

[0072] In the event that the purchase by Internet is done from a mobile telephone with WAP capacity, the buyer's telephone number will have been implicitly communicated to the seller upon establishing the communication between both, and the collection order is communicated to the buyer, either by the processes described for a purchase in person, or else by the WAP communication established between the transaction and payment center and the buyer's mobile telephone.

[0073] The invention also permits a purchase to be made from vending machines, in which case the proc-

Petitioner Askeladden LLC
Exhibit 1002 - Page 41 of 350

ess is exactly the same as the one described for a purchase in person with the difference that now it is the buyer who starts the transaction by means of a connection between his mobile telephone and the transaction and payment center, in such a way that identification thereof is carried out implicitly by the connection made; and the identification of the vending machine (seller) is made by transmitting an identification code of the machine associated to it, on the part of the buyer, by means of the connection made. For this purpose the vending machine should include a mobile telephone.

[0074] Once the transaction and payment center has verified the identity of the buyer and of the vending machine, a connection is made with said vending machine transmitting an activation signal thereof. This connection is made by a mobile telephone that is included in the vending machine, which after activation carries out the following steps: displaying the buyer's identity on a screen, which permits the buyer to select/choose the product, and then the product is dispensed.

[0075] In an embodiment of the invention, the charge orders accumulated in the vending machine are periodically questioned by the transaction and payment center which processes all accumulated orders for.

[0076] When the process of the invention is applied to a vending machine, the phases and means already described herein above in respect of the system of the invention, are used.

[0077] The invention also permits the purchase of Intellectual Property i.e. software files as mentioned herein above, to be made by Internet, for which purpose the buyer provides his mobile telephone number to the store on line, in this case a virtual store; and the collection transaction is started from this store just as it has been described in the case of payment by Internet, with the difference that in this case after clearing the files encrypted in the buyer's equipment, the buyer requests the decryption codes from the transaction and payment center, these codes being generated by the seller and transmitted along a safe channel to the transaction and payment center, which determines the acknowledgment of the files and therefore delivery thereof, comprising the subsequent transmission step, on the part of the transaction and payment center, of the decryption codes to the buyer's mobile telephone, which constitutes the verification of delivery of Intellectual Property.

[0078] The invention may further be used to carry out functions of an electronic delivery note, in which case the seller carries out the connection between his mobile telephone and the transaction and payment center, in such a way that the seller is implicitly identified by the connection made wherein the identification code of the product that is going to be delivered is transmitted, in such a way that after making said identification the seller requests a control number from the transaction and payment center, in order to make the delivery of a product to the buyer. Then the transaction and payment center by means of a connection with the buyer, transmits it the control number requested by the seller, as well as the product that is going to be delivered, and then his secret code is requested, which after being entered by his mobile telephone, this implies acknowledgment of the delivery and acceptance of the product.

[0079] In this way the physical receipt is replaced by the described process, permitting automation of the seller's logistic control eliminating paper, for which purpose a data base accessible to the seller is provided for.

[0080] In respect of this latter case it should be pointed out that the transaction may or may not be accompanied by payment, depending on what has been agreed upon between both parties.

[0081] Obviously, the operational and technical characteristics as described hereinbefore in respect of the system, are also applicable to the process of the present invention and viceversa.

BRIEF DESCRIPTION OF THE FIGURES

[0082] The invention will be hereafter be described on the grounds of drawings in which

Figure 1 is a functional block diagram of a possible embodiment of the system of the invention for making a purchase in person, a purchase in advance, and a purchase by Internet,

Figure 2 shows a functional block diagram of a possible embodiment of the system of the invention in order to make the purchase from a vending machine,

Figure 3 shows a functional block diagram of a possible embodiment of the system of the invention for purchasing Intellectual Property by Internet,

Figure 4 shows a possible embodiment of a functional block diagram of the system of the invention for carrying out the functions of an electronic delivery note according to the process of the invention,

Figure 5 shows a functional block diagram of a possible embodiment of the system of the invention for making a purchase by catalogue, a purchase in response to television commercials or pay per view,

Figure 6 shows a functional block diagram of a possible embodiment of the system of the invention in order to carry out a transaction between users,

Figure 7 shows a schematic representation of an embodiment of the interrelation of the various means constituting the first server included in the transaction and payment center represented in the preceding figures.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0083] A description is made hereinafter of the invention on the grounds of the above-cited figures.

[0084] Figure 1 illustrates the process for purchases in person, in other words the purchases wherein a payer

Petitioner Askeladden LLC
Exhibit 1002 - Page 42 of 350

(13), who in this case is a buyer, goes to the store of the payee (14), who in this case is a seller in order to make the purchase.

[0085] In order to make the purchase it is necessary for the seller (14) and the buyer (13) to be subscribed to a transaction and payment center (17), for which purpose each buyer (13) is assigned a secret code that is related to his mobile telephone number.

[0086] In the purchase in person the buyer (13) communicates, by means of a step (1a), to the seller (14) his Mobile Station International Number Integrated Services Digital Network Number (MSISDN) or a number related thereto, different from the secret identification code. This step (Ia) is carried out either orally or by means of an optical pencil provided for in the equipment of the seller (15), a pencil which reads a bar code of a label or customer's card. For example, this card can be adhered to the mobile telephone (16) of the buyer (13).

[0087] The seller (14), by means of the equipment (15) establishes a communication (2a) with a transaction and payment center (17) in order to request authorization of a transaction. In the communication (2a) a collection order that contains the buyer's (13) MSISDN or the number related thereto is transmitted, as well as the amount of the transaction whose authorization is being requested.

[0088] As an example, the equipment (15) can be comprised of a compact mobile terminal based on a microprocessor which stores the corresponding programming that permits the sale application according to the invention to be made, and that includes a screen, a keyboard and a mobile telephone with USSD step 2 communication capacity, in order to make the different communications with the transaction and payment center (17) by means of a mobile telephone.

[0089] In order to permit the establishment of the communication (2a), the transaction and payment center has USSD mobile communication equipment (19) by means of which the communication (2a) with the mobile telephone of the seller's equipment is established.

[0090] Moreover, the transaction and payment center (17) has an on line transaction and payment server (20) that includes a data bank (21) for storing the types of the mobile telephones (16) of each buyer (13) and of each seller (14), as well as the telephone number of each one of them; and that also includes a data bank (22) which stores the data referring to the transaction and payment center (17).

[0091] Said data bank (22) also stores first information on each buyer (13) and second information on each seller (14) being subscribed to the payment service materialized by the transaction and payment center (17); for which purpose the data bank (22) stores the buyers' telephone numbers, the secret code that is assigned to each buyer upon being subscribed to the payment service and a code of each buyer being his/her telephone number or a thereto related number. In the event that a number related to the buyer's telephone number is transmitted, this number is also stored in the data bank (22).

[0092] Hence, the server (20) verifies by means of first verifying means (20a) the merchant's identity by means of the source of the communication (2a), since his/her telephone number is implicit in the connection made by the equipment (15), and furthermore it verifies by means of the means (20a) that the buyer's telephone number transmitted, or the number related thereto, corresponds to a subscriber of the payment service and if the verification is correct it generates an acceptance message.

[0093] Furthermore the server (20) verifies by means of second verifying means (20b) a pre-established authorization criterion by verifying the buyer's balance or amount of credit, by means of step (3). The verification of the balance is made in a purse previously opened in the data bank (22) and if the verification is correct, a second acceptance message is generated.

[0094] If the previous verifications provide a positive result and as a result the acceptance messages have been generated, communication with the buyer (13) is established. In this communication the server (20) transmits to the buyer's (13) mobile telephone (16) a collection order confirmation request (5a) or (5b), either by means of the USSD mobile communication equipment (19) (5a) or mobile communication equipment materialized by a Short Message Center (18) (SMC) (5b), depending on the type of mobile telephone (16) owned by the buyer (13), in such a way that communication with any type of mobile telephone that the buyer has acquired, is permitted.

[0095] For the selection of the step (5a) or (5b), the server (20) consults, by means of step (4), the data bank (21), by means of the selecting means (20h), in order to verify what type of mobile telephone the buyer (13) owns and in order to select the equipment (18) or (19) through which the communication is carried out.

[0096] At this stage it should be pointed out that the data base (21) is updated automatically by means of one or more of the possibilities already described hereinbefore in chapter "Description of the Invention", by means of a consultation process of the nodes of the mobile communication network, in which the International Mobile Equipment Identifier (IMEI) of the buyers' (13) mobile telephones (16) are recorded, and from which the system knows said characteristics.

[0097] Figure 7 show, *inter alia,* an embodiment of the first server (20) with a plurality of materializations of inquiry and updating means for inquiring and updating the IMEI codes, in all of which each second information contained in the second data storage means (21) and referring to the type of digital mobile telephone (16,40) contained in the second data storage means in respect of each admissible telephone number of each associated payer (13) and each admissible identification code of each payee (40) (when this latter code is a number of a digital mobile telephone as will be explained herein

Petitioner Askeladden LLC
Exhibit 1002 - Page 43 of 350

below), is a first identifying code being representative of a IMEI code.

[0098] Thus, in a first materialization, the first inquiry means (20r) extract the IMEI code associated to each admissible phone number, from an Equipment Identifier Register (EIR) that contains an association between each admissible telephone number and the IMEI code corresponding to each admissible telephone number, and which receive said association from each Visitor Location Register as updated by said Visitor Location Register.

[0099] In a second materialization, the first inquiry means (20r) extract the IMEI code associated to each admissible telephone number, from an Unstructured Supplementary Service Data (USSD) frame into which each Visitor Location Register associated to each Mobile Switching Center (MSC) which has issued said frame, has inserted the IMEI code associated to the admissible telephone number corresponding to the user who has originated said frame.

[0100] In a third materialization, the first inquiry means (20r) extract the IMEI code associated to each admissible telephone number, through an interface between the Visitor Location Register and said inquiry means (20r).

[0101] In a fourth materialization, the first server (20) comprises second inquiry means (20t) for inquiring the IMEI code corresponding to each admissible telephone number, in Call Data Registers (CDR) of a data bank of a mobile telephony network operator, that contain a relation of each telephone number which, on the grounds of a call, has originated a Call Data Register with an IMEI code of the terminal from which said call originated, and second updating means (20u) for updating said second information in the second data storage means (21) on he basis of a comparison of each IMEI code inquired by the second inquiry means (20t) with each code being representative of the IMEI code associated to each admissible telephone number, contained in the second data storage means (21).

[0102] In a fifth materialization, the second information further comprises at least one datum being indicative of a communication capacity selected from a capacity of managing sessions according to Wireless Application Protocols (WAP), a capacity of managing sessions of Unstructured Supplementary Service Data (USSD), and combinations thereof, of each digital mobile telephone identified by an IMEI code and associated to an admissible telephone number.

[0103] Finally, in a sixth materialization, the first server (20) comprises second inquiry means (20t) for inquiring the IMEI code corresponding to each admissible telephone number, in Call Data Registers (CDR) of a data bank of a mobile telephony network operator, that contain a relation of each telephone number which, on the grounds of a call, has originated a Call Data Register with an IMEI code of the terminal from which said call originated, second updating means (20u) for updating said second information in the second data storage means (21) on he basis of a comparison of each IMEI code inquired by the second inquiry means (20t) with each code being representative of the IMEI code associated to each admissible telephone number, contained in the second data storage means (21).

[0104] Obviously, although figure 7 shows a plurality of materializations coexisting in the first server (20), the system of the invention may comprise only one or some of said materializations.

[0105] In the event that the mobile telephone (16) has USSD version 2 capacities, step (5a) is carried out by means of the transmission of a USSD frame, a process by means of which the connection between the mobile telephone (16) and the server (20) is open. Upon receiving this frame, the mobile telephone (16) displays on the screen the authorization request with the details of the collection order.

[0106] In the event that the mobile telephone (16) does not have USSD version 2 capacities, this request is made by the transmission (5b) of a class 0 short message with the de-tails of the collection order and instructions to transmit the authorization. Upon receiving a class 0 short message, the mobile telephone (16) displays it on the screen, without the need of the user navigating through the structure of menus stored in his mobile telephone. A short message center (18), that is characterized in carrying out synchronous communications, is used to transmit these confirmation request messages.

[0107] Returning to figure 1, it can be appreciated that the buyer (13) confirms the collection order received (5a) or (5b) by entering (6) the secret code that was assigned to him upon being subscribed to the service, by means of the keyboard of his mobile telephone. This identification code can be locally verified, in the mobile telephone, by step (33) in the event that the mobile telephone has SIM card authentication mechanisms. In this case, step (7d) is carried out, a step in which the result of the encrypted local authentication is transmitted to the payment server by means of a short message directed to the above-mentioned synchronous short message center (18). In this case the transaction and payment center decrypts and verifies the result of said verification from the user's secret identification code that is stored.

[0108] If these mechanisms are not available, the secret code is transmitted by using the ciphering of the mobile communication network described in the Description of the Invention, by means of any of the processes indicated hereinafter:

[0109] In the event that it is a mobile telephone (16) with USSD version 1 and 2 capacity, that has received the request by step (5a), the secret identification code that the buyer has keyed in step (6) is transmitted by step (7a) over the connection that was opened in said step (5a).

[0110] In the event that it is a mobile telephone with

Petitioner Askeladden LLC
Exhibit 1002 - Page 44 of 350

USSD version 1 capacity, that has received the request by step (5b), the sequence that the buyer has keyed consists of a USSD service code, followed by the secret code, and it is transmitted by step (7b) in a USSD version 1 operation frame originated in the mobile telephone.

[0111] In the event that it is a mobile telephone without USSD capacity, that has received the request by step (5b), the sequence that the buyer (13) keys consists of the secret code, that is transmitted by step (7c) in a short message, by a response to step (5b), either to a short number assigned to said service by the operator, depending on the buyer's (13) mobile telephone (16) number.

[0112] Then the server (20) verifies by means of third verifying means (20c) the secret code transmitted by the buyer (13). The verification is carried out by means of step (8), and in the event that the verification result is positive, a third acceptance message is generated.

[0113] The server (20) has authorizing means (20d) which when it receives the three authorization messages, it authorizes some account management means (20e) included in the server (20) to subtract the amount of the transaction from the buyer's purse/credit account and to credit said amount to the seller's account by means of step (9); and it transmits the confirmation of the transaction to the seller's (15) terminal as well as to the buyer's (13) mobile telephone (16) by means of steps (10). This confirmation is carried out by means of some confirmation message generating means (20g) included in the server (20). These means (20g) can also confirm to the buyer (13) and/or to the seller (14) the verifications carried out by the means (20a) and (20b).

[0114] Then by step (11) which is an off line step, the data are updated towards an administration and management server (23), from which the subscriber processes are forwarded to the stores and the debits to the buyers, depending on the type of payment selected, by the specific applications built in relation with the financial entities, with which communication is established by means of line (26). In order to carry out this function, the administration and management server (23) has a data bank (24) of the stores, and a data bank (25) of the buyers.

[0115] The server (20) has rejection message generating means (20f), which when at least one of the acceptance messages has not been generated, it transmits a rejection message to the seller and/or to the buyer.

[0116] The operation described is identical for the case in which the purchase is made by Internet, in which case the payer is a buyer (13) and the payee is a virtual store (27) to which the buyer transmits his mobile telephone number, or the number related thereto, by step (1b), by means of the communication between the buyer (13) and the virtual store (27), just as it is conventionally done in this type of purchase, in other words, by Internet.

[0117] Then the virtual store (27) transmits a collection order (2b), equivalent to a previously described collection order (2a), but with the difference that this collection order is transmitted to a network (28) by means of which the communication with the server (20) is established.

[0118] In this case the process is the same as the previously described one, for which purpose the transmission of the confirmation by step (10) is done by the communication network (28).

[0119] The communication network (28) can be Internet, a digital integrated service network, the switched telephone network or any other network.

[0120] These accesses will be provided with the safety mechanisms necessary for each case.

[0121] Furthermore, the process illustrated in figure 1, also permits purchases with payment in advance to be made, for which purpose in this case, the buyer (13) informs the seller (14) of his telephone number by means of a telephone connection with a service center or by an automatic sale system that the seller has operative for this purpose. As of this point the process is the same as the one for a purchase in person, but with the difference that when the seller communicates with the transaction and payment center (17), he transmits along with the data of the transaction and with the buyer's (13) telephone number, an instruction indicating a purchase with payment in advance that is detected by some first detecting means (20i) included in the server (20), which also has a collection code generating means (20j) by means of which a collection code is generated upon detecting said instruction. This code is transmitted to the buyer and seller in step (10), along with the described confirmation of this step 10. In this way, when the buyer goes in person to the seller's (14) store, the previously ordered product, should inform him of the collection code so that the seller may know who the buyer in question is and which product should be handed over to him.

[0122] This operating mode is particularly useful in those stores that produce the production of a product only under the premise that the product is already paid for, for example perishable goods, and therefore, there is certainty that although the product is not collected later on, the price thereof has already been collected. This schema is only possible when the transaction is done on line. The providing of the collection code by the buyer to the seller constitutes the verification that payment has already been made in advance.

[0123] By means of the system and process of the invention, payments can also be made in vending machines, which is illustrated in figure 2.

[0124] In this case the payee is a vending machine (29), which should include a mobile telephone with short message and data communication capacity.

[0125] The buyer (13) reads from the vending machine (29) an identification code of the machine, which has been represented by step (30).

[0126] Then the buyer (13) by means of a communication (31a) or (31b), depending on the type of mobile

Petitioner Askeladden LLC
Exhibit 1002 - Page 45 of 350

telephone (16) he has, as it has already been previously described, transmits the identification code of the vending machine (29) to the server (20).

[0127] This step would be equivalent to step (2a), (2b), described above, but with the difference that the buyer's identification is now carried out implicitly by the connection (31a) or (31b), and the store's identification, in this case the vending machine (29) is carried out by the code transmitted by the buyer.

[0128] The transaction and payment center verifies the customer's identity, his balance or credit limit, the type of mobile telephone (16) and the mobile telephone number that the vending machine (29) is provided with. This is done by steps (3) and (4).

[0129] Steps (5a) (5b), (6), (7a), (7b), (7c), (7d), (8) and (9) are identical to the ones described above.

[0130] Then an activation order (32) of the vending machine is transmitted by the mobile telephone network (equipment 18 or 19). This activation order is carried out by the communication with the mobile telephone of the vending machine (29), for which purpose the transaction and payment center (17) establishes communication with the mobile telephone of the machine, which upon receiving said order, is activated in the same way as if coins had been inserted therein. Along with the activation order of the vending machine (29), the buyer's (13) identification is transmitted, in such a way that the vending machine displays it on a screen and then the buyer selects and obtains the desired product according to step (31). For this purpose the first server (20) closes the communication with the vending machine (20) and allow the payer to make a selection by the display or keyboard of the vending machine (29).

In an embodiment of the system when being applicable to a vending machine, the confirmation message generating means (20g) establish a communication between the mobile telephone o(16) of the payer (13) and the vending machine (29) during a preestablished period of time during which the payer (13) may transmit, through the first server (20), a selection message to the vending machine (29), i.e. the selection of the product is made by means of the mobile telephone (16) instead of by the display of the vending machine. After expiration of this period of time, the communication between the first server (20), the vending machine (29) and the payer (13) is closed.

[0131] There is also the possibility of the first server (20) comprising deactivation detecting means (200) for detecting deactivation of the vending machine (29) which in this case also have the function of closing the communication between the first server (20), the vending machine (29) and the payer (13).

[0132] The vending machine (29) periodically, when it is questioned by the transaction and payment center (17), transmits to the server (20) the record of purchases and the users that have made them, according to step (12). For this purpose, the first server (20) comprises transaction recording means (20p) which record the transactions recorded in each vending machine (29) said recording means being associated to the authorization means (20d).

[0133] Step (10) is carried out upon making the periodic clearance of the purchases made.

[0134] In certain circumstances, such as for example the case in which the amounts of the transaction to be made are low, it could happen that it is not necessary to enter the buyer's secret code, in which case the steps corresponding to this operation would be eliminated.

[0135] The system of the invention is also applicable in_for processing purchases by Internet or other remote channels, which is illustrated in figure 3.

[0136] The buyer (13) (payer) by Internet, provides on line by means of step (1), his/her telephone number to the virtual store (27) (payee). Step (2), that consists of transmitting to the server (20) the collection order that contains the telephone number and the amount of the purchase to be made, is carried out from the virtual store (27) and by means of a network (28). In this operation the server (20) verifies the identities of the buyer and of the seller and generates a connection to the buyer's (13) mobile telephone (16), by means of the equipment (18) or (19) depending on the type of telephone that the buyer owns, in order to transmit a message that informs him of the store's identity, of the amount of the purchase and the secret code is requested according to the steps illustrated in figure 1. After verifying that there is an available balance, the transaction is confirmed to the buyer (13) and to the virtual store (27). Steps (1) to (10) are thus identical to the those already described herein above. Then the virtual store clears on line the software files encrypted in the buyer's (13) computer by Internet according to step (34). When the buyer (13) has received them, the decryption codes are requested from the server (20) by steps (12a) or (12b), depending on the type of mobile telephone. These codes are generated by the seller (27) and transmitted by a safe channel to the server (20) at the request thereof. Then the server's (20) confirmation message generating means (20g) generates a confirmation message that contains the decryption code of the software file that is transmitted to the buyer by means of steps (13a) or (13b), depending on the type of the buyer's (13) mobile telephone (16), and finally, the data are updated in the server (20) and in the administration and management server (23) by means of step (11) off line.

[0137] Furthermore, the system of the invention permits application thereof as an electronic delivery note, which is illustrated in figure 4.

[0138] When a supplier (14a) (payee) makes the delivery to a buyer's (13) premises, the supplier (14a) by a mobile telephone (15a) previously makes a communication (2c) with the transaction and payment center (17) to which the identification code of the product that is being purchased and the buyer's telephone number are transmitted, and furthermore a delivery code such as for example a control number is requested. For this

Petitioner Askeladden LLC
Exhibit 1002 - Page 46 of 350

purpose the seller transmits a second delivery management instruction that is detected by some second detecting means (20k) provided for in the server (20). Once the center (17) verifies the supplier's (14a) identity by the communication (2c), and as of said detection, by means of some generating means (201) of a delivery code, said code is generated and transmitted to the seller by step (35), in such a way that the center (17) identifies the type of the buyer's mobile telephone by step (4) and communicates with it by a connection (36a) or (36b), depending on the type of the buyer's (13) mobile telephone (16) just as it has already been explained. In the communication (36a) or (36b), the buyer (13) receives the data regarding the control number of the product that is delivered and the request of his secret code. For this purpose, the server (20) has message generating means (20m) for identifying said product or service.

[0139] Then the buyer enters his secret code, which implies acknowledgment of the delivery and acceptance of the product. The server (20) verifies that the data are correct by step (8a) in the manner already described in previous examples (step 8). Then by means of delivery management processing means (20n) included in the server (20), a entry is generated in a delivery note data base (37) and the delivery is confirmed to both by step (10). Finally the data of the delivery are updated by step (IIa) off line in the administration and management server (23). The server's (20) data base (37) is accessible to the supplier permitting him to conduct a computer control of the status of his deliveries, a control that bears the digital signature of acceptance of his customers by the transmission of the control number and the secret code. This is done by step (38).

[0140] In this way, the physical receipt that is conventionally handed over to the buyer is replaced by the described process.

[0141] Likewise, this step (38) can be carried out with a purchase in person, a purchase in advance and a purchase by Internet, which were previously described.

[0142] These transaction may or may not be accompanied with payment.

[0143] Figure 5 shows another possible embodiment of making a purchase by a product or a service code, that consists of assigning a code to the product or service in order to make a purchase by catalogue; a purchase in response to any type of commercial or advertisement, such as for example, television commercials or written advertisements, a pay per view, or any other type of purchase in which the indicated possibility is assigned.

[0144] In this case, for making the purchase, once the buyer knows the code assigned to the product that he/she wants to buy, the buyer calls the transaction and payment center (17) with his mobile telephone, establishing a communication (45a) or (45b), depending on the type of mobile telephone that the buyer (13) owns. The communication (45a) is established by means of the mobile communication equipment (19), and the communication (45b) is established by means of the short message center (18), just as it has been explained in the preceding cases.

[0145] By communication (45a) or (45b), the buyer transmits the telephone number corresponding to the product that he wants to buy This telephone number comprises a part indicating the code of the product that he wishes to buy, and another part indicating the seller's identity, and this is stored in the data bank (22).

[0146] At this point, it should be pointed out that, according to a further embodiment of the invention, there is the possibility that the telephone number itself dealt by the buyer for communicating with the transaction and payment center (17), permits access to the code of a series of different sellers, that are stored in the data bank (22), in such a way that when the transaction and payment center receives this telephone call, it has access to said data bank (22) and it transmits a message with the different options of the sellers to the buyer. As of this point, the selection, first of the seller, and then of the product that is to be purchased may be made. According to another embodiment, there is also the possibility that the number dialed by the buyer in order to have access to the transaction and payment center (17) refers to a specific seller, stored in the data bank (22) of the transaction and payment center, in such a way that the transaction and payment center (17) transmits a message with said seller's different products to be selected to the client.

[0147] This structure has the advantage that the user does not need to know the codes of the products, but rather on the contrary, the user can have access to the products of a specific seller, or of several sellers, by phoning a generic telephone number.

[0148] In any case, the selection of the mobile communication equipment (18, 19) for establishing the communication (45a) or (45b) with the buyer, is carried out by means of step (4), in which the server (20) consults the data bank (21), just as it has already been explained, in order to determine what type of mobile telephone the buyer (13) owns.

[0149] Likewise, in this case the server (20) verifies the buyer's identity by means of the source of the communication (45a) or (45b), since his telephone number is implicit in the connection made, and furthermore it verifies that the telephone number of the product corresponds to a seller subscribed to the payment service, and it determines the product that is purchased and the price thereof from the code received. This code, just as it has been indicated can be obtained directly from the number dialed by the buyer, or indirectly from the seller or sellers that the initially dialed telephone number refers to.

[0150] There is the possibility that the data referring to each product of each seller are stored in the equipment of the seller himself (46), in which case the transaction and payment center (17) questions the seller

Petitioner Askeladden LLC
Exhibit 1002 - Page 47 of 350

(46), by means of the communication network (47) that connects them, about the price and product to which the buyer is referring. The seller (46) responds with the adequate data and the transaction and payment center (17) informs the buyer (13) thereof.

[0151] Then step (3) for verifying the balance is carried out in any of the indicated cases, and if the previous verifications give a positive result the previously described steps (5a) or (5b) for confirming the collection order are generated.

[0152] Then the buyer (13) confirms the collection order (5a) or (5b) received, the secret code being introduced by means of the keyboard of his mobile telephone and being verified by means of step (8) from the previously described steps (33) and (7d) or (7a), (7b) or (7c).

[0153] In the event that the result of the verification is positive, the amount of the transactions is subtracted from the buyer's purse/credit account and the amount is credited to the seller's account by means of step (9), and the identification of the buyer and of the purchased product are communicated to the seller (46) by means of a communication network (47) so that the seller sends the purchased product to the buyer's domicile. Furthermore, the confirmation of the transaction is sent by means of steps (10).

[0154] Thereafter, previously described step (11) is carried out.

[0155] By means of the network (47), the seller (46) updates the data base (22) of the transaction and payment center (17) regarding its products, prices and codes that affect them, each time that said sellers make a modification thereof, when these data are stored in said center (17).

[0156] In the event that it is a pay per view, the buyer starts the typical transaction by telephoning the number that appears on the television screen, from which the transaction and payment center (17) communicates with the television broadcasting center that broadcasts the selected decoded program, and to which the buyer who is selecting the purchase of the program is indicated. In other words, it operates just like in the case of delivering a physical product, except that in this case the seller delivers a television signal.

[0157] Figure 6 shows another possible embodiment whereby transactions between users (13) and (40) who own a mobile telephone (16), (41), respectively, and who are obviously subscribed to the transaction and payment center (17) are made possible in the above-mentioned manner.

[0158] In this case the user (13) constitutes a payer, and the user (40) constitutes a payee.

[0159] Hence, when a payer (13) wishes to carry out a transaction in favor of a payee (40), a communication (39a) is established with the short message center (18) or a communication (39b) is established with the mobile communication equipment (19), depending on the type of mobile telephone that the user has.

[0160] In this case, the payment order that contains the payee's (40) telephone number or the number related thereto is transmitted in the communication (39a) or (39b) and furthermore, the amount of the transaction whose authorization is being requested, is transmitted. This may correspond, for example, to a debt that is to be settled, or to a credit that is to be made.

[0161] In this case the transaction and payment center stores the data corresponding to the payee (40) in its data banks (21) and (22), in the same way that it does with the payer (13).

[0162] The selection of the communication equipment in order to establish the communication (39a) or (39b) is carried out by means of step (4).

[0163] The payer's (13) identity and the payee's (40) telephone number are verified by means of the origin of the communication (39a) or (39b) and then, the payer's balance is verified by means of step (3).

[0164] When the previous verifications give a positive result, steps (5a), (6) and (7a), or (5b), (6) and (7b), or (5b), (6) and (7c), and finally step (8) are carried out in the manner that has already been described.

[0165] Then the server (20) transmits a payment order confirmation request (5c) or (5d) to the payee's (40) mobile telephone (41), depending on the type of mobile telephone that the payee (13a) owns. This is selected by means of step 4.

[0166] For the selection of steps (5c) or (5d), the server (20) carries out a process identical to the one described for steps (5a) or (5b), in such a way that steps (7) and (7f) are identical to steps (7a) and (7b), and steps (7g) and (7f) are identical to steps (7c) and (7d).

[0167] Firstly, the server verifies the secret code sent by the payee (40) by means of step (8), and in the event that the result of the verification of both secret identification codes corresponding to the payer and the payee is positive, the amount of the transaction is subtracted from the payer's purse or credit account by means of step (9) and the amount of the transaction is credited to the payee's purse/credit account by means of said step (9) and then, the confirmation is transmitted to the payer (13) and to the payee (40) by means of steps (10).

[0168] Finally, step (11) is carried out in the manner that has already been described.

[0169] Obviously, there is the possibility that the transaction may be started by the payee (40), in which case the process is carried out in the reverse manner from the one described, in other words, the confirmation of the payee's secret code is requested and then the confirmation of the payer's secret code is requested.

Claims

1. A system for processing payments and transactions between payers (13) and payees (27, 29, 14, 14a, 13a, 46) associated to the system, using at least one communication by means of digital mobile telephony, the system comprising

Petitioner Askeladden LLC
Exhibit 1002 - Page 48 of 350

- a first server (20) interconnected with telecommunication means (18, 19, 28, 47) with first data storage means (22), and including account management means (20e) that process first data of an account of each associated payer (13) and second data of an account of each associated payee (27, 29, 14, 14a, 40, 46);

wherein

- the first telecommunication means (18, 19, 28, 47) selectively communicate the first server (20) with a digital mobile telephone unit (16) identified by an admissible telephone number of an associated payer (13) and with a telecommunication terminal (15, 15a, 27, 29, 41, 46) identified by an admissible identification code of an associated payee (27, 29, 14, 14a, 40, 46); the telecommunication means (18, 19, 28, 47) comprising a plurality of telecommunication equipments (18, 19);
- the first data storage means (22) contain first information on each associated payer (13), said first information comprising at least the admissible telephone number, at least a pre-established authorization criterion for authorizing at least one transaction that requires a payment from the associated payer's (13) account and at least a safety criterion associated univocally to the associated payer's (13) telephone number, as well as some second information on each associated payee (27, 29, 14, 14a, 40, 46) that comprises at least the admissible identification code;

the first server (20) comprising

- first verifying means (20a) for verifying in the data storage means (22) whether a first message received through the telecommunication means (18, 19, 28, 47) contains an admissible telephone number of an associated payer (13) and an admissible identification code of an associated payee (27, 29, 14, 14a, 40, 46), said first verifying means (20a) generating a first acceptance message when they detect an admissible identification code and an admissible telephone number;
- second verifying means (20b) for verifying in the data storage means (22) whether a transaction authorization request received through the telecommunication means (18, 19, 28, 47) in addition to the admissible telephone number detected by the first verifying means, satisfies said pre-established authorization criterion, said second verifying means (20b) generating a second acceptance message when the authorization request satisfies said authorization criterion;
- third verifying means (20c) for verifying in the first data storage means (22) whether a safety parameter received through the telecommunication means (18, 19) satisfies the safety criterion associated to the admissible telephone number detected by the first verifying means, said third verifying means (20c) generating a third acceptance message when they detect that the safety parameter satisfies the safety criterion associated to the admissible telephone number;
- authorization means (20d) for authorizing the account management means (20e) on the basis of the authorization request, to process a debit in the associated payer's (13) account and to process a corresponding credit in the associated payee's (27, 29, 14, 14a, 40, 46) account as long as the first, second and third acceptance messages have been generated;
- rejection message generating means (20f) for generating a rejection message when at least one of the acceptance messages has not been generated, and for transmitting the rejection message to the telecommunication means (18, 19, 28, 47);
- confirmation message generating means (20g) for generating at least a confirmation message when at least one of the acceptance messages has been generated, and for transmitting said confirmation message to the telecommunication means (18, 19, 28, 47), and for selective transmission of the confirmation message to the mobile telephone (16,41) identified by the admissible telephone number in said first message, and to the telecommunication terminal (15,15a,27,29,41,46) identified by the admissible identification code;
- second data storage means (21) that contain at least first information referring to the admissible telephone number of each payer (13), and at least second information referring to the type of digital mobile telephone (16, 41) belonging to each telephone number;
- selecting means (20h) for verifying in said second data storage means (21), the second information corresponding to the digital mobile telephone unit (16, 41) identified by the admissible telephone number and for selecting one of the telecommunication equipments (18, 19) that communicates with a digital mobile telephone (16, 41) identified by the admissible telephone number by means of a telecommunication service being compatible with the type of digital mobile telephone (16, 41) identified in said second information.

2. A system according to claim 1, wherein the admissible identification code of each payee (27, 29, 14, 14a, 40, 46) is selected among a telephone number,

Petitioner Askeladden LLC
Exhibit 1002 - Page 49 of 350

a number related to a telephone number, an Internet code, a code representative of an Internet code, an e-mail address, and a code based on an e-mail address.

3. A system according to claim 1, wherein the first verifying means verify the payer's (13) admissible telephone number from a code received through the telecommunication means (18, 19, 28, 47), representative of said admissible telephone number and contained in the first data storage means (22).

4. A system according to claim 1, wherein the second acceptance message generates an order to the telecommunication means (18, 19) to transmit to the mobile telephone (16) of a payer (13) identified by the admissible telephone number, a first confirmation message that contains a request to transmit the safety parameter that is to be verified by the third verifying means (20c) against the safety criterion.

5. A system according to claim 4, wherein the second acceptance message further generates an order to the telecommunication means (18, 19, 28, 47) to communicate with the telecommunication terminal (15, 15a, 27, 29, 46) identified by the admissible identification code detected by the first verifying means (20a), to transmit a second confirmation message that confirms the generation of the first acceptance message.

6. A system according to claim 1, wherein the third acceptance message generated by the third verifying means (20c) generates an order to the telecommunication means (18, 19, 28, 47) to communicate with the telecommunication terminal (15, 15a, 27, 29, 46) identified by the admissible identification code detected by the first verifying means (20a) to transmit a third confirmation message that confirms the generation of the third acceptance message.

7. A system according to claim 1 or 6, wherein the third acceptance message generated by the third verifying means (20c) generates an order to the telecommunication means (18, 19) to communicate with the mobile telephone (16) identified by the admissible telephone number detected by the first verifying means (20a), and to transmit a fourth confirmation message that confirms the generation of the third acceptance message.

8. A system according to claim 1, 6 or 7, wherein the third acceptance message generated by the third verifying means (20c) generates a command to the account management means (20e) to process the debit in the payer's (13) account and to process the corresponding credit in the payee's (27, 29, 14, 14a, 40, 46) account.

9. A system according to claim 1 or 8, wherein the account management means (20e) control at least a first intermediate account of each payee (27, 29, 14, 14a, 40, 46) contained in the first data storage means (22) and in which each credit is made.

10. A system according to claim 9, wherein the account management means (20e) comprise first transmission means for transmitting said credit to an administration and management server (23) that comprises a payees' data bank (25) in which all credits made in favor of each payee (27, 29, 14, 14a, 46) are stored, the administration and management server (23) transferring the credits contained in the data bank (25) to financial entities that manage each payee's financial accounts.

11. A system according to claim 1 or 8, wherein the account management means (20e) control second intermediate accounts selected from prepayment accounts, debit accounts in real time and post-payment accounts, of the payers (13).

12. A system according to claim 11, wherein the prepayment accounts controlled by the account management means (20e) comprise an electronic purse previously created in the first data storage means (22) for each buyer (13).

13. A system according to claim 1, wherein the authorization request comprises data regarding the value of the transaction, and wherein the pre-established authorization criterion verified by the second verifying means (20b) is selected among an available balance, a maximum credit limit and combinations thereof, established for each account of each payer (13).

14. A system according to claim 8, wherein the account management means (20e) comprise second transmission means for transmitting said debit to an administration and management server (23) that comprises a payers' data bank (24) wherein all debits made against each payer (13) are stored, the administration and management server (23) transferring the credits contained in the payers' data bank (24) to financial entities that manage each payer's financial accounts.

15. A system according to claim 1, wherein the safety criterion verified by the third verifying means (20c) is a secret identification code known by the payer (13) and stored in the first data storage means (22).

16. A system according to claim 15, wherein the third verifying means (20c) directly verify whether the safety parameter contains the secret identification code.

Petitioner Askeladden LLC
Exhibit 1002 - Page 50 of 350

17. A system according to claim 15, wherein the third verifying means (20c) verify whether the safety parameter contains an encrypted result of a self-verification (33) carried out locally in the mobile telephone (16) after direct entry (6) of the secret identification code into the mobile telephone by the payer (13), by means of decryption means for decrypting the encrypted result, on the basis of the secret identification code stored in the first data storage means (22).

18. A system according to claim 4, wherein when the first message verified by the first verifying means (20a) is a message received from the telecommunication terminal (15, 15a, 27, 41, 46), the second acceptance message generates an order to the telecommunication means (18, 19) to establish communication with the mobile telephone (16) for requesting the payer (13) identified by the admissible telephone number to transmit the safety parameter.

19. A system according to claim 4, wherein, when the first message verified by the first verifying means (20a) is a message received from a payer's (13) mobile telephone (16), the second acceptance message generates an order to the telecommunication means (18, 19) to transmit a message to said mobile telephone (16) requesting the payer (13) identified by the admissible telephone number to transmit the safety parameter.

20. A system according to claim 4, 18 or 19, wherein the second acceptance message further generates an order to the telecommunication means (18, 19) to transmit at least the value of the transaction and an identification of the payee, which are transmitted together with the message requesting the safety criterion.

21. A system according to claim 1, wherein the first server (20) processes a first message that furthermore contains an identification of an e-mail address, wherein the payee (27) is a supplier of software files, and wherein the confirmation message generating means (20g) furthermore generate a further confirmation message that contains a decryption code of the software file, received from the payee (27) in the first server (20), said further confirmation message being transmitted to the payer's (13) mobile telephone (16).

22. A system according to claim 1, wherein the first server (20) further comprises first detecting means (20i) for detecting a first instruction to make a purchase with advance payment and collection code generating means (20j), and wherein the confirmation message generating means (20g) also generate a complementary confirmation message that contains the collection code, said complementary confirmation message being transmitted to the payer's (13) mobile telephone (16) and to the payee's (14, 14a, 27, 29, 46) telecommunication terminal (15, 15a, 27, 29, 46).

23. A system according to claim 1, wherein the first data storage means (22) further comprise, with respect to each payee (14a, 46), third information associated with said second information and that comprises data regarding products or services corresponding to each authorized transaction, and wherein the first server (20) further comprises

second detecting means (20k) for detecting a second instruction to manage a delivery in person corresponding to an authorized transaction and received from the telecommunication terminal (15a) being a payee's (14a) mobile telephone.

delivery code generating means (201) for generating a delivery code identifying at least a product or service to be delivered, and identification message generating means (20m) identifying said product or service, and wherein the confirmation message generating means (20g) further generate an additional message that contains the delivery code, said additional message being transmitted to the payer's (13) mobile telephone (16) and to the payee's (14a) mobile telephone (15a) and the identifying message being transmitted at least to the payer's (13) mobile telephone (16) along with a request to transmit the safety parameter,

and delivery management processing means (20n) that, when the third verifying means (20c) have verified that the safety parameter satisfies the safety criterion associated to the payer's (13) mobile telephone, generate an entry in a delivery note data base (37).

24. A system according to claim 1, wherein the first data storage means (22) also comprise fourth information associated to said second information and that comprise reference codes that identify the products or services of at least one payee (14a, 46) as well as a price associated to each product or service.

25. A system according to claim 24, wherein the fourth information also comprises a first selectable telephone number comprised of one of said reference codes and an identification code of the corresponding payee (14, 46), and that constitutes the admissible identification code.

26. A system according to claim 24 or 25, wherein the fourth information also comprises the admissible identification code in the form of a telephone

Petitioner Askeladden LLC
Exhibit 1002 - Page 51 of 350

number for access to the payee (16,46) associated to at least a first menu comprised of the reference codes, the products or services identified respectively by each one of said reference codes and the price of said products or services.

27. A system according to claim 1, wherein the admissible identification code is an admissible access telephone number for accessing a second menu of respective admissible identification codes of a plurality of associated payees (14a, 46) and wherein the first data storage means (22) further comprise fifth information associated to said second information and that comprise reference codes that identify products or services of each one of the payees (14a, 46) as well as a price associated to each product or service.

28. A system according to claim 27, wherein the fifth information further comprises a first selectable telephone number comprised of one of said reference codes and an identification code of the corresponding payee (14, 46) and that constitutes the admissible identification code.

29. A system according to claim 27 or 28, wherein the fifth information further comprises the admissible identification code as an access telephone number of the payee (14,46) being associated to at least a first menu comprised of the reference codes, the products or services identified respectively by each of said reference codes and the price of each of said products or services.

30. A system according to claim 1, wherein the second information in the first data storage means (22) comprise

identification codes of a plurality of vending machines (29) each one of which includes a digital mobile telephone (29a) as a telecommunication terminal, identified by a mobile telephone number as an admissible identification code;
an authorization code associated to the admissible identification code of each vending machine;
an activation code for activating the vending machine (29), associated to each authorization code that activates the vending machine for receiving a request from the payer (13) identified by the admissible telephone number;
and wherein
the confirmation message generating means (20g) generate, when the first, second and third verifying means (20a, 20b, 20c) have respectively generated the first, second and third acceptance message, and transmit the confirmation message that comprises at least the code for activating the vending machine and the admissible telephone number of the payer's (13) mobile telephone (16).

31. A system according to claim 30, wherein the confirmation message generating means (20g) establish a communication between the payer's (13) mobile telephone and the vending machine (29), for a preestablished period of time during which the payer (13) can transmit, through the first server (20), a selection message to the vending machine (29); and wherein the server (20) further comprises deactivation detecting means (20o) for detecting deactivation of the vending machine (29).

32. A system according to claim 31, wherein the authorization criterion associated to the admissible telephone number of each vending machine is a direct authorization code that establishes a maximum limit selected from an economic value and a number of dispensing requests, admitted in a specific period of time in respect of requests made from the same mobile telephone, and wherein the confirmation message generating means (20g) generate the confirmation message when the direct authorization code has been detected.

33. A system according to claim 30, wherein when the confirmation message generating means (20g) in the first server (20), close the communication with the vending machine (29) after having transmitted the confirmation message, so that the payer (13) may make his selection directly by means of the selection display of the vending machine.

34. A system according to claim 30,31,32 or 33, wherein the first server (20) further comprises recording means (20p) associated to the authorization means (20d), for recording transactions recorded in each vending machine (29).

35. A system according to claim 1, wherein the first verifying means (20a) of the first server (20) further comprise complementary verifying means (20g) being associated to the selecting means (20h), for verifying if the admissible identification code that has been verified by the first verifying means (20a) in said first message received from a payer (13) identified by a first admissible telephone number and containing a transaction request that has been verified by the second verifying means (20b), corresponds to a second admissible telephone number from among the admissible telephone numbers of a digital mobile telephone (41) comprised within the first information contained in the first data storage means (22) and if the first message identifies the second admissible telephone number as identification of a payee (40), the complementary verifying

Petitioner Askeladden LLC
Exhibit 1002 - Page 52 of 350

means (20q) generating a fourth acceptance message when detecting that said second admissible telephone number corresponds to a payee (40), said fourth acceptance message being processable by the confirmation message generating means (20g), and wherein the rejection message generating means (20f) generate a rejection message when the fourth message has not been generated.

36. A system according to claim 35, wherein

the confirmation message generating means (20g) generate, when detecting the first, second, third and fourth acceptance message, a first confirmation message containing an identification of the payer (13), an identification of the transaction and a petition for conformity to the payee (40) identified in the first message; said petition for conformity comprising a request of transmission of the safety parameter, and transmit said confirmation message to the mobile telephone (41) of the payee (40) identified by the second admissible telephone number through the telecommunication means (18,19) selected by the selecting means;
the third verifying means (20c) furthermore verify if the safety parameter transmitted from the mobile telephone (41) in response to the petition for conformity, satisfies the safety criterion associated to the second admissible telephone number, said third verifying means (20c) generating a fifth acceptance message when said parameter satisfies said safety criterion;
the authorization means (20e) authorize the account management means (20d) when said fifth acceptance message has been generated;
the confirmation message generating means (20g) generate and transmit a second confirmation message to the mobile telephone (16) of the payer and to the mobile telephone (41) of the payee (41).

37. A system according to any of claims 1, 35 or 36, wherein, in the first server (20), each second information contained in the second data storage means (21) and referring to the type of digital mobile telephone corresponding to each admissible telephone number of each associated payer (13) and each admissible identification code of each payee (40) when the latter is a number of a digital mobile telephone, is a first identifying code being representative of the International Mobile Equipment Identifier (IMEI).

38. A system according to claim 37, wherein the first server (20) comprises first inquiry means (20r) for inquiring in at least one Visitor Location Register (VLR) comprising a first register relating telephone numbers with an IMEI code, the IMEI code corresponding to each of the admissible telephone numbers, and updating means (20s) for updating said second information in the second data storage means (21) by comparing each IMEI code inquired by the first inquiry means (20r) with each code being representative of the IMEI code associated to each admissible telephone number as contained in the second data storage means (21).

39. A system according to claim 38, wherein the first inquiry means (20r) extract the IMEI code associated to each admissible phone number, from an Equipment Identifier Register (EIR) that contains an association between each admissible telephone number and the IMEI code corresponding to each admissible telephone number, and which receive said association from each Visitor Location Register as updated by said Visitor Location Register.

40. A system according to claim 38 or 39, wherein the first inquiry means (20r) extract the IMEI code associated to each admissible telephone number, from an Unstructured Supplementary Service Data (USSD) frame into which each Visitor Location Register associated to each Mobile Switching Center (MSC) which has issued said frame, has inserted the IMEI code associated to the admissible telephone number corresponding to the user who has originated said frame.

41. A system according to claim 38, wherein the first inquiry means (20r) extract the IMEI code associated to each admissible telephone number, through an interface between the Visitor Location Register and said inquiry means (20r).

42. A system according to claim 37, wherein the first server (20) comprises

second inquiry means (20t) for inquiring the IMEI code corresponding to each admissible telephone number, in Call Data Registers (CDR) of a data bank of a mobile telephony network operator, that contain a relation of each telephone number which, on the grounds of a call, has originated a Call Data Register with an IMEI code of the terminal from which said call originated,
second updating means (20u) for updating said second information in the second data storage means (21) on he basis of a comparison of each IMEI code inquired by the second inquiry means (20t) with each code being representative of the IMEI code associated to each admissible telephone number, contained in the second data storage means (21).

Petitioner Askeladden LLC
Exhibit 1002 - Page 53 of 350

43. A system according to claim 37, wherein the second information further comprises at least one datum being indicative of a communication capacity selected from a capacity of managing sessions according to Wireless Application Protocols (WAP), a capacity of managing sessions of Unstructured Supplementary Service Data (USSD), and combinations thereof, of each digital mobile telephone identified by an IMEI code and associated to an admissible telephone number.

44. A system according to claim 37, wherein the first server (20) comprises

third inquiry means (20v) for inquiring in a data bank of a mobile telephony network operator, registers that each Mobile Switching Center (MSC) transfers immediately each time a USSD frame or a voice call is addressed to a specific telephone number, said registers containing a relation of each telephone number from which a call was made or originated the USSD frame with an IMEI code of the terminal from which said call or frame originated, in respect of the IMEI codes corresponding to each admissible telephone number, and
third updating means (20w) for updating said second information in said second data storage means (21) on the basis of a comparison of each inquired IMEI code inquired by the third inquiry means (20v) with each code being representative of the IMEI code associated to each admissible telephone number contained in the second data storage means.

45. A process for processing payments and transactions between payers (13) and payees (27,29,14,14a,13a,40,46), wherein a system as defined in any of the preceding claims is used.

46. A process according to claim 45, the process comprising

- selectively receiving, through telecommunication means (18,19,28,47), in a payment and transaction center (17), a first message comprising the number of a mobile telephone (16) of a payer (13) or an identification code of a payee (27,29,14,14a,13a,40,46), and, furthermore,
- receiving the amount of a purchase or of a code identifying a product or service, in the payment ad transaction center (17),
- verifying if the first message originates from a payer (13) identified by an admissible telephone number or an admissible identification code of a payee (27,29,14,14a,13a,40,46);
- verifying if conditions of a transaction requested in the first message, satisfy transaction criteria stored in first data storing means (22);
- verifying the type of digital mobile telephone associated to the admissible telephone number, in second data storage means (21), and selecting one telecommunications equipment (18,19) for communicating with the digital mobile telephone (16) identified by the admissible telephone number, through a telecommunications service being compatible with the type of digital mobile telephone (16) identified by the admissible telephone number;
- checking "on line", in the first data storage means (22), if the payer (13) has a disposable balance in a previously created electronic purse in said transaction and payment center (17);
- requesting the payer (13) identified in the first message, when the transaction condition is satisfied and there is a sufficient disposable balance for authorizing the transaction, to introduce into the mobile telephone (16) identified in the first message, and to transmit, a safety parameter;
- verifying in the first data storage means (22), if the safety parameter introduced into and transmitted by, the mobile telephone (16) of the payer, satisfies a safety criterion univocally assigned to said mobile telephone (16);
- authorizing and carrying out the transaction as requested when the safety parameter satisfies the safety criterion; and
- sending a confirmation that the transaction has been carried out, to the mobile telephone (16) of the payer and to the payee (27,29,14,14a, 13a,40,46).

Petitioner Askeladden LLC
Exhibit 1002 - Page 54 of 350

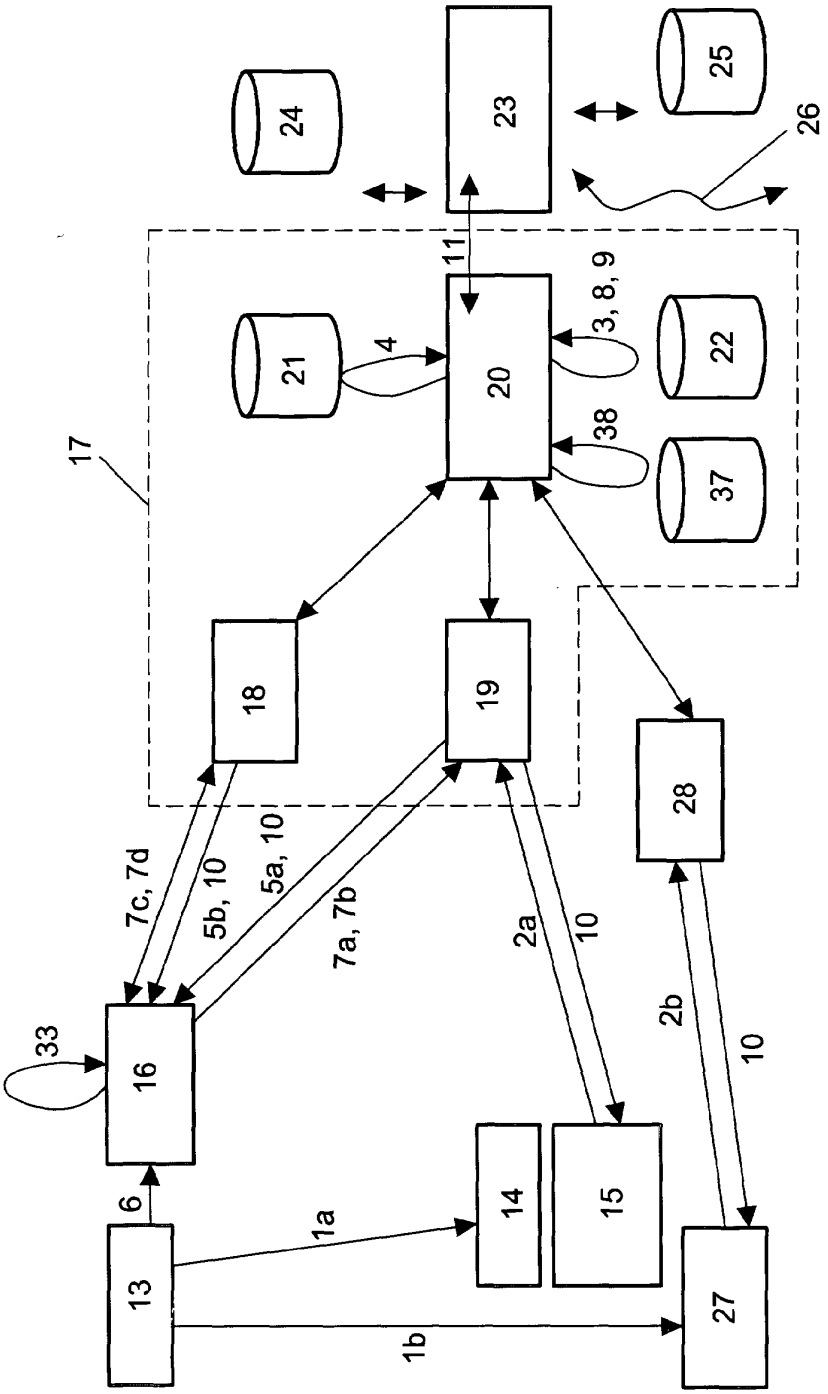


FIG. 1

Petitioner Askeladden LLC
Exhibit 1002 - Page 55 of 350

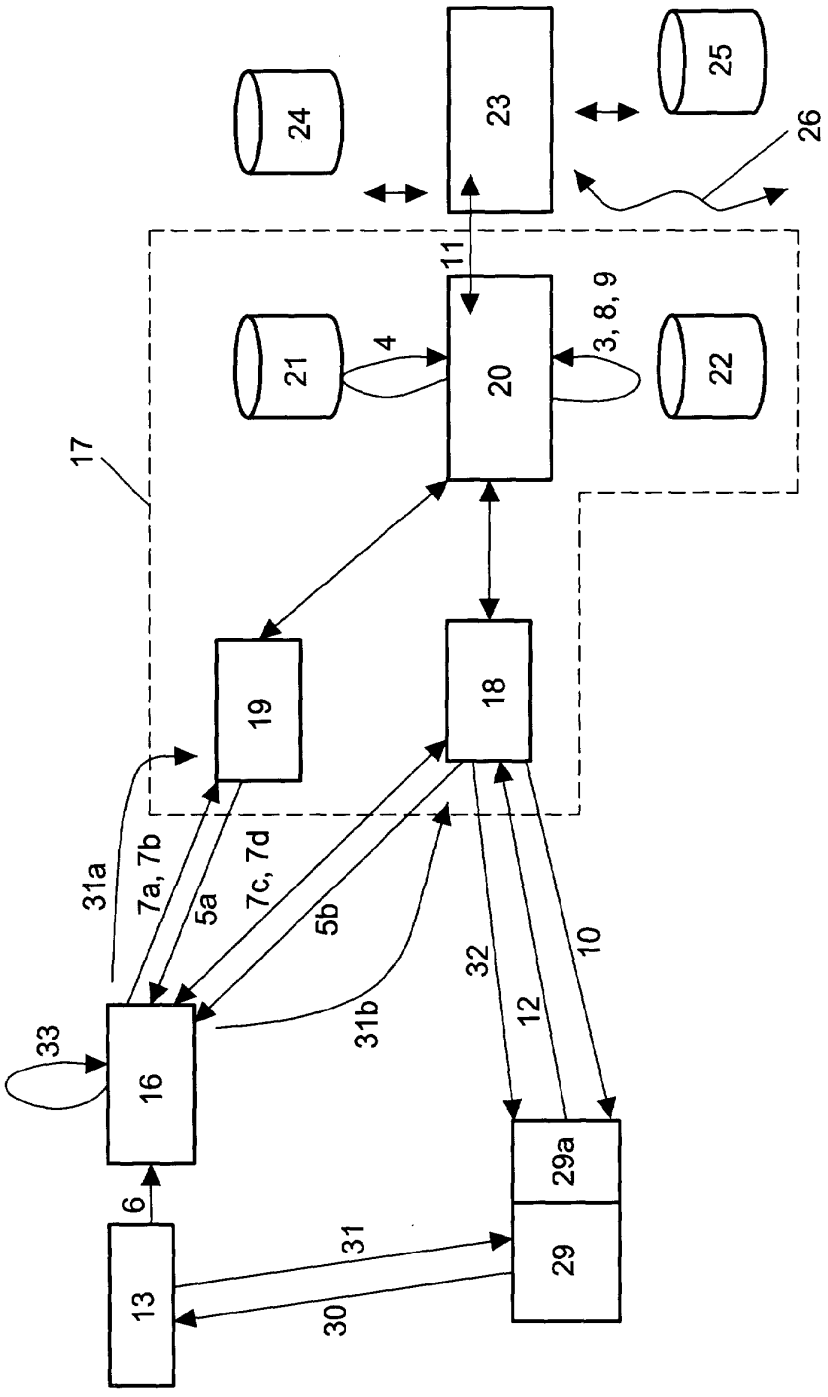


FIG. 2

Petitioner Askeladden LLC
Exhibit 1002 - Page 56 of 350

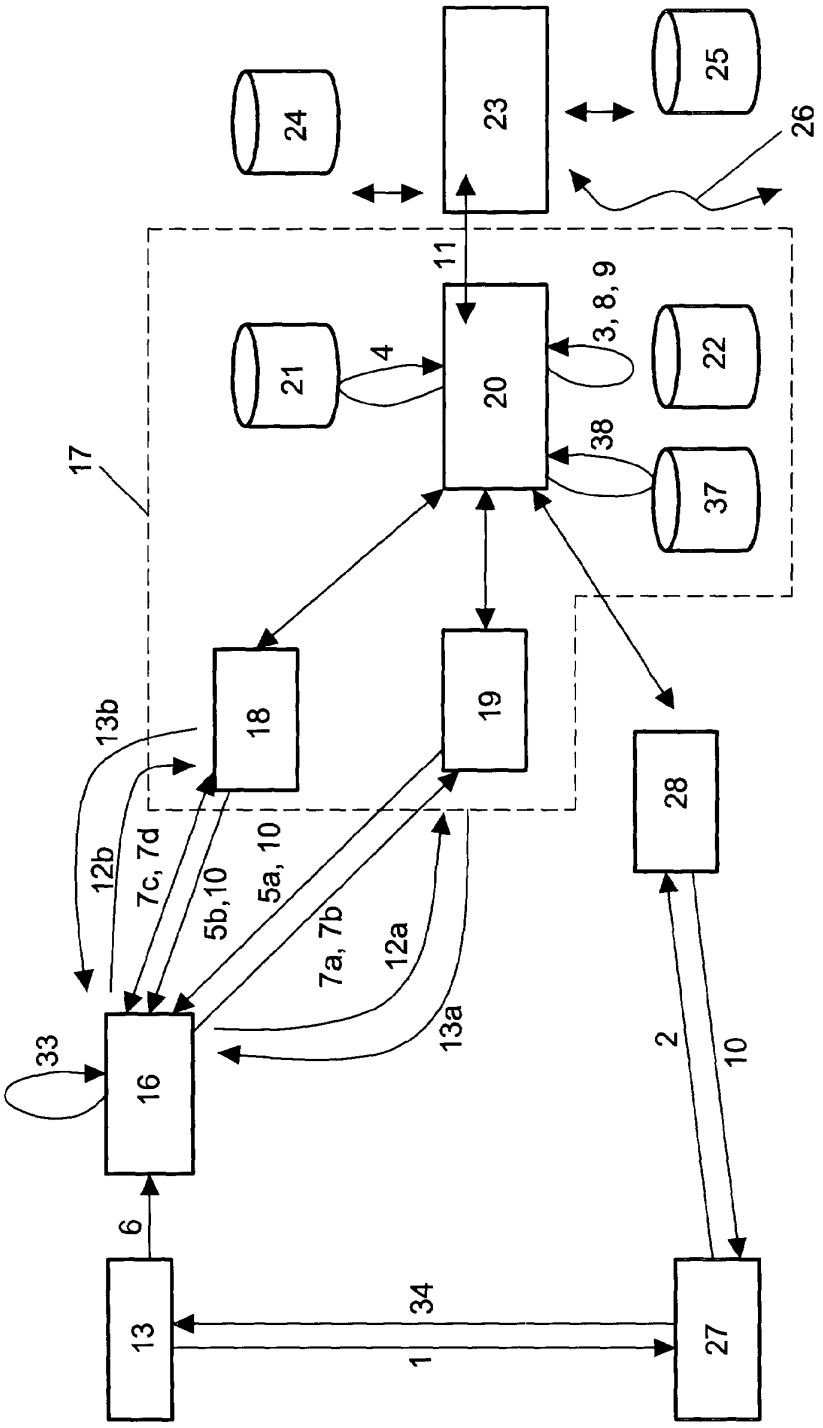


FIG. 3

Petitioner Askeladden LLC
Exhibit 1002 - Page 57 of 350

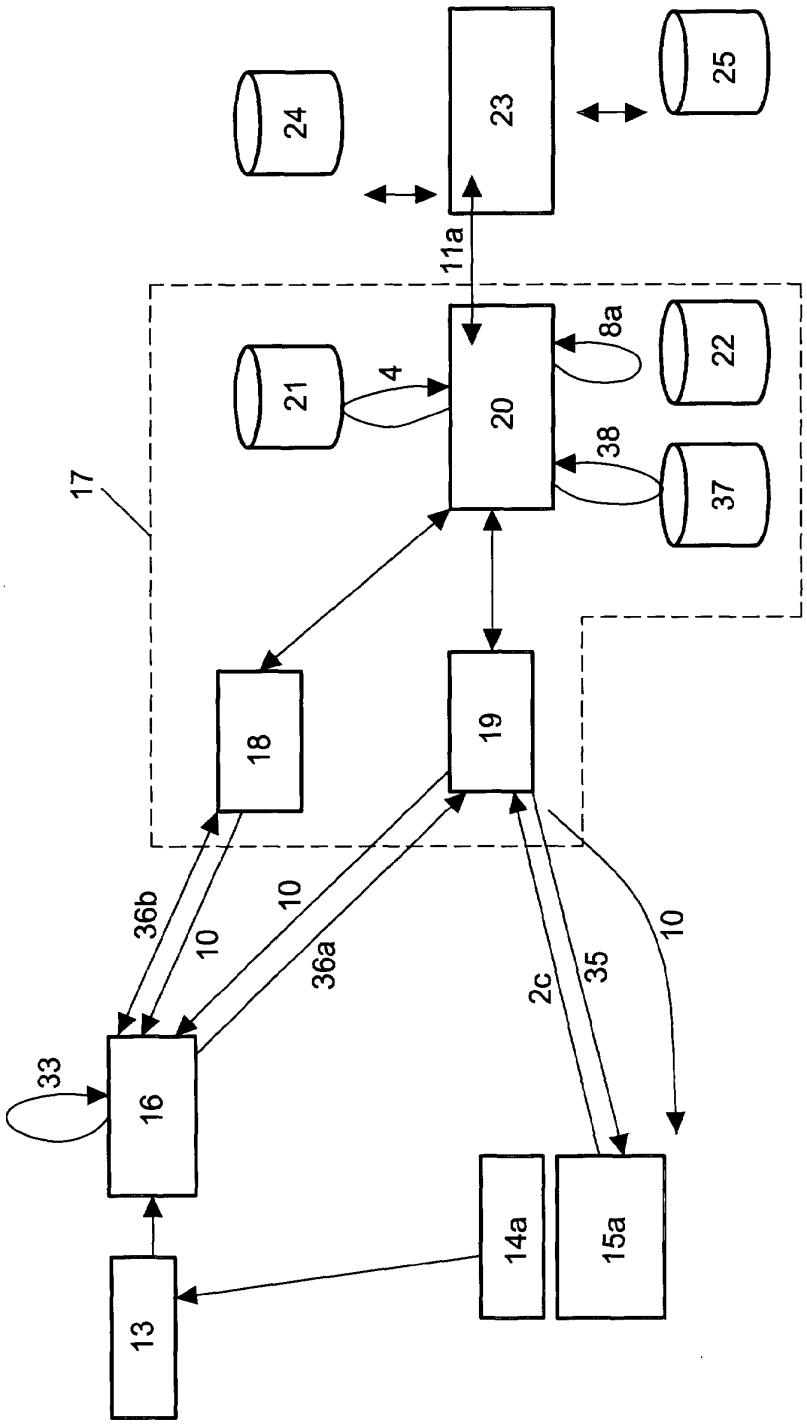


FIG. 4

Petitioner Askeladden LLC
Exhibit 1002 - Page 58 of 350

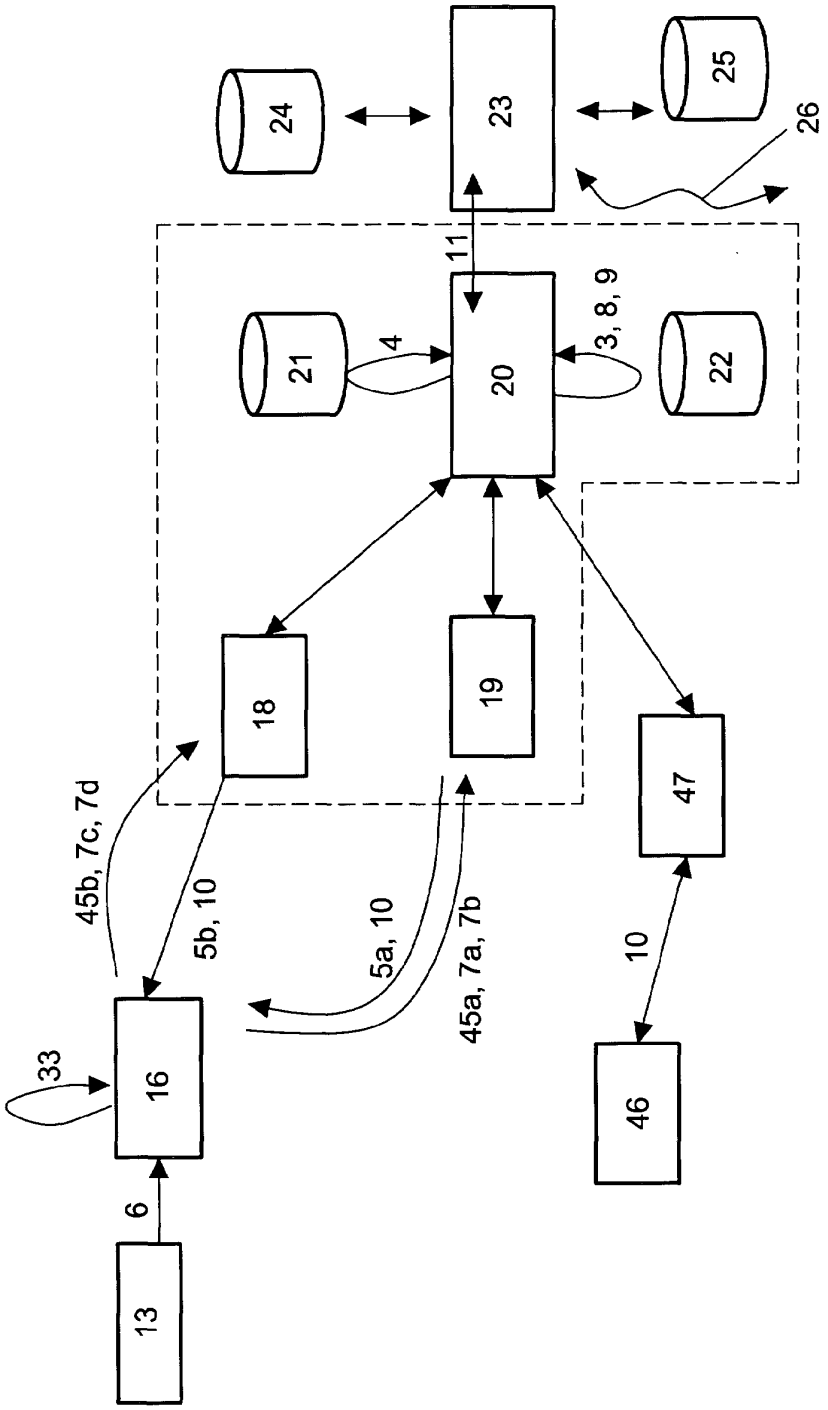


FIG. 5

Petitioner Askeladden LLC
Exhibit 1002 - Page 59 of 350

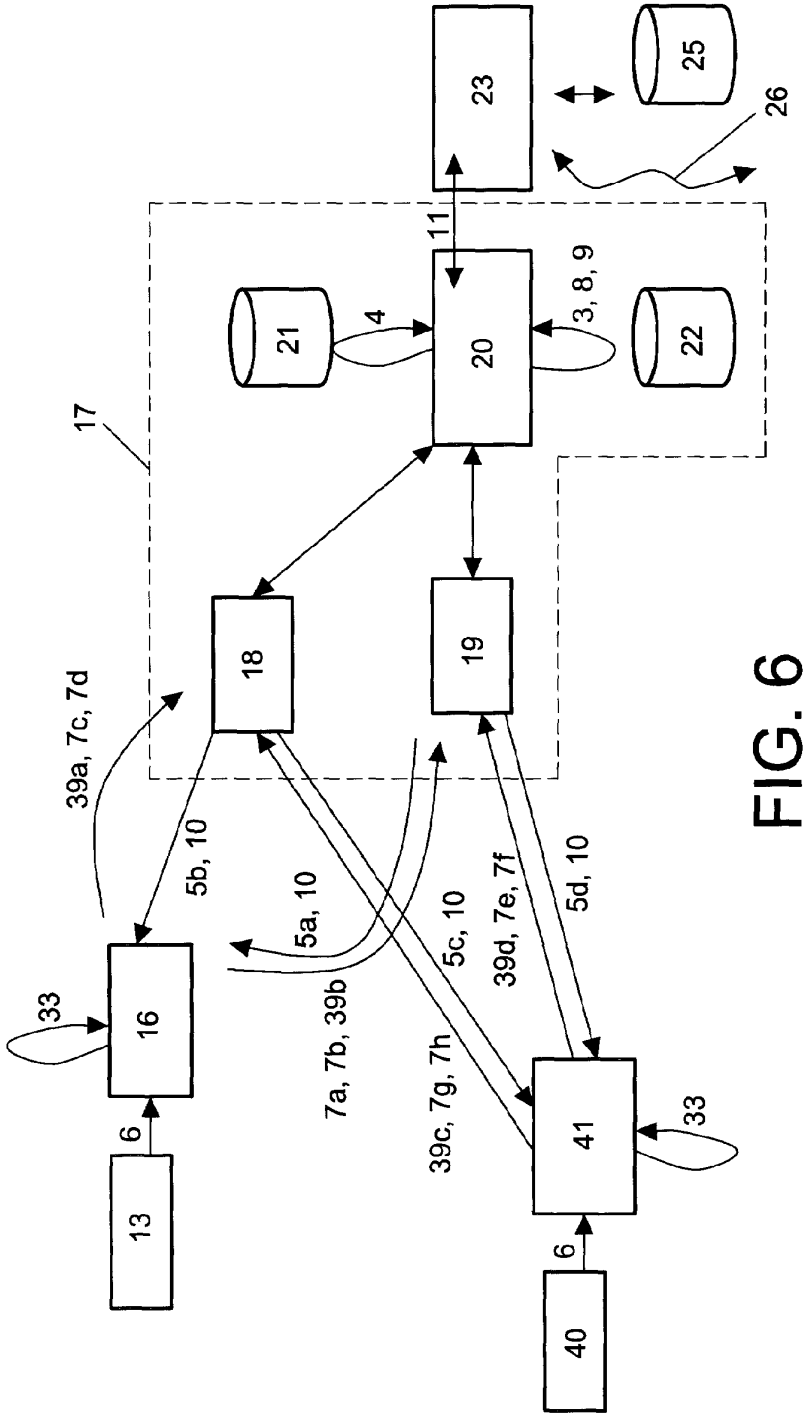


FIG. 6

Petitioner Askeladden LLC
Exhibit 1002 - Page 60 of 350

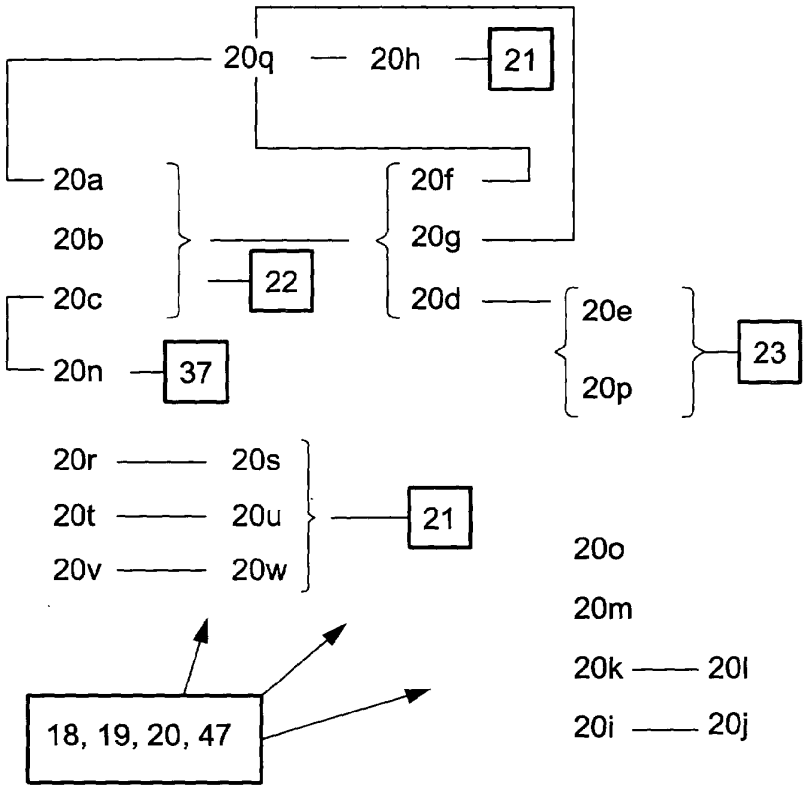


FIG. 7

Petitioner Askeladden LLC
Exhibit 1002 - Page 61 of 350

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 20 2720

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A,D	EP 0 986 275 A (SWISSCOM AG) 15 March 2000 (2000-03-15) * the whole document *	1-9,21, 24,25, 35-45	G07F7/10 //G07F19/00
A	WO 99 33034 A (GLOBAL MOBILITY SYSTEMS INC) 1 July 1999 (1999-07-01) * page 7, line 9 - page 11, line 20 * * page 14, line 3 - page 16, line 23 *	15,24, 27,28, 30-34	
A,D	WO 98 47116 A (ERICSSON TELEFON AB L M) 22 October 1998 (1998-10-22) * page 7, line 1 - page 19, line 21 * * figure 3 *	1,3, 9-11,15	
A	WO 99 22346 A (SONERA OY ;VIHINEN SEPPO (FI); STEWEN TEEMU (FI)) 6 May 1999 (1999-05-06) * page 3, line 3 - page 7, line 27 * * page 8, line 34 - page 9, line 22 * * figure *	24,27-34	
A	WO 97 41499 A (MARTINEZ JERRY R) 6 November 1997 (1997-11-06) * page 9, line 22 - page 12, line 5 * * page 15, line 12 - page 16, line 16 *	23	
A	"DIALOG. SUN-SENTINEL" DIALOG. SUN-SENTINEL, XP002932299		

TECHNICAL FIELDS SEARCHED (Int.Cl.7)
G07F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	13 June 2001	Bocage, S

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Petitioner Askeladden LLC
Exhibit 1002 - Page 62 of 350

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 20 2720

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

13-06-2001

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0986275 A	15-03-2000	JP 2000163487 A	16-06-2000
WO 9933034 A	01-07-1999	AU 2087099 A	12-07-1999
		EP 1046144 A	25-10-2000
WO 9847116 A	22-10-1998	AU 7094398 A	11-11-1998
		BR 9808534 A	23-05-2000
		CN 1260895 T	19-07-2000
		EP 0976116 A	02-02-2000
		NO 995031 A	16-12-1999
WO 9922346 A	06-05-1999	FI 3450 U	10-07-1998
		AU 1033499 A	17-05-1999
		CN 1278354 T	27-12-2000
		EP 1027684 A	16-08-2000
		NO 20002266 A	28-04-2000
		PL 340249 A	29-01-2001
WO 9741499 A	06-11-1997	AU 2802797 A	19-11-1997

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Petitioner Askeladden LLC
Exhibit 1002 - Page 63 of 350

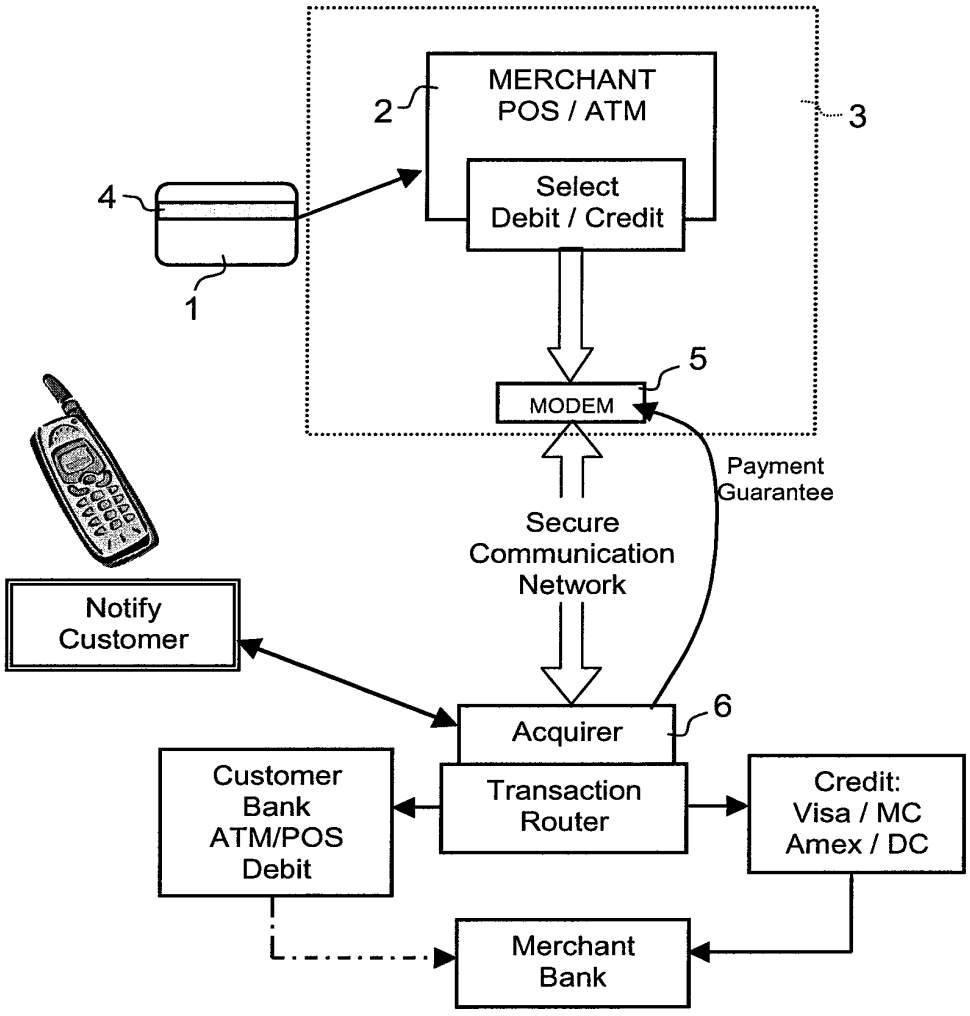

MERCHANT
POS / ATM
2
3
Select
Debit / Credit
4
1
5
MODEM
Payment
Guarantee
Secure
Communication
Network
Notify
Customer
6
Acquirer
Customer
Bank
ATM/POS
Debit
Transaction
Router
Credit:
Visa / MC
Amex / DC
Merchant
Bank

FIG. 1

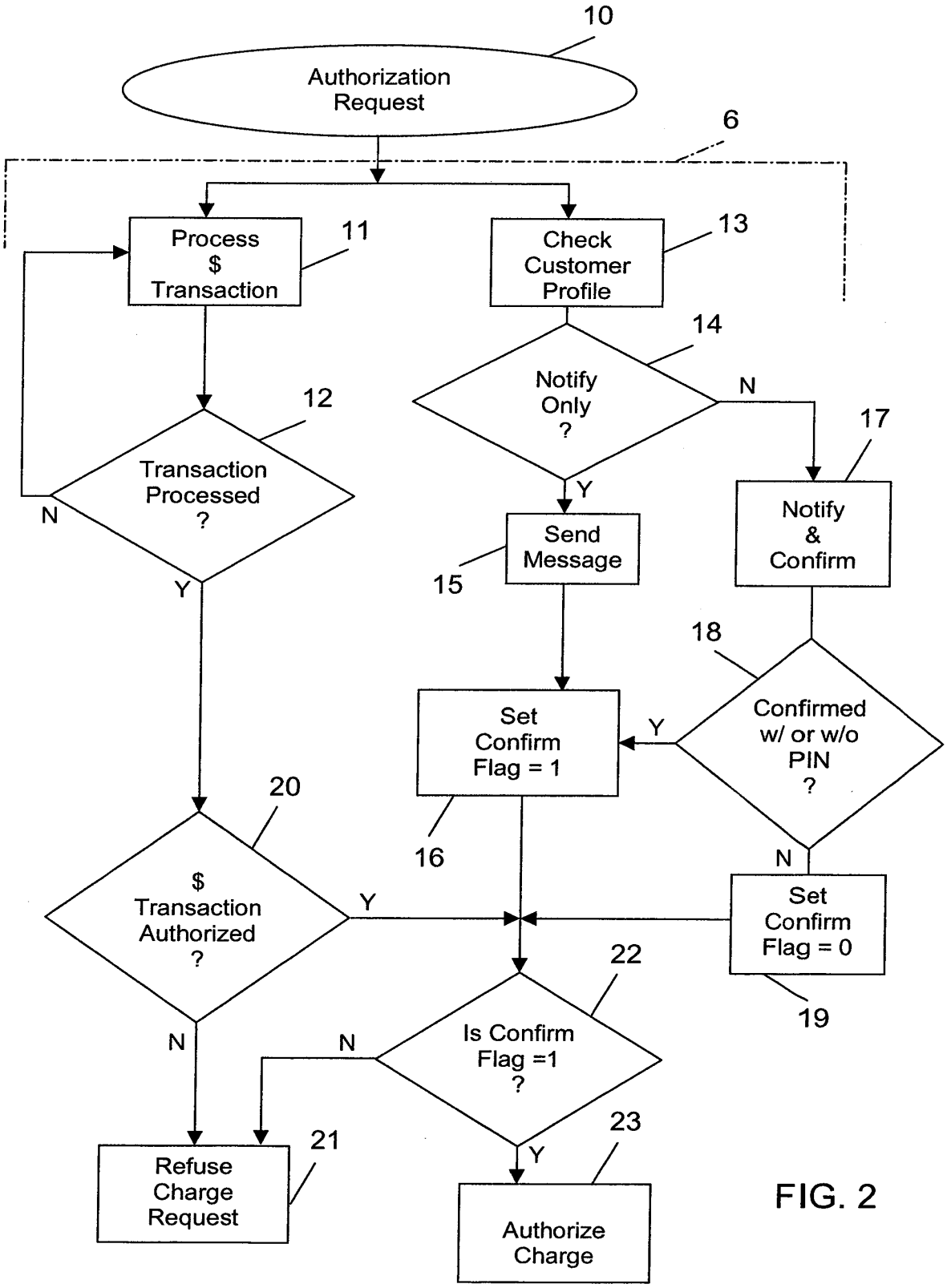

10
Authorization Request
6
Process $ Transaction
11
Check Customer Profile
13
Notify Only ?
14
N
Y
17
Notify & Confirm
12
Transaction Processed ?
N
Y
Send Message
15
18
Confirmed w/ or w/o PIN ?
Y
Set Confirm Flag = 1
16
N
Set Confirm Flag = 0
19
20
$ Transaction Authorized ?
Y
22
Is Confirm Flag =1 ?
N
N
23
Y
21
Refuse Charge Request
Authorize Charge

FIG. 2

W-9001D3

TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of copending patent application No. 13/088,514, filed April 18, 2011; which was a continuation of patent application No. 12/043,235, filed March 6, 2008, now U.S. Patent No. US 7,954,706 B2; which was a divisional of patent application No. 11/077,783, filed March 11, 2005, now U.S. Patent No. US 7,357,310 B2; the prior applications are herewith incorporated by reference in their entirety.

BACKGROUND OF THE INVENTION

Field of the Invention

[0002] The invention lies in the financial transaction processing field. More specifically, the invention relates to credit and debit transactions and to related charge notification and charge authorization.

Petitioner Askeladden LLC
Exhibit 1002 - Page 66 of 350

[0003] Credit cards and charge cards have become the primary vehicle by which payments for consumer services and consumer goods are transacted. In today's environment, credit payments are authorized at the point of sale (POS) and the authorization is provided by the cardholder's signature on a receipt. Often, the transaction is performed under considerable time pressure (e.g., in a long cash-out line) and mistakes are only recognized after the transaction has been completed. The consumer may, for example, have been charged too much, and he may have authorized the incorrect amount. As many consumers know, correcting such simple mistakes is not at all simple and the correction is time consuming and it is an expensive service for the credit card and credit clearing houses to maintain.

[0004] Mistakes such as the foregoing, however, are not the main reason for considerable losses. Often, incorrect or non-authorized charges are effected because of fraudulent or even innocent mistakes that could have been avoided, had better authorization security been assured. It is well known that charge errors and charge fraud causes millions of dollars in losses in the United States alone.

Petitioner Askeladden LLC
Exhibit 1002 - Page 67 of 350

[0005] Extraneous authorization security, on the other hand, may be too intrusive in many cases and may even have a negative impact on the transaction.

SUMMARY OF THE INVENTION

[0006] It is accordingly an object of the invention to provide a credit card transaction notification and authorization method, which overcomes the above-mentioned disadvantages of the heretofore-known devices and methods of this general type and which provides for a non-intrusive, user-selectable notification and authorization system for credit card transactions.

[0007] With the above and other objects in view there is provided, in accordance with the invention, an improved charge payment authorization method. First, a charge is requested at a merchant's and account information for payment of a customer's purchase is acquired at the merchant's. Then an authorization request is transmitted to a remote charge processing facility, and the charge request is processed. This conventional process is improved as follows: a notification of the charge request is transmitted in the form of a SMS or text through a cellular network to a wireless device associated with the customer no later than immediately after authorizing the charge request and the charge request is processed

Petitioner Askeladden LLC
Exhibit 1002 - Page 68 of 350

without requiring a response from the wireless device associated with the customer, i.e., without waiting for an authorization from the customer.

[0008] With the foregoing and other objects in view there is provided, in accordance with the invention, a payment authorization method, which comprises:

gathering, at a merchant's, account information for payment of a customer's purchase;

transmitting an authorization request to a financial authorization system requesting payment authorization for the customer's purchase, the authorization request including the account information;

notifying the customer by sending a message to a communications device associated with the customer.

[0009] In accordance with an added feature of the invention, the gathering step comprises swiping a card presented by the customer and containing the account information.

Petitioner Askeladden LLC
Exhibit 1002 - Page 69 of 350

[0010] With the above and other objects in view there is also provided, in accordance with a second embodiment of the invention, a payment authorization method, which comprises:

gathering, at a merchant's, account information for payment of a customer's purchase;

transmitting an authorization request to a financial authorization system requesting payment authorization for the customer's purchase, the authorization request including the account information;

calling a communications device associated with the customer and prompting the customer for confirmation or refusal of the transaction; and

processing the authorization request in accordance with the customer's response by either refusing the transaction or processing the purchase.

[0011] In accordance with an alternative implementation of the invention the customer is required to enter their personal identifier (e.g., a PIN) upon being prompted. A proper PIN response is considered an authorization, while an incorrect PIN or no response at all is considered a refusal.

Petitioner Askeladden LLC
Exhibit 1002 - Page 70 of 350

[0012] With the above and other objects in view there is also provided, in accordance with the invention, a charge card processing method, which comprises:

inputting a transaction request to a stationary merchant terminal disposed at a merchant location;

processing the transaction request with the merchant terminal, including a transmission of a first authorization request to a remote processing facility and receipt of a notification that authorization has been accepted or declined;

transmitting a second authorization request from a remote processing facility to a mobile communications device of a customer associated with the requested transaction via a wireless link; and

authorizing the requested transaction only if authorization has been accepted for the first authorization request and a proper response has been received by the remote processing facility to the second authorization request.

Petitioner Askeladden LLC
Exhibit 1002 - Page 71 of 350

[0013] With the above and other objects in view there is also provided, in accordance with the invention, a charge processing method, which comprises:

preauthorizing an imminent given transaction by transmitting a preauthorization for the imminent given transaction from a customer to a financial authorization system;

subsequently inputting a transaction request concerning the given transaction at a merchant terminal disposed at a merchant location;

processing the transaction request at the merchant terminal, including a transmission of an authorization request for the given transaction to the financial authorization system;

transmitting a response to the authorization request from the financial authorization system to the merchant terminal, and thereby authorizing the transaction request at the merchant's if the preauthorization from the customer is available in the financial authorization system, and otherwise contacting the customer for authorization or declining the authorization request.

[0014] In accordance with a concomitant feature of the invention, the preauthorization from the customer includes a maximum amount to be

Petitioner Askeladden LLC
Exhibit 1002 - Page 72 of 350

authorized for the transaction and a time period within which the preauthorization is valid.

[0015] Other features which are considered as characteristic for the invention are set forth in the appended claims.

[0016] Although the invention is illustrated and described herein as embodied in a credit card transaction notification and authorization system, it is nevertheless not intended to be limited to the details shown, since various modifications and structural changes may be made therein without departing from the spirit of the invention and within the scope and range of equivalents of the claims.

[0017] The construction of the invention, however, together with additional objects and advantages thereof will be best understood from the following description of the specific embodiment when read in connection with the accompanying drawings.

Petitioner Askeladden LLC
Exhibit 1002 - Page 73 of 350

BRIEF DESCRIPTION OF THE DRAWING

[0018] Fig. 1 is a schematic diagram illustrating a transaction according to the invention, in which the customer is notified immediately during the transaction; and

[0019] Fig. 2 is a flow diagram illustrating a method for charge request processing according to the invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0020] Referring now to the figures of the drawing in detail and first, particularly, to Fig. 1 thereof, there is seen a simplified process stream in a cash-less sales transaction. A charge card 1 is swiped at a magnetic card reader 2 at a merchant terminal 3, or the card number is manually entered at the merchant terminal 3. The latter may represent a store, it may be a teller or an automated teller machine (ATM), or it may be a virtual terminal in an internet-type transaction. The cardholder, or the person swiping the card, may now be prompted to select a debit transaction or a credit transaction on the merchant terminal 3. If debit is selected, the cardholder enters the PIN associated with the card or with the account. If credit is selected, the cardholder is requested to sign for the purchase.

Petitioner Askeladden LLC
Exhibit 1002 - Page 74 of 350

[0021] Prior to the customer's signing for the purchase, the merchant terminal 3 connects, through a modem 5, to an acquirer 6. The latter obtains the information from the modem 5 and checks against its data sources whether or not the transaction should be authorized. At the same time, a corresponding customer profile is checked as to the customer's set preferences concerning the notification/authorization options according to the invention.

[0022] Here, the customer's profile is set to simple "notification," which means that the system only notifies the cardholder by sending a message to his wireless device (e.g., cell phone). The message may be an audible message such as, for example, "%amount% charged on %date% at %merchant name%", or it may be an SMS (short message service) sent to the customer's phone. The customer's profile, however, may be set to any of several other options. For instance, the profile may be set to a simple notification, as above, followed by a prompt to confirm the purchase. The confirmation, again, may take any of several forms. For example, a simple "1" in answer to the confirmation request may be a code for authorization and a "2" may be a refusal. Or else, the customer may be prompted to enter a PIN or any set password which is stored in the customer profile. If the profile is set to authorization, the payment authorization and the payment

Petitioner Askeladden LLC
Exhibit 1002 - Page 75 of 350

guarantee are not provided. That is, the card transaction is declined at the merchant terminal 3.

[0023] The simple notification, of course, does not add any time to the transaction. If confirmation is required, the transaction is slightly extended. The added security, however, may well justify the delay. In either case, it is up to the customer to choose and set his profile accordingly.

[0024] The possible delay may be avoided by way of a further modification of the invention. Here, we provide for preauthorization when a charge request is imminent. By way of example: waiting in a checkout line, the customer may call “ahead” and provide preauthorization for the impending purchase. This may be entirely automated. The system will prompt the customer to identify a period of time for which the authorization is valid. For example, the purchase may be expected within 10 minutes and, accordingly, the customer will select, say, the half-hour authorization option. The system may also prompt for a maximum amount that would be authorized. For example, the purchase may be expected to cost $ 50.00 and, accordingly, the customer may set the maximum authorized amount to, say, $ 100.00. Proper preauthorization parameters may be empirically or statistically developed and the system may be set accordingly.

Petitioner Askeladden LLC
Exhibit 1002 - Page 76 of 350

[0025] The process flow may be best understood by reference to a realistic example in a restaurant environment: The server has presented the customer a check, the customer has briefly reviewed the check, found the total amount of, say, $40.00 agreeable, and handed the server the check and the credit card. The server then moves to a backroom and processes the transaction, by swiping the card and entering the amount of $40.00 into a register terminal. Immediately upon receiving the authorization request, the credit card authorization system (e.g., the acquirer 6) sends an SMS message to the customer's cell phone. The customer receives the message telling him that the restaurant has requested authorization for a charge of $40.00. This happens well before the server returns with the transaction slip requesting the customer's signature.

[0026] When the final transaction is posted – the customer may have added a tip and the actual total may come out to, say, $48.00 – the customer may or may not be notified again. This depends on the profile associated with the customer.

[0027] In the foregoing scenario, unfortunately, the customer's credit card is less than safe. It is possible, for example, for the server to swipe the

Petitioner Askeladden LLC
Exhibit 1002 - Page 77 of 350

card for one or two additional transactions, to be posted the next day or the next week. With the invention, the additionally swiped transactions would not be authorized, because the customer would decline. If only notification were requested according to the profile, the customer would still be alerted to the questionable transaction and could thus take the necessary countermeasure steps. Still in the same scenario, the credit card number and the name could be copied down very quickly. In addition, the three-digit security code could be copied down as well. The customer's credit card, while physically long returned to the customer, could now be used to make online and telephone purchases.

[0028] It will be understood that the foregoing scenario is merely exemplary and is in no way limiting with regard to the application of the instant invention (nor is it intended to be disparaging to the restaurant industry). Indeed, there exist numerous situations where proper customer notification and customer authorization may prevent fraudulent transactions and even wrongful transactions that are based on honest mistakes.

[0029] It will also be understood that the foregoing description is not only applicable to credit card processing, but also to debit and ATM card processing. The term "charge card" encompasses all of these cards and

Petitioner Askeladden LLC
Exhibit 1002 - Page 78 of 350

equivalent or similar payment mechanisms. For example, if cash is requested at an ATM (automated teller machine), the customer may be prompted to authorize the dispensing of the given amount via his cell phone, in addition to entering the PIN at the ATM terminal. In a further modification, however, it is possible to dispense with the prompt for the PIN entry at the terminal altogether and to only require the entry of a PIN through the customer's cell phone.

[0030] This leads to yet another modification or, rather, to a further application of the novel system according to the invention. It is possible for the customer profile to be set to notify (and/or require confirmation from) a third party. Such third party notification/confirmation may be beneficial in a parent/child relationship, or in an employer/employee relationship. The cell phone (or beeper, or equivalent wireless device) to which the notification is to be sent is set by the cardholder and it may be freely changed through secure access (e.g., by telephone through customer service, online through the Internet).

[0031] Referring now briefly to Fig. 2, after the required information has been gathered at the merchant's (POS, ATM, online, telephone, etc.), an authorization request or charge request 10 is sent to the financial processing

Petitioner Askeladden LLC
Exhibit 1002 - Page 79 of 350

facility 6. There, the request is processed in a conventional manner as indicated by the boxes 11 and 12. At the same time, the customer profile associated with the account number is checked at 13. The customer profile may be set to "no action" or it may not be set at all. In that case, the right-hand branch is immediately terminated. If the profile is set to *Notify Only*, the query 14 returns a corresponding response and the customer's wireless device (e.g., cell phone or beeper) is notified at 15. The message may be an SMS message or it may be a voice announcement, depending on the customer profile. Once the notification has been sent at 15, a flag is set at 16.

[0032] If the customer profile is set to *Notify & Confirm*, the message to the customer's wireless device contains a message as above and a prompt for confirmation at 17. The confirmation may be a simple reply to an SMS message, it may consist of any key depressed (during a live call), or it may be a full fledged PIN or password. In a further modification, which adds yet another level of security, the customer may be prompted for a voice reply and the reply may then be subjected to "voice recognition" by comparing a frequency hysteresis chart associated with the customer to the voice reply.

Petitioner Askeladden LLC
Exhibit 1002 - Page 80 of 350

[0033] If the customer (or the person in the possession of the wireless device) returns the proper response, the query 18 directs the process flow to the box 16, where the confirm flag is once more set to "1." If no response is received, or if an incorrect response is received, the confirm flag is set to "0" at 19.

[0034] At approximately the same time as the confirm flag is set to "1" or "0" – signifying proper or improper notification and/or proper customer side authorization – the financial transaction processing also has reached an end point at 20. If the transaction has been rejected, the merchant is notified accordingly by refusing the transaction at 21. If the financial transaction has been authorized at 20, the process queries whether or not the confirm flag has been set ("1") to indicate that the customer has been notified of the transaction and/or has authorized the transaction at 22. If the flag is not set ("0"), the transaction at the merchant's is refused. If the flag is set, the charge is authorized.

Petitioner Askeladden LLC
Exhibit 1002 - Page 81 of 350

WE CLAIM

1. A method for processing a transaction, comprising the steps of:

receiving a request for authorizing a transaction for an account, said request received via a first transmission channel, said request including at least an identification of the customer's account;

determining whether or not the account includes a request for notification to the customer of any transactions;

notifying the customer via a second transmission channel only if the account includes a request for notification of any transactions;

the second transmission channel being distinct from the first transmission channel; and

authorizing the transaction without requiring a response from the customer.

2. The method according to claim 1, wherein the notifying step comprises sending an SMS message to the customer.

3. The method according to claim 1, wherein the request is from the group consisting of a customer, an account holder, an authorized person, and an unauthorized person .

Petitioner Askeladden LLC
Exhibit 1002 - Page 82 of 350

4. The method according to claim 1, wherein the request is provided from the group consisting of an ATM, a POS terminal, a telephone and a device for virtual communication.

5. The method according to claim 1, wherein the request is a virtual request provided via the Internet.

6. The method according to claim 1, wherein the transaction is selected from the group consisting of credit card, debit card, charge card, and ATM.

7. The method according to claim 1, wherein the first transmission channel is selected from the group consisting of wireless and landline channels.

8. The method according to claim 1, which comprises receiving the request at a remote processing facility.

9. The method according to claim 1, wherein said steps of notifying and authorizing are performed substantially concurrently.

Petitioner Askeladden LLC
Exhibit 1002 - Page 83 of 350

10. A method of notifying an account owner of an impending transaction to an account associated with the account owner, the method comprising:

receiving a message, at a remote processing facility, that a transaction has been requested, the message including at least the account number of an account associated with the account owner;

substantially immediately upon receiving the message, transmitting through a cellular network to a wireless device associated with the account owner, a notification that the transaction has been requested, the notification including sufficient information about the transaction to enable the account owner to take countermeasure steps if the transaction is not to be approved; and

responding to the message by transmitting a response as to whether countermeasure steps have been taken in response to the notification.

11. The method according to claim 10, wherein the notification is an SMS message.

12. The method according to claim 10, wherein the notification includes, in addition to the amount to be charged, information regarding the merchant requesting the charge and a time when the request was made.

Petitioner Askeladden LLC
Exhibit 1002 - Page 84 of 350

13. The method according to claim 10, wherein transaction is an impending charge to a charge account.

14. A method for processing a transaction, comprising the steps of:

a. receiving a request for authorizing a transaction for an account, said request received via a first transmission channel, said request including at least an identification of the customer's account;

b. determining if the account includes a request for notification to the customer of any transactions;

c. sending a notification to the customer via a second transmission channel only if the account includes a request for notification of at least one form of transaction;

d. the second transmission channel being distinct from the first transmission channel;

e. receiving a response to the notification; and

f. authorizing the transaction only if the response is proper.

15. The method according to claim 14, wherein the request is from the group consisting of a customer and an authorized person.

Petitioner Askeladden LLC
Exhibit 1002 - Page 85 of 350

16. The method according to claim 14, wherein the request is provided from the group consisting of an ATM, a POS terminal, a telephone and virtual.

17. The method according to claim 14, wherein the transaction is selected from the group consisting of credit card, debit card, charge card, and ATM.

18. The method according to claim 14, wherein the first transmission channel is selected from the group consisting of wireless and landline channels.

19. The method according to claim 14, wherein the transaction is selected from the group consisting of credit cards, debit cards and ATM cards.

20. The method according to claim 14, wherein the first and second transmission channels are both wireless channels.

21. The method according to claim 14, wherein the request for authorizing a transaction is received from a merchant.

Petitioner Askeladden LLC
Exhibit 1002 - Page 86 of 350

22. The method according to claim 14, wherein the request for authorizing a transaction is received from the group consisting of a merchant and a customer.

23. The method according to claim 14, wherein the response is selected from the group consisting of a reply to an SMS message, a key depressed during a telephone call, a PIN, a password, and a voice reply.

Petitioner Askeladden LLC
Exhibit 1002 - Page 87 of 350

ABSTRACT OF THE DISCLOSURE

An added level of security is provided for charge transactions. Upon presenting a charge card number for a purchase, for example, the cardholder receives a message (e.g., SMS) on his cell phone or PDA that a charge authorization request has been received. The message may include the merchant, a charge amount, and a time and date.

Petitioner Askeladden LLC
Exhibit 1002 - Page 88 of 350

Docket No.: W-9001

COMBINED DECLARATION AND POWER OF ATTORNEY IN ORIGINAL APPLICATION

As a below named inventor, I hereby declare that: my residence, post office address and citizenship are as stated below next to my name; that I verily believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

MOBILE PHONE CHARGE CARD NOTIFICATION AND AUTHORIZATION METHOD

described and claimed in the specification bearing that title, that I understand the content of the specification, that I do not know and do not believe the same was ever known or used in the United States of America before my or our invention thereof, or patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months prior to this application, that I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in 37 CFR § 1.56, and that no application for patent or inventor's certificate of this invention has been filed earlier than the following in any country foreign to the United States prior to this application by me or my legal representatives or assigns:

I hereby appoint practitioners associated with the Customer Number

24131

as my attorneys and/or agents to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith.

Address all correspondence and telephone calls to the mailing address/contact numbers associated with Customer Number

24131

LERNER AND GREENBERG, P.A.
POST OFFICE BOX 2480
HOLLYWOOD, FLORIDA 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF FIRST JOINT INVENTOR: Gerry CALABRESE

Inventor's Signature

3-11-05
Date

Residence: Fort Lauderdale, Florida

Country of Citizenship: United States of America

Post Office Address: 15951 S.W. 41st Street, Suite 600
Fort Lauderdale, FL 33331

FULL NAME OF SECOND JOINT INVENTOR: Werner STEMER

Inventor's Signature

3/11/2005
Date

Residence: Fort Lauderdale, Florida

Country of Citizenship: Austria

Post Office Address: 1008 SW 5th Place
Fort Lauderdale, FL 33312

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W-9001D3
	Application Number	
Title of Invention	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	GERRY		CALABRESE	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	SOUTHWEST RANCHES	State/Province	FL	Country of Residence i	US

Mailing Address of Inventor:

Address 1	13810 EAST PALOMINO DRIVE		
Address 2			
City	SOUTHWEST RANCHES	State/Province	FL
Postal Code	33330	Country i	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	WERNER		STEMER	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	FORT LAUDERDALE	State/Province	FL	Country of Residence i	US

Mailing Address of Inventor:

Address 1	1008 SW 5 PLACE		
Address 2			
City	FORT LAUDERDALE	State/Province	FL
Postal Code	33312	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W-9001D3
	Application Number	
Title of Invention	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD	

☐ An Address is being provided for the correspondence Information of this application.			
Customer Number	24131		
Email Address	OFFICE@PATENTUSA.COM	Add Email	Remove Email

Application Information:

Title of the Invention	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD		
Attorney Docket Number	W-9001D3	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	2	**Suggested Figure for Publication (if any)**	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for thr Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	24131		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13088514	2011-04-18

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W-9001D3
	Application Number	
Title of Invention	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD	

Prior Application Status	Patented			Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13088514	Continuation of	12043235	2008-03-06	7954706	2011-06-07
Prior Application Status	Patented			Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12043235	Division of	11077783	2005-03-11	7357310	2008-04-15

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country i	Filing Date (YYYY-MM-DD)	Priority Claimed
			◉ Yes ○ No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W-9001D3
	Application Number	
Title of Invention	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Remove

◯ Assignee	◯ Legal Representative under 35 U.S.C. 117
◯ Person to whom the inventor is obligated to assign.	◯ Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information:

Address 1			
Address 2			
City		**State/Province**	
Country [i]		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

Signature	/WERNER H. STEMER/			Date (YYYY-MM-DD)	2013-08-23
First Name	WERNER	Last Name	STEMER	Registration Number	34956

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W-9001D3
	Application Number	
Title of Invention	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Petitioner Askeladden LLC
Exhibit 1002 - Page 96 of 350

Docket No.: W-9001D3

DECLARATION

As a below named inventor, I hereby declare that:

- this declaration is directed to the attached application entitled

  TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD

  which claims the benefit of Application No. 11/007,783, filed March 11, 2011, now U.S. patent No. 7,357,310 B2; Application No. 12/043,235, filed March 6, 2008, now U.S. patent No. 7,954,706 B2; and copending application No. 13/088,514, filed April 18, 2011;
- I believe that I am the original inventor or an original joint inventor of a claimed invention in this application;
- the application was made or authorized to be made by me.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. § 1001 by fine or imprisonment of not more than five (5) years, or both.

LEGAL NAME OF INVENTOR: **GERRY CALABRESE**

Signature

8/23/13
Date

LEGAL NAME OF INVENTOR: **WERNER STEMER**

Signature

Aug. 23, 2013
Date

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD
First Named Inventor/Applicant Name:	GERRY CALABRESE
Filer:	Werner H. Stemer/Rebekka Rymanowski
Attorney Docket Number:	W-9001D3

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Claims:				
Claims in excess of 20	2202	3	40	120
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**850**

Electronic Acknowledgement Receipt

EFS ID:	16667728
Application Number:	13974462
International Application Number:	
Confirmation Number:	4957
Title of Invention:	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD
First Named Inventor/Applicant Name:	GERRY CALABRESE
Customer Number:	24131
Filer:	Werner H. Stemer/Michelle Janca
Filer Authorized By:	Werner H. Stemer
Attorney Docket Number:	W-9001D3
Receipt Date:	23-AUG-2013
Filing Date:	
Time Stamp:	14:28:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$850
RAM confirmation Number	880
Deposit Account	121099
Authorized User	GREENBERG, LAURENCE A

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Authorization for Extension of Time all replies	W-9001D3-ChargeAuthorization.pdf	73577 c1d3190bb553f734baef4ce877d503d821ffe216	no	1
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	W-9001D3-IDSForm.pdf	613350 e2ad65710f2d157c02895 1886a5c95e4909dfe97	no	6
Warnings:					
Information:					
3	Foreign Reference	EP0745961A2.pdf	1413586 43f84d34056c65f4af60fe5733582148c63c3ce6	no	25
Warnings:					
Information:					
4	Foreign Reference	EP1136961A1.pdf	2279423 0779ee78b2b176da55af2a16bb0e60330ab61e6c	no	32
Warnings:					
Information:					
5	Drawings-only black and white line drawings	W-9001Figs-.pdf	42584 caec5aa4b5eafec7073a3b4b07669daf465784c4	no	2
Warnings:					
Information:					
6		W-9001D3-Specification.pdf	187541 23fb256a7e6878088ade96918e89593373aacb11	yes	23

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	16
Claims	17	22
Abstract	23	23

Warnings:					
Information:					
7	Oath or Declaration filed	W-9001-SignedDecl.pdf	97875 cbc2a8cd7e8e07ea4eb2fa169fe51b104f0a3e97	no	2

Warnings:					
Information:					
8	Application Data Sheet	W-9001D3-ADS.pdf	1882384 75edd27e42755b09d39aee0ced10360e39d3958a	no	6
Warnings:					
Information:					
9	Oath or Declaration filed	W-9001D3-Declaration-signed.pdf	66200 7d9fc4e3093e78960a2e0b1c3ded3f2d8bf3752e	no	1
Warnings:					
Information:					
10	Fee Worksheet (SB06)	fee-info.pdf	36755 3ccdf08d88b91491155e15910ea34926e960f2d5	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	6693275	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Docket No.: W-9001D3

CHARGE AUTHORIZATION

The Patent Office is hereby authorized to charge any fees due under 37 CFR §§ 1.16 and 1.17 or deficiencies in required fees to deposit account 12-1099 of Lerner Greenberg Stemer LLP during the pendency of this application.

/Werner H. Stemer/
Werner H. Stemer
Reg. No. 34,956

Practitioner's Docket No.: W-9001D3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.	:	13/974,462	Confirmation No. 4957
Filing Date	:	August 23, 2013	
Applicant	:	Gerry Calabrese, et al.	
Title	:	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD	
Docket No.	:	W-9001D3	
Customer No.	:	24131	

Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR EARLY PUBLICATION

Sir:

In accordance with 37 CFR §1.219, applicants herewith request early publication of the above-identified application. The fee in the amount of $300.00 is submitted herewith.

Respectfully submitted,

/Werner H. Stemer/
Werner H. Stemer
Reg. No. 34956

September 11, 2013
Lerner Greenberg Stemer LLP
P.O. Box 2480
Hollywood, Florida 33022-2480
Tel.: (954) 925-1100
Fax: (954) 925-1101 /bb

Petitioner Askeladden LLC
Exhibit 1002 - Page 104 of 350

Electronic Patent Application Fee Transmittal

Application Number:	13974462
Filing Date:	23-Aug-2013
Title of Invention:	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD
First Named Inventor/Applicant Name:	GERRY CALABRESE
Filer:	Werner H. Stemer/Birgit Bartell
Attorney Docket Number:	W-9001D3

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Publ. Fee- Early, Voluntary, or Normal	1504	1	300	300
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**300**

Electronic Acknowledgement Receipt

EFS ID:	16826653
Application Number:	13974462
International Application Number:	
Confirmation Number:	4957
Title of Invention:	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD
First Named Inventor/Applicant Name:	GERRY CALABRESE
Customer Number:	24131
Filer:	Werner H. Stemer/Michelle Janca
Filer Authorized By:	Werner H. Stemer
Attorney Docket Number:	W-9001D3
Receipt Date:	11-SEP-2013
Filing Date:	23-AUG-2013
Time Stamp:	16:31:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$300
RAM confirmation Number	3675
Deposit Account	121099
Authorized User	GREENBERG, LAURENCE A

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Early Publication	W-9001-EarlyPublication.pdf	59189 1fd21af8df3742ac5a5c4cec26cedd042c1955b5	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30223 38f0d293c3895bcd1499493bd31efbf419029dc8	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	89412		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/974,462

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	23 minus 20 =	* 3	x 40 =	120	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	850		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/974,462	08/23/2013	2876	1150	W-9001D3	23	3

CONFIRMATION NO. 4957

24131
LERNER GREENBERG STEMER LLP
P O BOX 2480
HOLLYWOOD, FL 33022-2480

FILING RECEIPT

OC000000063748495

Date Mailed: 09/17/2013

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

GERRY CALABRESE, SOUTHWEST RANCHES, FL;
WERNER STEMER, FORT LAUDERDALE, FL;

Applicant(s)

GERRY CALABRESE, SOUTHWEST RANCHES, FL;
WERNER STEMER, FORT LAUDERDALE, FL;

Power of Attorney: The patent practitioners associated with Customer Number 24131

Domestic Priority data as claimed by applicant

This application is a CON of 13/088,514 04/18/2011
which is a CON of 12/043,235 03/06/2008 PAT 7954706
which is a DIV of 11/077,783 03/11/2005 PAT 7357310

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 09/11/2013
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/974,462**
Projected Publication Date: 12/26/2013
Non-Publication Request: No
Early Publication Request: Yes
** **SMALL ENTITY** **

Petitioner Askeladden LLC
Exhibit 1002 - Page 110 of 350

Title

TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD

Preliminary Class

235

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

Petitioner Askeladden LLC
Exhibit 1002 - Page 111 of 350

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/974,462	08/23/2013	GERRY CALABRESE	W-9001D3	4957

24131 7590 12/04/2013
LERNER GREENBERG STEMER LLP
P O BOX 2480
HOLLYWOOD, FL 33022-2480

EXAMINER	
KIM, AHSHIK	
ART UNIT	PAPER NUMBER
2876	
MAIL DATE	DELIVERY MODE
12/04/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Petitioner Askeladden LLC
Exhibit 1002 - Page 113 of 350

Office Action Summary	Application No. 13/974,462	Applicant(s) CALABRESE ET AL.	
	Examiner AHSHIK KIM	Art Unit 2876	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *8/23/13 (initial filing of application)*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-23* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☒ Claim(s) *1-9 and 14-23* is/are allowed.

7)☒ Claim(s) *10-13* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *8/23/13* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *8/23/13*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

Petitioner Askeladden LLC
Exhibit 1002 - Page 114 of 350

DETAILED ACTION

1. The present application is being examined under the pre-AIA first to invent provisions.

2. This is the first action relating to U.S. Application Serial No. 13/974,462 filed on August 23, 2013. Currently claims 1-23 remain in the examination.

3. Applicant's disclosure of related application information is acknowledged.

Claim Rejections - 35 USC § 102

4. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

5. The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 10-13 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by US 2002/0143634 A1 to Kumar et al. (hereinafter "Kumar").

Regarding claim 10, Kumar discloses a method and a payment system wherein a buyer initiates a transaction using a first transmission channel from the buyer's computer system 435

(see figure 4 and paragraphs 0054-0058); and the transaction including account number (see paragraph 0040); the server sending message to a buyer's mobile phone using cellular network and notifying the buyer about the impending transaction with the transaction details (see paragraphs 0041,0049, and steps 352 in figure 3B). Responding to the message, the can approve or reject the transaction (see paragraph 0041). Rejection of transaction can certainly be construed to be a countermeasure responding to the notification.

Regarding claim 11, the notification is an SMS message (see paragraphs 0041 and 0049).

Regarding claim 12, the transaction data includes MID – a merchant identifier and a POS device ID (see paragraph 0031 and 0038). Although not stated in explicit manner, POS, when generating transaction record, includes an automatic timestamp of the when the transaction is initiated or transmitted.

Regarding claim 13, the POS reads credit card or debit card (see paragraph 0029), which is linked to a credit account or a debit account.

Allowable Subject Matter

7. Claims 1-9 and 14-23 are allowed.

8. The following is a statement of reasons for the indication of allowable subject matter: The claims are directed at a method for processing transaction wherein a request for authorizing a transaction is received via a first transmission channel and notifying the customer via a transmission channel about the transaction. The notification is made only if the customer account includes a request for notification of transactions. Such a method is neither disclosed nor suggested by the cited references. .

Conclusion

The pertinent prior arts made of record but not relied are listed in the attached form PTO-892. These are considered pertinent to Applicant's disclosure. Applicant is respectfully suggested to carefully review these references.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to *Ahshik Kim* whose telephone number is (571)272-2393. The examiner can normally be reached between the hours of 8:00 AM to 5:00 PM Monday thru Friday. Examiner's fax phone number is (571)273-2393.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee, can be reached on (571)272-2398. The fax phone number for this Group is (571)273-8300.

Communications via Internet e-mail regarding this application, other than those under 35 U.S.C. 132 or which otherwise require a signature, may be used by the applicant and should be addressed to [ahshik.kim@uspto.gov].

PTO employees do not engage in Internet communications where there exists a possibility that sensitive information could be identified or exchanged unless the record includes a properly signed express waiver of the confidentiality requirements of 35 U.S.C. 122. This is more clearly set forth in the Interim Internet Usage Policy published in the Official Gazette of the Patent and Trademark on February 25, 1997 at 1195 OG 89.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/AHSHIK KIM/
Primary Examiner, Art Unit 2876

December 2, 2013

Notice of References Cited	Application/Control No. 13/974,462	Applicant(s)/Patent Under Reexamination CALABRESE ET AL.	
	Examiner AHSHIK KIM	Art Unit 2876	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2002/0143634	10-2002	Kumar et al.	705/18
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Petitioner Askeladden LLC
Exhibit 1002 - Page 119 of 350

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	
	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	W-9001D3

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5221838		1993-06-22	Gutman et al.	
	2	5359182		1994-10-25	Schilling	
	3	5521363		1996-05-28	Tannenbaum	
	4	6366893	B2	2002-04-02	Hannula et al.	
	5	6442532	B1	2002-08-27	Kawan	
	6	6494367	B1	2002-12-17	Zacharias	
	7	6726098	B2	2004-04-27	Schilling	
	8	6754636	B1	2004-06-22	Walker et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.K./

Receipt date: 08/23/2013	Application Number	13974462 - GAU: 2876
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	W-9001D3

	9	7024396	B2	2006-04-04	Woodward	
	10	7181432	B2	2007-02-20	Wells et al.	
	11	5530438	A	1996-06-25	Bickham et al.	
	12	5615110	A	1997-03-25	Wong	
	13	6064990	A	2000-05-16	Goldsmith	
	14	7096003	B2	2006-08-22	Joao et al.	
	15	7389275	B2	2008-06-17	Kemper et al.	
	16	5708422	A	1998-01-13	Blonder et al.	Corresponds to EP 0745961 A2
	17	5903830	A	1999-05-11	Joao et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.K./

Receipt date: 08/23/2013	Application Number	13974462 - GAU: 2876
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	W-9001D3

	1	20020035539	A1	2002-03-21	O'Connell	
	2	20020107755	A1	2002-08-08	Steed et al.	
	3	20020107791	A1	2002-08-08	Nobrega et al.	
	4	20020156689	A1	2002-10-24	Spalding	
	5	20030221125	A1	2003-11-27	Rolfe	
	6	20070027803	A1	2007-02-01	Brandes et al.	Corresponds to EP 1136961 A1

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1136961	EP	A1	2001-09-26	Calvo et al.	Published in the English language and corresponds to US 20070027803 A1	☐
	2	0745961	EP	A2	1996-12-04	Blonder et al.	Published in the English language and corresponds to US 5708422 A	☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.K./

Receipt date: 08/23/2013	Application Number	13974462 - GAU: 2876
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	W-9001D3

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Ahshik Kim/	Date Considered	12/01/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.K./

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 4957

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/974,462	08/23/2013 RULE	235	2876	W-9001D3

APPLICANTS

INVENTORS

GERRY CALABRESE, SOUTHWEST RANCHES, FL;
WERNER STEMER, FORT LAUDERDALE, FL;

**** CONTINUING DATA ***************************

This application is a CON of 13/088,514 04/18/2011
which is a CON of 12/043,235 03/06/2008 PAT 7954706
which is a DIV of 11/077,783 03/11/2005 PAT 7357310

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
09/11/2013

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ Yes ☑ No	☐ Yes ☑ No	/AHSHIK KIM/ Examiner's Signature	☐ Initials	FL	2	23	3

ADDRESS

LERNER GREENBERG STEMER LLP
P O BOX 2480
HOLLYWOOD, FL 33022-2480
UNITED STATES

TITLE

TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD

FILING FEE RECEIVED		
1150	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13974462	CALABRESE ET AL.
	Examiner	Art Unit
	AHSHIK KIM	2876

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/01/2013								
	1	=								
	2	=								
	3	=								
	4	=								
	5	=								
	6	=								
	7	=								
	8	=								
	9	=								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	=								
	15	=								
	16	=								
	17	=								
	18	=								
	19	=								
	20	=								
	21	=								
	22	=								
	23	=								

Petitioner Askeladden LLC
Exhibit 1002 - Page 125 of 350

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13974462	CALABRESE ET AL.
	Examiner	Art Unit
	AHSHIK KIM	2876

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
235	380	12/1/2013	ak
	382	12/1/2013	ak
	379	12/1/2013	ak
705	77		ak

SEARCH NOTES		
Search Notes	Date	Examiner
See attached EAST search history	12/1/2013	ak
Reviewed parent cases	12/1/2013	ak

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	"235"/$7.ccls. and "forslund".in.	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2006/09/20 20:05
S2	5	("5015830" | "5613159" | "5635701" | "5895903" | "5936220").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2006/06/05 11:27
S3	21	("6250557").URPN.	USPAT	OR	OFF	2006/06/05 11:29
S4	16	"235"/$7.ccls. and ("financial" with "transaction" with "wireless"$3)	USPAT	OR	ON	2006/06/05 11:30
S5	38	("4305059" | "4424529" | "4529870" | "4575621" | "4686407" | "4707592" | "4819039" | "4965568" | "5159632" | "5192947" | "5265033" | "5285496" | "5347580" | "5359182" | "5371493" | "5412192" | "5440634" | "5442707" | "5452356" | "5453601" | "5455864" | "5467398" | "5473143" | "5473667" | "5477215" | "5481255" | "5483595" | "5510778" | "5521363" | "5539189" | "5541583" | "5557518" | "5572004" | "5585787" | "5585789" | "5590038" | "5591949" | "5754655").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2006/06/05 11:31
S6	104	("5359182").URPN.	USPAT	OR	OFF	2006/06/05 11:33
S7	36	("4305059" | "4529870" | "4575621" | "4707592" | "5159632" | "5192947" | "5221838" | "5265033" | "5285496" | "5347580" | "5359182" | "5371493" | "5412192" | "5440634" | "5442707" | "5452356" | "5453601" | "5455864" | "5467398" | "5473143" | "5473667" | "5477215" | "5481255" | "5483595" | "5510778" | "5521363" | "5539189" | "5541583" | "5557518" | "5572004" | "5585787" | "5585789" | "5590038" | "5591949" | "5929773" | "6144848").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2006/06/05 11:35
S8	93	"235"/$7.ccls. and ("financial" with "transaction" with "approv"$6)	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2006/06/05 11:57
S9	105	"235"/$7.ccls. and ("financial" with "transaction" with "approv"$6)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2006/06/05 11:57

Petitioner Askeladden LLC
Exhibit 1002 - Page 127 of 350

S10	46	S9 and "wireless"$3	US-PGPUB; USPAT; EPO; JPO	OR	ON	2006/06/05 11:57
S11	215	("5221838").URPN.	USPAT	OR	OFF	2006/06/05 12:01
S12	93	S11 and "wireless"$3	USPAT	OR	OFF	2006/06/05 12:01
S13	4	("5221838" | "5387784" | "5608778" | "5887266").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2006/06/05 12:23
S14	1	("6442532").PN.	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2006/06/05 12:37
S15	133	"235"/$7.ccls. and "lapstun".in.	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2006/06/06 09:11
S16	1	("6442532").PN.	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2006/09/20 14:49
S17	108	("5359182").URPN.	USPAT	OR	OFF	2006/09/20 15:07
S18	1	"235"/$7.ccls. and "forslund".in.	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2006/09/20 15:15
S19	5	("5015830" | "5613159" | "5635701" | "5895903" | "5936220").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2006/09/20 15:18
S20	21	("6250557").URPN.	USPAT	OR	OFF	2006/09/20 15:18
S21	20	("20020023215" | "20020038287" | "20020046185" | "20020077993" | "20020107755" | "20020143634" | "20020143655" | "20020169719" | "20020179704" | "20030024979" | "20030061170" | "20030154139" | "20040078328" | "20050131838" | "5221838" | "6026379" | "6212634" | "6250557" | "6270011" | "6938019").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2006/09/20 15:19
S22	13	"235"/$7.ccls. and ("notif"$8 with "phone" with "transaction")	US-PGPUB; USPAT; EPO; JPO	OR	ON	2006/09/20 20:17
S23	81	"235"/$7.ccls. and ("authoriz"$8 with "phone" with "transaction")	US-PGPUB; USPAT; EPO;	OR	ON	2006/09/20 20:17

Petitioner Askeladden LLC
Exhibit 1002 - Page 128 of 350

			JPO			
S24	33	S23 and "pos"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2006/09/20 20:17
S25	1	("6442532").PN.	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2006/10/11 09:58
S26	1	11/077783	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2007/03/05 13:07
S27	20	("20020023215" | "20020038287" | "20020046185" | "20020077993" | "20020107755" | "20020143634" | "20020143655" | "20020169719" | "20020179704" | "20030024979" | "20030061170" | "20030154139" | "20040078328" | "20050131838" | "5221838" | "6026379" | "6212634" | "6250557" | "6270011" | "6938019").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2007/03/05 13:27
S28	774	"pos" with "wireless"	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2007/03/05 13:48
S29	177	"pos" with "wireless" with "transaction"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2007/03/05 13:48
S30	27	("235"/$7.ccls. or "705"/$7.ccls.) and ("preauthoriz"$6 with "time")	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2007/03/07 10:04
S31	27	("235"/$7.ccls. or "705"/$7.ccls.) and ("preauthoriz"$6 with "time")	US-PGPUB; USPAT; EPO; JPO	OR	ON	2007/03/07 10:05
S32	131	("235"/$7.ccls. or "705"/$7.ccls.) and (("preauthoriz"$6 or "pre-authori"$6) with "time")	US-PGPUB; USPAT; EPO; JPO	OR	ON	2007/03/07 10:06
S33	44	S32 and "pos"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2007/03/07 10:06
S34	0	11/557171	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2007/03/07 14:06

Petitioner Askeladden LLC
Exhibit 1002 - Page 129 of 350

S35	1	11/077783	US-PGPUB; USPAT; EPO; JPO	OR	OFF	2007/09/19 17:04
S36	1	("7357310").PN.	USPAT; USOCR	OR	OFF	2010/11/03 11:40
S37	75	("235"/$7.ccls. or "705"/$7.ccls.) and ("approv"$6 with ("preauthorized" or "pre-authorized"))	US-PGPUB; USPAT	OR	ON	2010/11/03 12:42
S38	1475	("235"/$7.ccls. or "705"/$7.ccls.) and (("preapproved" or "pre-approved"))	US-PGPUB; USPAT	OR	ON	2010/11/03 12:44
S39	143	("235"/$7.ccls. or "705"/$7.ccls.) and (("preapproved" or "pre-approved") with ("transaciton" or "purchase"))	US-PGPUB; USPAT	OR	ON	2010/11/03 12:44
S40	109	("235"/$7.ccls. or "705"/$7.ccls.) and (("preapproved" or "pre-approved" or "preauthorized" or "preauthorized") with "code")	US-PGPUB; USPAT	OR	ON	2010/11/03 13:16
S41	23	("235"/$7.ccls. or "705"/$7.ccls.) and (("preapproved" or "pre-approved" or "preauthorized" or "preauthorized") with "voice")	US-PGPUB; USPAT	OR	ON	2010/11/03 13:48
S42	53	("235"/$7.ccls. or "705"/$7.ccls.) and (("preapproved" or "pre-approved" or "preauthorized" or "preauthorized") same "voice")	US-PGPUB; USPAT	OR	ON	2010/11/03 13:48
S43	2	(("7954706") or ("7357210")).PN.	USPAT; USOCR	OR	OFF	2012/05/06 17:19
S44	2	(("7395961") or ("6685093")).PN.	USPAT; USOCR	OR	OFF	2012/05/18 15:32
S45	1	("20020107791").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/06 13:37
S46	102	("235"/$7.ccls. or "705"/$7.ccls.) and (("unauthorized" or "suspect" or "suspicious") with ("transaction" or "purchas"$4) with "notif"$4)	US-PGPUB; USPAT	OR	ON	2013/03/07 14:16
S47	28	("3723655" | "3938090" | "4485300" | "4758714" | "4947027" | "5173594" | "5177342" | "5243645" | "5335278" | "5345595" | "5357563" | "5406619" | "5444616" | "5444763" | "5473667" | "5479510" | "5485510" | "5513250" | "5526407" | "5530438" | "5615110" | "5631947" | "5655007" | "5661285" | "5699528" | "5708422" | "5878337" | "5903830").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/07 14:17
S48	28	("3723655" | "3938090" | "4485300" | "4758714" | "4947027" | "5173594" | "5177342" | "5243645" | "5335278" | "5345595" | "5357563" | "5406619" | "5444616" | "5444763" | "5473667" | "5479510" | "5485510" | "5513250" | "5526407" | "5530438" | "5615110" | "5631947" | "5655007" | "5661285" | "5699528" | "5708422" | "5878337" |	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/07 14:17

Petitioner Askeladden LLC
Exhibit 1002 - Page 130 of 350

		"5903830").PN.				
S49	1	("7954706").PN.	USPAT; USOCR	OR	OFF	2013/03/07 14:34
S50	1	13/088514	US-PGPUB; USPAT	OR	OFF	2013/03/07 14:36
S51	234	("235"/$7.ccls. or "705"/$7.ccls.) and (("telephone" or "phone") with "approv"$4 with "transaction")	USPAT	OR	ON	2013/11/25 14:24
S52	760	("235"/$7.ccls. or "705"/$7.ccls.) and (("telephone" or "phone") with "approv"$4 with "transaction")	US-PGPUB; USPAT	OR	ON	2013/11/25 14:25
S53	419	("5283829").URPN.	USPAT	OR	OFF	2013/11/25 14:37

EAST Search History (Interference)

<This search history is empty>

12/1/2013 11:33:51 PM
C:\Users\akim2\Documents\EAST\Workspaces\C11077783.wsp

Petitioner Askeladden LLC
Exhibit 1002 - Page 131 of 350

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/974,462	08/23/2013	GERRY CALABRESE	W-9001D3

CONFIRMATION NO. 4957

24131
LERNER GREENBERG STEMER LLP
P O BOX 2480
HOLLYWOOD, FL 33022-2480

PUBLICATION NOTICE



Title:TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD

Publication No.US-2013-0346312-A1
Publication Date:12/26/2013

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Petitioner Askeladden LLC
Exhibit 1002 - Page 132 of 350

W-9001D3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applic. No.	:	13/974,462	Confirmation No: 4957
Applicant	:	Gerry Calabrese, et al.	
Filed	:	August 23, 2013	
Title	:	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD	
Art Unit	:	2876	
Examiner	:	Ahshik Kim	
Docket No.	:	W-9001D3	
Customer No.	:	24131	

Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

A M E N D M E N T

S i r :

Responsive to the Office action dated December 4, 2013 kindly amend the above-identified application as follows:

- **Amendments to the Claims** begin on page 2 of this paper.
- **Remarks/Arguments** begin on page 7 of this paper.

Petitioner Askeladden LLC
Exhibit 1002 - Page 133 of 350

Amendments to the Claims

Listing of Claims:

Claim 1 (original). A method for processing a transaction, comprising the steps of:

receiving a request for authorizing a transaction for an account, said request received via a first transmission channel, said request including at least an identification of the customer's account;

determining whether or not the account includes a request for notification to the customer of any transactions;

notifying the customer via a second transmission channel only if the account includes a request for notification of any transactions;

the second transmission channel being distinct from the first transmission channel; and

authorizing the transaction without requiring a response from the customer.

Claim 2 (original). The method according to claim 1, wherein the notifying step comprises sending an SMS message to the customer.

Petitioner Askeladden LLC
Exhibit 1002 - Page 134 of 350

Claim 3 (original). The method according to claim 1, wherein the request is from the group consisting of a customer, an account holder, an authorized person, and an unauthorized person .

Claim 4 (original). The method according to claim 1, wherein the request is provided from the group consisting of an ATM, a POS terminal, a telephone and a device for virtual communication.

Claim 5 (original). The method according to claim 1, wherein the request is a virtual request provided via the Internet.

Claim 6 (original). The method according to claim 1, wherein the transaction is selected from the group consisting of credit card, debit card, charge card, and ATM.

Claim 7 (original). The method according to claim 1, wherein the first transmission channel is selected from the group consisting of wireless and landline channels.

Claim 8 (original). The method according to claim 1, which comprises receiving the request at a remote processing facility.

Petitioner Askeladden LLC
Exhibit 1002 - Page 135 of 350

Claim 9 (original). The method according to claim 1, wherein said steps of notifying and authorizing are performed substantially concurrently.

Claim 10 -13 (canceled).

Claim 14 (original). A method for processing a transaction, comprising the steps of:

a. receiving a request for authorizing a transaction for an account, said request received via a first transmission channel, said request including at least an identification of the customer's account;

b. determining if the account includes a request for notification to the customer of any transactions;

c. sending a notification to the customer via a second transmission channel only if the account includes a request for notification of at least one form of transaction;

d. the second transmission channel being distinct from the first transmission channel;

e. receiving a response to the notification; and

f. authorizing the transaction only if the response is proper.

Petitioner Askeladden LLC
Exhibit 1002 - Page 136 of 350

Claim 15 (original). The method according to claim 14, wherein the request is from the group consisting of a customer and an authorized person.

Claim 16 (original). The method according to claim 14, wherein the request is provided from the group consisting of an ATM, a POS terminal, a telephone and virtual.

Claim 17 (original). The method according to claim 14, wherein the transaction is selected from the group consisting of credit card, debit card, charge card, and ATM.

Claim 18 (original). The method according to claim 14, wherein the first transmission channel is selected from the group consisting of wireless and landline channels.

Claim 19 (original). The method according to claim 14, wherein the transaction is selected from the group consisting of credit cards, debit cards and ATM cards.

Petitioner Askeladden LLC
Exhibit 1002 - Page 137 of 350

Claim 20 (original). The method according to claim 14, wherein the first and second transmission channels are both wireless channels.

Claim 21 (original). The method according to claim 14, wherein the request for authorizing a transaction is received from a merchant.

Claim 22 (original). The method according to claim 14, wherein the request for authorizing a transaction is received from the group consisting of a merchant and a customer.

Claim 23 (original). The method according to claim 14, wherein the response is selected from the group consisting of a reply to an SMS message, a key depressed during a telephone call, a PIN, a password, and a voice reply.

Petitioner Askeladden LLC
Exhibit 1002 - Page 138 of 350

REMARKS/ARGUMENTS

Reconsideration of the application is requested.

Claims 1-9 and 14-23 are now in the application. Claims 10-13 have been canceled. Since claims 1-9 and 14-23 have been allowed, the application is now in condition for allowance.

An Information Disclosure Statement is being submitted concurrently herewith. The prior art listed therein was found during a recent search of prior art. The additional prior art does not originate from a corresponding foreign application and, as such, the second certification in the IDS form applies. Applicants apologize for the relatively late submission of prior art. The Examiner is thanked in advance for reviewing the documents vis-a-vis the claimed invention.

Respectfully submitted,

/Werner H. Stemer/

Werner H. Stemer
(Reg. No. 34,956)

WHS:ay - January 14, 2014
Lerner Greenberg Stemer LLP
P.O. Box 2480
Hollywood, Florida 33022-2480
Tel.: 954·925·1100
Fax: 954·925·1101

Petitioner Askeladden LLC
Exhibit 1002 - Page 139 of 350

Electronic Acknowledgement Receipt

EFS ID:	17904813
Application Number:	13974462
International Application Number:	
Confirmation Number:	4957
Title of Invention:	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD
First Named Inventor/Applicant Name:	GERRY CALABRESE
Customer Number:	24131
Filer:	Werner H. Stemer
Filer Authorized By:	
Attorney Docket Number:	W-9001D3
Receipt Date:	14-JAN-2014
Filing Date:	23-AUG-2013
Time Stamp:	15:22:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	W-9001D3-IDS.pdf	614354 ef1576cf6da7ebaf16d685ebff65826fb414904b	no	6

Warnings:	
Information:	

2	Foreign Reference	WO1999014711.pdf	1377093 4a406b5577c0efd259e81dd378858e7e55bb2078	no	32
Warnings:					
Information:					
3	Foreign Reference	FR2823882.pdf	532248 45a39ba971708923f5b577ee9086a163427a3df7	no	24
Warnings:					
Information:					
4	Foreign Reference	WO2005031541.pdf	611881 6fe4c02b2b4a6f57a993bb71f4a9c40fe1697b6f	no	14
Warnings:					
Information:					
5	Foreign Reference	EP1067492A3.pdf	107881 3e3814753a4fe973fa4c9a419978f88bc2fbc7b8	no	3
Warnings:					
Information:					
6	Foreign Reference	EP2287793A1.pdf	544717 03fe5a82b64bdc6147a9dfe3eb89c8ef018286f7	no	16
Warnings:					
Information:					
7	Foreign Reference	WO2003046778.pdf	641107 fd28aeff6562e99cde746d4207e70d1b5ac6630d	no	18
Warnings:					
Information:					
8	Foreign Reference	WO2001093213.pdf	1159489 39169e8cea1433e6a1bb884c2a41a8d1d43dc987	no	29
Warnings:					
Information:					
9	Foreign Reference	WO2002082392.pdf	931016 c4209a7e3c3cd89af686f64f97824c8484d96a88	no	22
Warnings:					
Information:					
10	Non Patent Literature	NPL-1.pdf	117870 21f993c1c9a4d9f18921bfc926af761786cbe4eb	no	6
Warnings:					
Information:					

11	Non Patent Literature	NPL-2-.pdf	495149 12873a35e93801cc06d8fa323069dfb97a821d89	no	23
Warnings:					
Information:					
12	Non Patent Literature	NPL-3-.pdf	6162534 6c811759f26f2f7403b00a8343818fe2c67af8c0	no	12
Warnings:					
Information:					
13	Non Patent Literature	NPL-4.pdf	73284 ed528fb41bf33e039535c8c54838e3ea499ed5b6	no	13
Warnings:					
Information:					
14	Non Patent Literature	NPL-5-.pdf	199051 15d3265c1900029e7548212 8b4061f7c60c9e40c	no	6
Warnings:					
Information:					
15	Non Patent Literature	NPL-6.pdf	78245 f11343677cc444a74311ef010ca68fe94b3788f6	no	17
Warnings:					
Information:					
16	Non Patent Literature	NPL-7-.pdf	272420 6e464157acd7305e6e36f6329872502748bc0899	no	7
Warnings:					
Information:					
17	Non Patent Literature	NPL-8-.pdf	5345 97fbda4470caba2f0dd91720fa2e012372f68bdf	no	2
Warnings:					
Information:					
18	Non Patent Literature	NPL-9-.pdf	232262 6a262a5b4c302f58aee67c2a01977714729c9e41	no	6
Warnings:					
Information:					
19	Non Patent Literature	D1-Emerging_eCommerce_2002-.pdf	158771 b717402968215c7c66cd3aec3c6bb1dd5c81131c	no	8
Warnings:					
Information:					

20	Non Patent Literature	D2-MobilePayment_2004-.pdf	540629 5f19a5178c2d1ac5ba4d04dd5fdd894bbcb4510a	no	23
Warnings:					
Information:					
21	Non Patent Literature	D3-Enhancing_security_2003-.pdf	834060 f1a18218802dc9c88197b463f3689e6442d7c4af	no	183
Warnings:					
Information:					
22	Non Patent Literature	D4-Authorization_2004.pdf	143683 2b1902178f0035a5c23f81a9d1a45e88079e11c5	no	11
Warnings:					
Information:					
23	Non Patent Literature	D5-MobileSecurity_2001-.pdf	5362 923b925b7ae95eecea8a28551bfc36874e8fa7a7	no	2
Warnings:					
Information:					
24		W-9001D3-am1.pdf	108044 20c70bf04732b12b9b93f1f2a444bbd9c162ffce	yes	7

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	6
Applicant Arguments/Remarks Made in an Amendment	7	7

Warnings:	
Information:	
Total Files Size (in bytes):	15946495

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	13974462
Filing Date	2013-08-23
First Named Inventor	Gerry Calabrese et al.
Art Unit	2876
Examiner Name	Ahshik Kim
Attorney Docket Number	W-9001D3

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8296228	B1	2012-10-23	Kloor	
	2	7427021	B2	2008-09-23	Kemper et al.	Corresponds to EP 2287793 A1

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010051920	A1	2001-12-13	Joao et al.	
	2	20060085337	A1	2006-04-20	Conforti et al.	Corresponds to WO 2005031541 A2
	3	20030105707	A1	2003-06-05	Audebert et al.	Corresponds to WO 03046778 A2
	4	20020161724	A1	2002-10-31	Peters	Corresponds to WO 02082392 A2

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13974462
	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	2876
	Examiner Name	Ahshik Kim
	Attorney Docket Number	W-9001D3

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	9914711	WO	A2	1999-03-25	Andrasev	Published in the English language	☐
	2	2823882	FR	A1	2002-10-25	Inventor not named	English abstract	☒
	3	2005031541	WO	A2	2005-04-07	Conforti et al.	Published in the English language and corresponds to US 20060085337 A1	☐
	4	1067492	EP	A3	2001-01-17	Palmquist	Published in the English language	☐
	5	2287793	EP	A1	2011-02-23	Kemper et al.	Published in the English language and corresponds to US 7427021 B2	☐
	6	03046778	WO	A2	2003-06-05	Audebert et al.	Published in the English language and corresponds to US20030105707 A1	☐
	7	0193213	WO	A2	2001-12-06	Mani et al.	Published in the English language	☐
	8	02082392	WO	A2	2002-10-17	Peters	Published in the English language and corresponds to US 20020161724 A1	☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

Petitioner Askeladden LLC
Exhibit 1002 - Page 146 of 350

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13974462
	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	2876
	Examiner Name	Ahshik Kim
	Attorney Docket Number	W-9001D3

	1	SAXENA ET AL., "MMPS: A Versatile Mobile-to-Mobile Payment System", Proceedings of the International Conference on Mobile Business (ICMB'05), 2005, IEEE, pages 1-6	☐
	2	2.1 Electronic Payment System, 23 pages	☐
	3	WOLFGANG WOPPERER, "Fraud Risks in E-commerce Transactions", The Geneva Papers on Risk and Insurance, Vol. 27 No. 3 (July 2002), pages 383-394	☐
	4	WRONA ET AL., "Mobile Payments - State of the Art and Open Problems", Ericsson Research, Germany, 13 pages	☐
	5	AMIR HERZBERG, "Payments and Banking with Mobile Personal Devices", Communications of the ACM, May 2003, Vol. 46, No. 5, pages 53-58	☐
	6	GORDON AGNEW, Chapter 10 Secure Electronic Transactions: Overview, Capabilities, and Current Status, pages 211-226	☐
	7	WANG ET AL., "Secure Wireless Payment Protocol", Proceedings of International Conference on Wireless Networks (ICWN), Las Vegas, Nevada, 2003 pages 1-7	☐
	8	CAROL L. CLARK, "Shopping without cash: The emergence of the e-purse", 4Q/2005, Economic Perspectives, pages 34-51	☐
	9	HALL ET AL., "WPP: A Secure Payment Protocol for Supporting Credit- And Debit-Card Transactions Over Wireless Networks, IEEE International Conference on Telecomuniations (ICT), Bucharest, June 2001, pages 1-6	☐
	10	MARK E. PETERS, "Emerging eCommerce Credit and Debit Card Protocols", Proceedings of the 3rd International Symposium on Electronic Commerce (ISEC'02), 2002, IEEE Computer Society, 8 pages	☐
	11	KARNOUSKOS ET AL., "Mobile Payment: A Journey Through Existing Procedures and Standardization Initiatives" IEEE Communications Surveys, Fouth Quarter 2004, Volume 6, No. 4, pages 44-66	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13974462
	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	2876
	Examiner Name	Ahshik Kim
	Attorney Docket Number	W-9001D3

	12	VORAPRANEE KHU-SMITH, "Enhancing the security of electronic commerce transactions", Technical Report RHUL-MA-2003-7, June 2003, Royal Holloway Univesity of London, Department of Mathematics, England, 183 pages	☐
	13	CAI ET AL., "Authorization Mechanisms for Mobile Commerce Implementations in Enhanced Prepaid Solutions", Bell Labs Technical Journal 8(4), 2004, pages 121-131	☐
	14	XINGJIANG SONG, "Mobile Payment and Security", Article in T-110.501 Seminar on Network Security 2001 ISBN 951-22-5807-2, Publications in Telecommunications Software and Multimedia TML-C7 ISSN 1455-9749, Helsinky University of Technology, Telecommunications Software and Multimedia Laboratory, 15 pages	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13974462
	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	2876
	Examiner Name	Ahshik Kim
	Attorney Docket Number	W-9001D3

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Werner H. Stemer/	Date (YYYY-MM-DD)	2014-01-14
Name/Print	Werner H. Stemer	Registration Number	34956

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Petitioner Askeladden LLC
Exhibit 1002 - Page 150 of 350

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/10, 19/00	A2	(11) International Publication Number: **WO 99/14711** (43) International Publication Date: 25 March 1999 (25.03.99)

(21) International Application Number: PCT/HU98/00087

(22) International Filing Date: 17 September 1998 (17.09.98)

(30) Priority Data:

P 97 01553	17 September 1997 (17.09.97)	HU
P 97 02485	17 December 1997 (17.12.97)	HU
P 98 02109	17 September 1998 (17.09.98)	HU

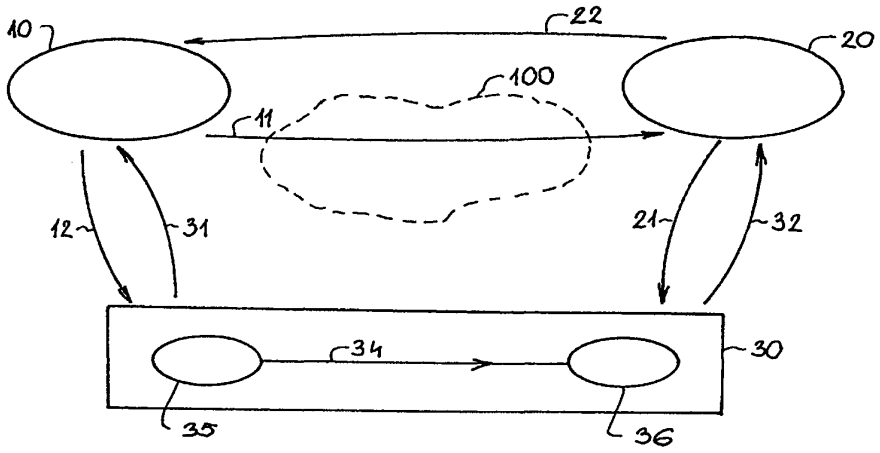
(71)(72) Applicant and Inventor: ANDRASEV, Ákos [HU/HU]; Ulászló u. 45, H–1113 Budapest (HU).

(74) Agent: DANUBIA; Bajcsy–Zsilinszky út 16, H–1051 Budapest (HU).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, 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), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD FOR CHECKING RIGHTFUL USE OF A DEBIT CARD OR SIMILAR MEANS GIVING RIGHT OF DISPOSING OF A BANK ACCOUNT



(57) Abstract

The procedure according to the invention can be used both for granting authority verbally or electronically for the usage of a bank card, or for performing the investigation of the authority of a money order, prior to its execution. The essence of the procedure is that, prior to each intended transaction, in addition to the otherwise well known authorizing signal with a meaning of permitting the use of the card or to issue a money order, the authorizing signal will be overwritten by an authorization override signal, deducted from a return message signal obtained previously from the decision maker through a telecommunication network, preferably through a digital mobile telecommunication network, in the form of an SMS message signal, as a reply to an authorization override request message, and the transaction is authorized by means of the authorizing signal validated by and having the meaning of the override authorization signal.

Petitioner Askeladden LLC
Exhibit 1002 - Page 151 of 350

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		

Petitioner Askeladden LLC
Exhibit 1002 - Page 152 of 350

METHOD FOR CHECKING RIGHTFUL USE OF A DEBIT CARD OR SIMILAR MEANS GIVING RIGHT OF DISPOSING OF A BANK ACCOUNT

Technical field

The present invention relates to a procedure to ensure the authority of using a bank card or other means providing right of disposal of a bank account, said procedure being applicable both in verbal or electronic way of authorization to use a bank card, and during the investigation of a commission to perform a cash disbursement or money remittance prior to its execution, being suitable also for preventing damages resulting from unauthorized use of bank cards or other means. In the course of performing the procedure according to the present invention, granting the authority to use a bank card or other means is carried out in order to execute a transaction which results in changing the balance of a given bank account, and during the execution of the procedure of the present invention the authority to use the card or other means is granted.

Background art

In the present description below the term "bank card" or "card" is meant to include the terms "deposit card", "credit card", "mixed card" and "virtual bank card", and further the definition "means providing right of disposal of a bank account" refers to the possibility available for a person of disposing of a given bank account by means of a verbal or written order or by way of using some other specified means such as, e.g. a written money order or other commissions transmittable in written form; verbal instructions given by word of mouth or transmitted through a telecommunication network; instruction signals generated in a computer; e-mail messages; SMS messages; a remote input terminal, etc.

Petitioner Askeladden LLC
Exhibit 1002 - Page 153 of 350

It is known that when using a bank card to perform a transaction e.g. to withdraw cash, to buy something, availing oneself of a service or executing a purchase in a commercial unit, or in case of a purchase by using the card number or the bank account number only in a virtual warehouse, operated through the INTERNET or other networks, the unit accepting the card, usually a commercial unit or post office, an automatic teller machine (ATM) or a warehouse, etc., in order to get authorization to execute the transaction, contacts the principal bank or banking institution keeping the backing account of the card through reading the bank card electronically by means of its POS terminal or by other means, provided if said commercial unit has full or semi-on-line connection directly or through its own principal bank with the principal banking institution keeping the backing account of the card.

The bank, in its procedure aimed at granting the authorization, checks the existence and validity of the card and seeks whether sufficient funds are available on the backing account to cover the requested transaction. The authorization procedure is carried out in such a way that the data signal, generated by composing the details of the transaction to be carried out with the characteristic data of the card and that of the backing account, is evaluated by means of comparing said data signal with the respective set of data stored in the appropriate data file of its own computer and, depending on the results of the evaluation, a signal permitting or prohibiting the requested transaction is generated, which signal is then returned to the site of usage.

If the result of the above authorization procedure is positive, then the commercial unit, besides checking the right of disposing of the card e.g. by identifying the person using the card, by his identification card or by signature comparison, or by verifying the rightful use of the of card in some other way as well, e.g. by asking for entering the PIN code, draws up the

charge certificate, in case of a purchase makes out the bill and, in such cases, the user of the card is usually asked to sign the bill and, depending on the characteristics of the available connection, either immediately or at a later time, in an accumulated form, withdraws the corresponding equivalent sum from the specified account of the card holder.

Practically, a similar procedure is followed also in places having no POS terminal. In such cases, permission for granting the use of the card at the unit, e.g. a commercial unit, a post office, etc., is obtained from the bank verbally through a telephone link, and in the possession of such a permission the charge certificate is drawn up, and the bearer is asked to sign it. The account of the card holder is charged on the basis of this signed charge certificate.

Concern arises, however, when somebody tries to use a card illegally, e.g. trying to pay with a stolen or found card, but the card itself is not forged, and the required sum is available on the bank account serving as backing of the card, either in the form of deposit or amount of credit granted, and the unauthorized user is capable of making pretense of authorized usage of the bank card, e.g. by imitating the signature, or by having unwarrantedly got to know the PIN code. It may also cause concern when the identification number of somebody's card or bank account becomes known to an unwarranted person, e.g. by having read off the number either directly or in other way, e.g. from the INTERNET web and, with that knowledge, he buys to the debit of the bank account of the card holder or holder of the bank account, under an arrangement requiring no other identification to receive the purchased goods, or the unwarranted user has managed to become acquainted with the required second set of identification data, name, address, etc.

Similarly, remittances initiated illegally from a terminal located at the customer and linked up with the computer of the bank, permitting direct

remittances requiring no further personal intervention, such as e.g. remittances requested outside the office hours of the bank because the working hours of the beneficiary lie in another time zone, as well as remittances initiated in the possession of the illegally acquired identification data through telephone will become known to the holder of the account only when the charges have already appeared on his bank account, i.e. when the holder has already suffered the loss.

In such cases, according to the present state of the art, unauthorized use of the card or unlawful charging of a bank account cannot be prevented in a satisfactory way, which imposes a loss on the bank as owner of the card and/or on the holder of the card and on the holder of the bank account, respectively.

It is also true that the holder of a card, in the case of loosing, theft or unauthorized use of his card, or after becoming aware of unauthorized charging of his bank account is entitled to stop the validity of the card, i.e. to freeze his account or other arrangement serving as coverage of his card at the issuing bank, or to stop payments from his bank account in the case of an unauthorized remittance, or to issue a coverage verification or garnishment of payments, but this is usually done only after the card holder has become aware of the appearance of cost of purchases made to the debit of his account but not performed by him or with his consent, or when the holder of the bank account has noticed the remittances charged on the account or, very often, only after having received notice on the exhaustion of his account, and this way only after the owner suffered the loss.

The main periods of using the bank card as cash substituting means usually fall outside the working hours of the bank, and in some cases the card usage takes place in another time-zone and, generally, the sum spent is not too much, the purchased goods serving the requirements of a single person or a family. Considering the present state of the art and the usual

volume of such purchases, obtaining previous approvals of the holder of the account to eliminate unauthorized use of the bank card would render such shopping too cumbersome, causing unnecessary delays and, due to the possible inaccessibility of the holder of the account, a high proportion of purchases would fail and the operating costs and the closing times would considerably increase. It is an established practice of banks for preventing undesirable uncovered shopping to which, sooner or later, an unauthorized use of the card would lead, to limit the number of such purchases to one card/day, and to restrict the maximum sum/day that can be withdrawn from a card-backing account, yet this practice offers advantages for the banks only and does not protect the account holder against unauthorized usage of, or remittance through, a bank card.

The damage imposed on card owners and/or card holders, as well as on the bank account holders, as well the annoyance of holders of bank accounts, affecting many things, has rendered necessary to find an arrangement offering the possibility of introducing a procedure more efficient than those known so far to ensure the authorization to use of a bank card or other means providing right of disposing of a bank account for performing transactions effecting a change in the balance of a bank account, particularly such as shopping through the INTERNET, withdrawing cash, paying with a bank card, performing remittances from a bank account etc., in order to prevent unauthorized payments and unauthorized remittances, thereby successfully averting the occurrence of damages.

Disclosure of the invention

The present invention is based on the recognition that any unauthorized use of bank cards and illegal remittances can effectively be prevented only if, in the case of natural persons, the card owner or bank account holder and, in the case of legal entities, the person named as

decision maker is drawn into the approval of each transaction. Another recognition is the fact that, at the present state of art of the communication means, involving the owner of the card or the account holder can be done without causing any concern or hindrance to the cash flow. Further connected to this is the recognition that the extra authorization should be carried out in such a way, that excludes the possibility of performing it by an unwarranted person. Further, there is the recognition too, that by cutting the authorization procedure into two levels, besides it makes the unwarranted use of a card even more difficult, it also makes the authorization itself faster.

Thus, in the procedure proposed by the present invention to ensure the authority of using a bank card or some other means providing right of disposal of a bank account to perform a transaction resulting in a change of balance of the bank account and checking the authority of an involvement into the authorization procedure, the usage will be authorized and, depending on the result of this authorization procedure, the use of the card or other means will either be permitted or prohibited. The essence of the procedure is that an authorization override request signal, preferably an authorization override request signal carrying certain information about the transaction and/or the bank account to be charged by the transaction and/or the expected change in the balance of the bank account involved, is generated, the authorization override request signal is converted into a message signal that can be sent through a telecommunication network, preferably through a digital mobile telecommunication network, preferably in SMS mode of operation, and this message signal is transmitted through the telecommunication network, preferably in SMS mode of operation, to a telecommunication device, preferably a mobile telephone set, which is capable of sending a return signal, and having a call number given by the person having the right of disposal of the bank account to be charged by

the transaction, then from the return signal received through the telecommunication network, preferably in SMS or DTFM mode of operation, or from the return signal received in the form of a tone, or in case such a return signal is not received within a predetermined period of time, a return signal, that can be evaluated by the computer, is deducted, an authorization overriding signal with a meaning of either permission or prohibition, corresponding to the information content of the received signal is generated, by means of which authorization overriding signal the usage is either permitted or prohibited.

During the execution of the procedure according to the present invention, within the framework of the authorization the data signal, generated with the characteristics of the intended transaction and with the characteristics of the bank card or other means and/or with the characteristics of the bank account to be charged, is evaluated by way of comparison, in the known way, with the set of data stored in the computer in the respective data file and, depending on the result of this evaluation, a signal with the meaning of either permission or prohibition is generated. This signal is then transmitted to the site of usage.

In a second preferred embodiment of the present invention the authorization override request signal is generated prior to the authorization.

In a third preferred embodiment of the present invention the authorization override request signal is generated after the authorization.

In a fourth preferred embodiment of the present invention the authorization override request signal is generated simultaneously with the authorization.

In the second embodiment of the solution according to the present invention, besides that during the procedure to ensure the authority of using a bank card or some other means providing right of disposal of a bank account to perform a transaction resulting in a change of balance of a bank

account and checking the authority of an involvement into the authorization procedure, the usage will be authorized and, depending on the result of this authorization procedure, the use of the card or other means will either be permitted or prohibited, the procedure is carried out in such a way that an authorization override message signal, preferable an authorization override message signal carrying certain information about the transaction and/or the bank account to be charged by the transaction and/or the expected change in the balance of the bank account involved, is generated, the authorization override message signal is transferred to the bank keeping the account through a telecommunication network, preferably in SMS mode of operation or in DTFM mode of operation or in tonal form, there an authorization override signal that can be evaluated by a computer is deducted from the authorization override message signal, by means of which authorization overriding signal the usage is either permitted or prohibited.

In the third embodiment of the solution according to the present invention, where during the procedure for ensuring the authorization of using a ban card or some other means providing right of disposal of a bank account to perform a transaction resulting in a change of balance of a bank account and ensuring the authority of an involvement into the authorization procedure, the usage will be authorized and, within the framework of the authorization procedure a data signal generated with the characteristics of the intended transaction and with the characteristics of the bank card and/or the bank account to be charged is evaluated by way of comparison in the known way with the set of data stored in the computer in the respective data file and, depending on the result of this evaluation, a signal with the meaning of either permission or prohibition is generated, which signal is used then as a proof of authority, which signal will, in certain cases, be transmitted to the site of usage, the procedure is carried out in

such a way, that an authorization override request signal carrying certain characteristic data of the transaction and, in certain cases, that of the bank card and/or the bank account to be charged by the transaction, is generated, the authorization override request signal is converted into a message signal that can be transmitted through a digital mobile telecommunication network in SMS mode of operation, the message signal is transmitted through the telecommunication network to, and written into the message storing memory of the mobile telephone set, the call number of which is given by the person having the right of disposal of the bank account to be charged by the transaction, at the same time the message is displayed on the display unit of the mobile phone, then the return signal received through the telecommunication network, preferably in SMS mode of operation, or the lack of such a return signal within a predetermined period of time, is converted into a return signal that can be evaluated by a computer, this return signal is then evaluated by the computer, and an authorization overriding signal, with a meaning of either permission or prohibition corresponding to the information contents of the received signal, is generated, by means of which authorization overriding signal the permissive authorization signal will be overwritten.

Brief description of the drawings

Figure 1 is a flowchart of a first embodiment of the first version of the procedure according to the present invention, where the bank requesting the authorization and the principal bank of the account holder is the same;

Figure 2 is a flowchart of a second embodiment of the first version of the procedure according to the present invention where the account holder is registered in the bank requesting the authorization, but his account is kept by another bank;

Figure 3 is a flowchart of the second version of the procedure according to the present invention, where the principal bank of the authorization requester and the principal bank of the account holder are different, and the account holder gives his authorization override to his principal bank in advance;

Figure 4 is a flowchart of a such an embodiment of the first version of the procedure according to the present invention, where the principal bank keeping the account of the authorization requester and the principal bank of the account holder are different, and the account holder is in contact only with his principal bank;

Figure 5 is a flowchart of such an embodiment of the first version of the procedure according to the present invention where, the authorization override through the authorization network precedes the authorization; and

Figure 6 is a flowchart of such an embodiment of the first version of the procedure according to the present invention, where an authorization override procedure through a network, e.g. through the INTERNET network, precedes the authorization.

Best mode of carrying out the invention

Figure 1 is a flowchart of an embodiment, given as an example, of the first version of the procedure according to the present invention to ensure authorization, where there are three participants in the procedure, the first one of them being the person who has the right of disposing of a bank account, which is to be charged by a given transaction, and the payment is to be done by using a bank card, virtual bank card or other means, for sake of simplicity hereinafter called bank card, this person hereinafter is called an account holder 10; the second participant is a person or organization, e.g. a warehouse, a POS terminal, etc., which sells goods or provides services or other values, e.g. dispenses money, and at

which participant payment is possible by using a bank card, and which participant would like to obtain the payment through a remittance to his bank account, for sake of simplicity this participant hereinafter is called a requester of authorization 20; and finally the third participant is a bank 30 which keeps, on the one hand, a certain account 36 of the requester of authorization and, on the other hand, a covering account 35 of the bank card of the account holder 10, where, among others, the data required for establishing a quick connection to the account holder 10 through a telecommunication network are also stored. In the course of purchasing, account holder 10, preferably by establishing a computer linkage, either personally or through a telephone or computer network, e.g. through the INTERNET network 100, submits his order and, at the same time, his bank card or his initiative 11 including the identification data of his bank card together with other data referring to the mode of payment to the requester of authorization 20, who requests an authorization permitting the use of the bank card by issuing, through his appropriate terminal, a request of authorization signal 21 to the bank 30. Out of the appropriate data of the authorization requesting signal 21, an authorization override request signal is produced by the bank 30 using electronic data processing, and from this authorization override request signal a message signal 31 is deducted, again by using electronic data processing, which message signal 31 is transmitted, preferably in SMS format, through an appropriate terminal and usually through the center of a mobile telephone network, to the mobile telephone set of account holder 10. Depending on the information content of message signal 31, received by his mobile telephone set, either a permitting or a prohibiting return message signal 12 is produced by the account holder 10, which will then be returned to the bank 30 through the telecommunication network, preferably in SMS or DTFM mode of operation or in the form of a tone signal. From this return message signal 12 or from

Petitioner Askeladden LLC
Exhibit 1002 - Page 163 of 350

the lack of it within a predetermined period of time, a return signal understandable by a computer is produced at the bank 30, and an authorization override signal with a meaning of either permission or prohibition is generated, depending on the information content of the return signal. Besides this, bank 30 checks whether enough funds are available on a backing account 35 of the account holder 10 to cover the particular transaction, and accordingly, produces an authorizing signal with the appropriate meaning. In case of an authorization override signal with an affirmative meaning for the authorization requester 20, the bank 30 authorizes the use of the card by sending an authorizing signal 32 generated from the corresponding authorization signal with the appropriate meaning, then, at the occurrence of the use of the card, it also charges the backing account 35 of the account holder 10 with the consideration sum, which, together with a remittance 34, it also will credit to an account 36 of the authorization requester 20. The acceptance of the order will be signaled back to the account holder 10 by the authorization requester 20 by sending an acknowledgement 22 with the appropriate meaning.

In the case, when a return message signal 12 with a meaning of prohibition has been received by the bank 30, it issues an authorizing signal 32 with a meaning of prohibiting the use of the card to the authorization requester 20.

Figure 2 is a flowchart of a second embodiment, given as an example, of the first version of the procedure according to the present invention to ensure authority where, besides account holder 110 and an authorization requester 120, shown in connection with Fig. 1 and having the functions described there, there are further participants, i.e. a bank 130 keeping an account 136 of the authorization requester 120, a bank 150 keeping an account 156 of the account holder 110, and an authorization network 140 connecting the two banks. Account holder 110 is registered at

the bank 130, and, among his registered data 135, the appropriate data required for establishing a quick connection with the account holder 110 through a telecommunication network are also stored. In the course of a purchase, similarly to the procedure described in connection with Fig. 1, account holder 110, preferably by establishing a computer connection, either personally or through a telephone or computer network, e.g. through the INTERNET network 100, submits his order and, at the same time, his bank card or his initiative 11 including the identification data of his bank card together with other data referring to the mode of payment to the requester of authorization 120, who requests an authorization permitting the use of the bank card by issuing, through his appropriate terminal, a request of authorization signal 121 to the bank 130. Out of the appropriate data of the authorization requesting signal 121, an authorization override request signal is produced by the bank 130 using electronic data processing, and from this signal a message signal 131, transmittable through a telecommunication network, is deducted, again by using electronic data processing, which message signal 131 is transmitted, preferably in SMS format, through an appropriate terminal and usually through the center of a mobile telephone network to the mobile telephone set of account holder 110. Using the data, recorded in the register 135 of the bank 130, message signal 31 is transmitted, preferably in SMS format, usually through the center of a mobile telephone network to the mobile telephone set of account holder 110. Depending on the information contents of message signal 131 received by his mobile telephone set, either a permitting or a prohibiting return message signal 112 is produced by the account holder 110, which will then be returned to the bank 130 in the way described in connection with Fig. 1. At the same time, in order to authorize the given usage of the bank card, a signal 132 and an authorizing signal 141 deducted from signal 132 is sent through the authorization network 140 by

the bank 130 to the principal bank 150 of account holder 110 keeping his card backing account 156, to which a return signal 151 with a meaning of permission or prohibition and an authorization signal 142 deducted from signal 151 will be received, also through the authorization network 140. From the return message signal 112, received through the telecommunication network or from the lack of this return message signal 112 within a predetermined period of time, a return signal understandable by a computer is produced, and an authorization override signal with a meaning of either permission or prohibition is generated, depending on the information content of the return signal. With the exception of a return message signal 112 of prohibition, the use of the card is permitted by sending an authorizing signal 133 with a meaning which corresponds to the meaning of the authorizing signal 142 to the authorization requester 120.

The acceptance of the order will be signaled back to the account holder 110 by the authorization requester 120, by sending an acknowledgement 122 with the appropriate meaning.

At the occurrence of the card usage, its backing account 156 of account holder 110 kept at the bank 150 will be charged with the consideration sum, which will also be credited to the account 136 of the authorization requester 120 at the bank 130.

If a return message signal 112 with a meaning of prohibition has been received by the bank 130, then it issues an authorizing signal 133 with a meaning of prohibiting the use of the card to the authorization requester 120.

Figure 3. is a flowchart of an embodiment, given as an example, of the second version of the procedure according to the present invention to ensure authority where, besides account holder 210 and an authorization requester 220 shown in connection with Fig. 1 and having the functions described there, there are further participants, i.e. a bank 230 keeping an

account of authorization requester 220, a bank 250 keeping an account of account holder 210, and an authorization network 140 connecting the two banks. At the bank 250 data are also stored that are necessary for establishing quick connection with account holder 210. In the course of a purchase, similarly to the procedure described in connection with Fig. 1, account holder 210, preferably by establishing a computer connection, either personally or through a telephone or computer network, e.g. through the INTERNET network 100, submits his order and, at the same time, his bank card or his initiative 211 including the identification data of his bank card together with other data, referring to the mode of payment, to the requester of authorization 220, who requests an authorization permitting the use of the bank card by issuing, through his appropriate terminal, a request of authorization signal 221 to the bank 230. At the same time, account holder 210 sends an authorization override message signal 212 to his own principal bank 250 with an information content that enables the intended simultaneous purchase with the card, limiting its location and sum. Bank 230 sends a signal 231 and an authorizing signal 241 deducted from signal 231 through the authorizing network 240 to the account holder's 210 principal bank 250 keeping his card backing account, in order to authorize the use of the card, to which a return signal 251, overridden by the authorization override message signal 212, and a usage authorization signal 231, deducted from signal 251, will be received, also through the authorization network 240, at the bank 230 which also sends an authorization signal 232 with a corresponding meaning to authorization requester 220.

The acceptance of the order will be signaled back to the account holder 210 by the authorization requester 220, by sending an acknowledgement 222 with the appropriate meaning.

Petitioner Askeladden LLC
Exhibit 1002 - Page 167 of 350

At the occurrence of the card usage, payment of the consideration sum will be carried out in the known way, by charging the backing account of account holder 210 kept at his principal bank 250.

Figure 4 is a flowchart of a third embodiment, given as an example, of the first version of the procedure according to the present invention to ensure authority, where connections exist among account holder 310, authorization requester 320, the principal bank 330 keeping the account of authorization requester 320, the principal bank 350 keeping the card backing account of account holder 310 and the authorization network 340 connecting the two banks, already shown in connection with Fig. 3 and each participant has the functions described there, with the addition that the data, required for establishing a quick connection with account holder 310 through a telecommunication network, are also stored in bank 350.

The purchase, the authorization of the card usage, the payment of the consideration sum and the acknowledgement of the purchase are carried out in a way described in connection with Fig. 3. The difference is in the authorization overriding of the card usage which, in case of this example, is initiated by the bank 350 at receiving the authorization request 341, and it is carried out in the way explained above in connection with Fig. 1 or Fig. 2, preferably by transmitting in SMS mode of operation through a digital mobile telecommunication network, and the authorization checking is carried out at the time chosen accordingly, and the card usage authorizing signal 352, already overwritten with authorization override signal 312, is transmitted to bank 330 through the authorization network, and the corresponding authorizing signal 332 is transmitted to the authorization requester 320.

The flowchart shown in Fig. 5 illustrates such an embodiment of the procedure according to the present invention to ensure authority where connections exist among account holder 410, authorization requester 420,

the principal bank 430 keeping the account of authorization requester 420, the principal bank 450 keeping the card backing account of account holder 410 and the authorization network 440 connecting the two banks, already shown in connection with Fig. 3 and 4 and each participant has the functions described there. Data, required for establishing a quick connection with account holder 410 through a telecommunication network, are also stored in bank 450.

In the course of the purchase, account holder 410 submits his order and, simultaneously, his card or his initiative 411 including the identification data of his card, together with other data referring to the mode of payment, by establishing a computer connection or in any other way described in more detail above, to the requester of authorization 420, which is usually a virtual warehouse or a certain kind of business partner. Based on the card identification data provided by account holder 410, authorization requester 420 sends an authorization override procedure initiating signal 421 to his own bank 430 through his own banking connection. Using the information contents of the authorization override procedure initiating signal 421, received through the authorization network 440, or that of signal 431 or signal 441 deducted from signal 421, bank 430 generates a message signal 451 and transmits this signal, e.g. by means of a mobile telephone network and preferably in SMS format, to the mobile telephone set of account holder 410. Through his mobile telephone set, account holder 410 sends a return signal 412 to the bank 450 which, by processing and returning it to bank 430, in the form of signal 452 or 442, sends an authorization procedure initiating signal 432 to the authorization requester 420. In case of a signal 432 with a meaning of enabling the initiation of the authorization procedure, authorization requester 420 sends an authorization requesting signal 422 to his principal bank 430. In order to issue the authorization, by using the procedure described above in more detail,

principal bank 430 turns to principal bank 450 of account holder 410 with an authorization requesting message 423 or 443, through the clearing network 440. In possession of and in accordance with the meaning of the return message signal 412, received from account holder 410, bank 450 transmits usage authorizing signals 453 and 444 and, through the clearing network 440 and bank 430, an authorizing signal 434, too, with a meaning of corresponding to signal 412, to authorization requester 420.

The flowchart shown in Fig. 6 illustrates such an embodiment of the procedure according to the present invention to ensure authority where connections exist among account holder 510, authorization requester 520, the principal bank 530 keeping the account of authorization requester 520, the principal bank 550 keeping the card backing account of account holder 510 and the authorization network 540 ensuring the clearing connection between the two banks, already shown in connection with Fig. 3 and 4 and each participant has the functions described there. Data required for establishing a quick connection with account holder 510 through a telecommunication network are also stored in bank 550.

In the course of the purchase, account holder 510 submits his order and, simultaneously, his card or his initiative 511 including the identification data of his card together with other data referring to the mode of payment, by establishing a computer connection through the INTERNET 100 or any other network with similar functions, to the requester of authorization 520 which is usually a virtual warehouse or a certain kind of business partner. Based on the card identification data provided by account holder 510, authorization requester 520 sends an authorization override procedure initiating signal 521 to the principal bank 550 of account holder 510 through the INTERNET network 100. Using the information contents of the authorization override procedure initiating signal 521, bank 550 generates a message signal 551 and transmits this signal, e.g. by means of a mobile

Petitioner Askeladden LLC
Exhibit 1002 - Page 170 of 350

telephone network and preferably in SMS format, to the mobile telephone set of account holder 510. Through his mobile telephone set, account holder 510 sends a return signal 512 to bank 550 which, by processing it, sends an authorization procedure initiating signal 552 by means of a computer link through the INTERNET network 100. In case of a signal 552 with a meaning of enabling the initiation of the authorizing procedure, authorization requester 520 sends an authorization requesting signal 522 to the principal bank 530. In order to issue the authorization, by using the procedure described above in more detail, principal bank 530 turns to the principal bank 550 of account holder 510 with an authorization requesting message 531 or 541, through the clearing network 540. In possession of and in accordance with the meaning of the return message signal 512 received from account holder 510 bank 550 transmits usage authorizing signals 553 and 542 and, through the clearing network 540 and bank 530, the authorizing signal 532, with a meaning of corresponding to signal 512, to authorization requester 520.

Acknowledging the order is done by means of acknowledgement 523 and, at the occurrence of the card usage, balancing off the consideration will be done, in a way known by itself, through the clearing network.

By making the use of a bank card or the execution of a money order dependent on not only an authorization but on an override authorization, too, the procedure according to the invention provides a possibility to completely exclude an unauthorized use. The card holder or the user of the device or the person having the right of disposal of the bank account always carries his telecommunication device, which can be a pager, a pager made suitable to reply, a telephone set in a coupled network or a mobile telephone set, or a telecommunication device developed specifically for this purpose, with him and operates it, and therefore, in case

of proper use, there is a very slight chance of loosing or being stolen of his bank card or his other means providing a right of disposal of his bank account and his mobile telephone set at the same time. Furthermore, even such a person cannot use a bank card or other means, e.g. the identification number of a bank card, in itself, who happens also to be in the possession of the mobile telephone set, or who gets to possess the telephone set only, because even if such a person detects the incoming authorization override request signal, he does not know the proper way of reply or possibilities of giving the authorization instructions, and therefore, lacking the override authorization, even if the requester can provide all the necessary data or all data are available for him, the use of the card or other means or the execution of the remittance will be denied of him. A further advantage of the procedure is that the authorization overriding can be used efficiently not only in case of authorization requests or remittance orders received from POS terminals, but also in cases of authorization requests arriving, e.g. through a telecommunication network, from fax machines or from the remote terminal of a computer, too. The procedure according to the present invention increases the length of time of the authorization process slightly only, and its extra costs are negligible compared to the increase of its security.

CLAIMS

1. Procedure for ensuring the authorization of using a bank card or some other means providing right of disposal of a bank account, said usage being aimed at performing a transaction resulting in a change of balance of a bank account, in the course of which the usage is subject to an authorization, and depending on the result of such an authorization the use of the bank card or other means is either granted or rejected, **characterized in** that an authorization override request signal, preferably an authorization override request signal carrying information about the transaction and/or the bank account to be charged and/or the expected change in the balance of said bank account, the authorization override request signal is converted into a message signal (31, 131, 351, 451, 551) transmittable through a telecommunication network, preferably through a digital mobile telecommunication network, preferably in SMS mode of operation, the a message signal (31, 131, 351, 451, 551) is transmitted to a telecommunication device, preferably a mobile telephone set, with a call number specified by the person having the right of disposal over the bank account to be charged and suitable to send a return message signal, the transmission is carried out preferably in SMS mode of operation, then from the return message signal (12, 112, 312, 412, 512) received through the telecommunication network, preferably in SMS mode of operation or DTFM mode of operation or in the form of a tone or from the lack of such a return message signal within a predetermined period of time, a return signal that can be evaluated by a computer is deducted, an override authorization signal with a meaning of either permission or rejection according to the information content of the return signal is generated, which override authorization signal is then used to either permit or reject the authorization of the usage.

2. Procedure according to claim 1 characterized in that the authorization override request signal is generated prior to the authorization.

3. Procedure according to claim 1 characterized in that the authorization override request signal is generated after the authorization.

4. Procedure according to claim 1 characterized in that the authorization override request signal is generated simultaneously with the authorization.

5. Procedure for ensuring the authorization of using a bank card or some other means providing right of disposal of a bank account, said usage being aimed at performing a transaction resulting in a change of balance of a bank account, in the course of which the usage is subject to an authorization and, depending on the result of such an authorization, the use of the bank card or other means is either granted or rejected, characterized in that an authorization override request signal, preferably an authorization override message signal (212) carrying information about the transaction and/or the bank account to be charged and/or the expected change in the balance of said bank account, the authorization override message signal (212) is transmitted through a telecommunication network, preferably through a digital mobile telecommunication network, preferably in SMS mode of operation or in DFTM mode of operation or in the form of a tone, to the principal bank keeping the account, then an authorization override signal, that can be evaluated by a computer, is deducted from the received authorization override message signal at the bank, which authorization override signal is used to enable the usage authorization.

6. Procedure for ensuring the authorization of using a bank card or some other means providing right of disposal of a bank account, said usage being aimed at performing a transaction resulting in a change of

balance of a bank account, in the course of which the usage is subject to an authorization, where in the course of the authorization a data signal generated with the characteristics of the intended transaction and that of the bank card and the bank account to be charged is evaluated by means of comparison with the corresponding data set of a data file stored in a computer and, depending on the result of such a comparison, an authorizing signal (32, 133, 332, 434, 532) with a meaning of either granting or rejecting the usage or the transaction is generated, which signal will be used as a signal checking the authority and, in certain cases it is transferred to the site of usage, **characterized in** that an authorization override request signal, containing the characteristic data of the transaction and, in certain cases, the identification data of the bank card and/or the bank account to be charged, is generated, the authorization override request signal is converted into a message signal (31, 131, 351, 451, 551) transmittable through a digital mobile telecommunication network in SMS mode of operation, the message signal (31, 131, 351, 451, 551) is transmitted through a digital mobile telecommunication network to the message storing memory of a mobile telephone set the call number of which has been specified by the person having the right of disposal of the bank account to be charged and, at the same time, the arrival of the message is displayed on the display unit of the same telephone set, then the return message signal (12, 112, 312, 412, 512) received through the telecommunication network, preferably a return message signal received in SMS mode of operation, or the lack of such a return message signal is converted into a return signal that can be evaluated by a computer, the return signal is evaluated by a computer, and an overriding authorization signal with an information contents corresponding to the evaluation is generated, which overriding authorization signal will be used to overwrite

the authorizing signal (32, 133, 332, 434, 532) having a meaning of permission.

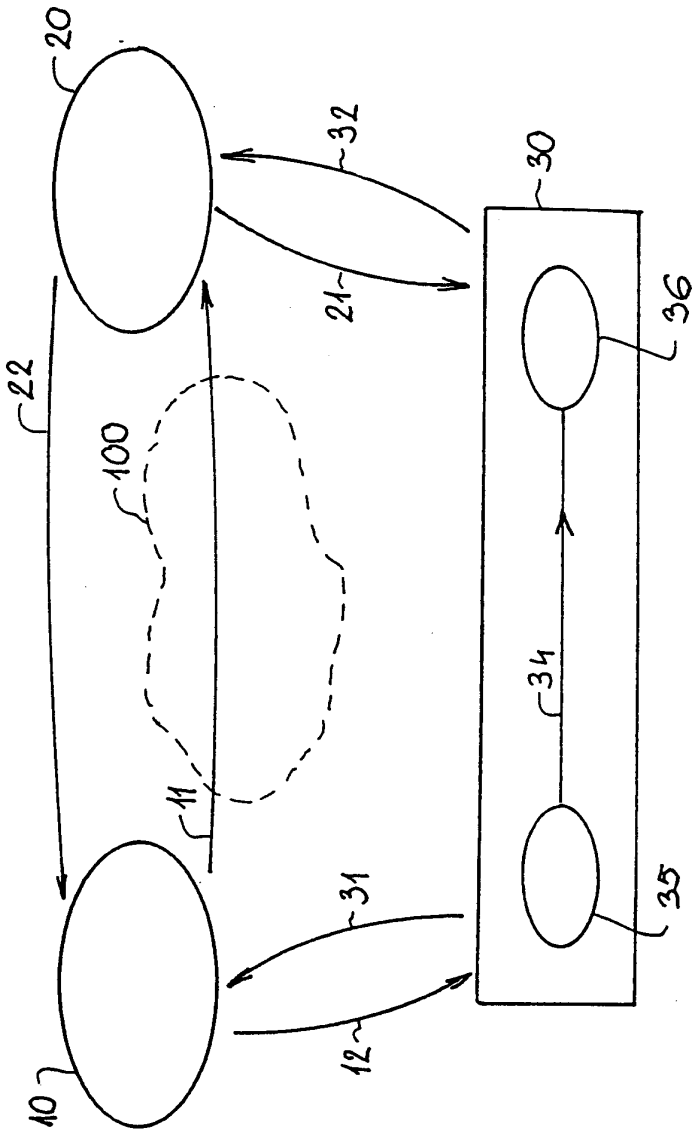


FIG. 1.

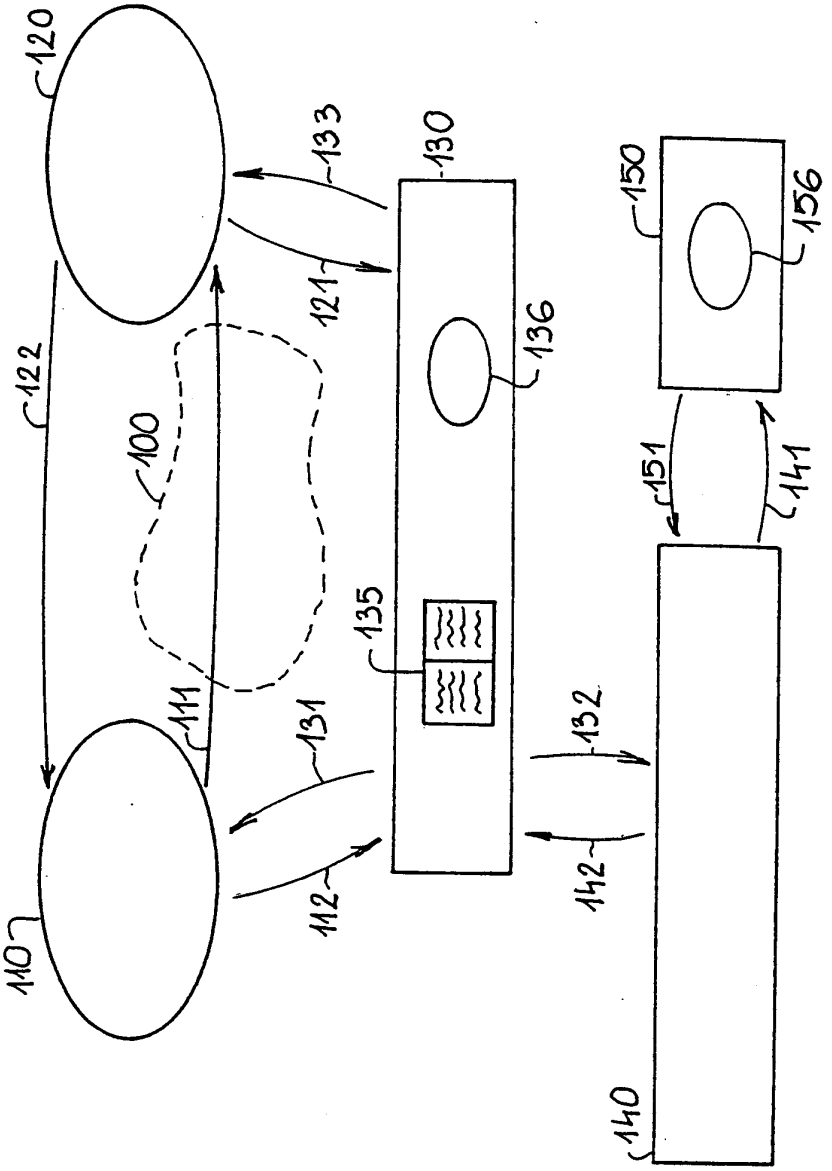


FIG 2.

Petitioner Askeladden LLC
Exhibit 1002 - Page 178 of 350

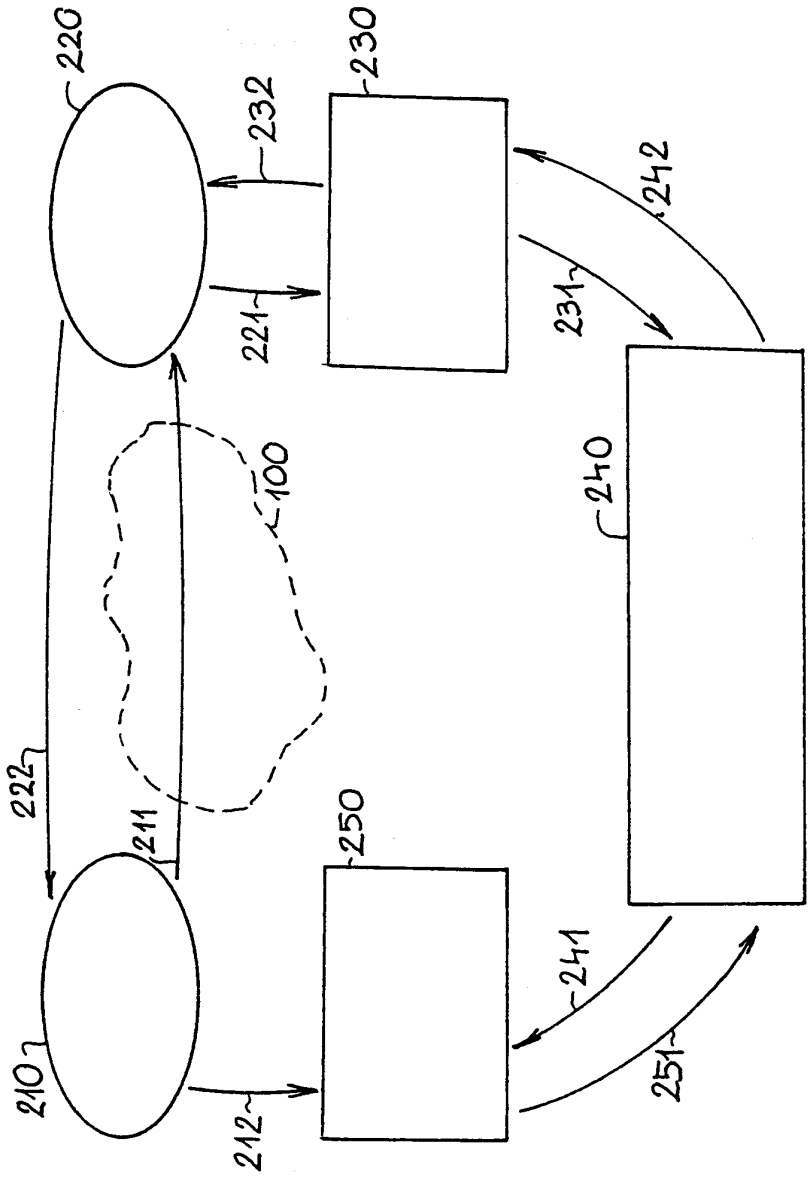


FIG 3.

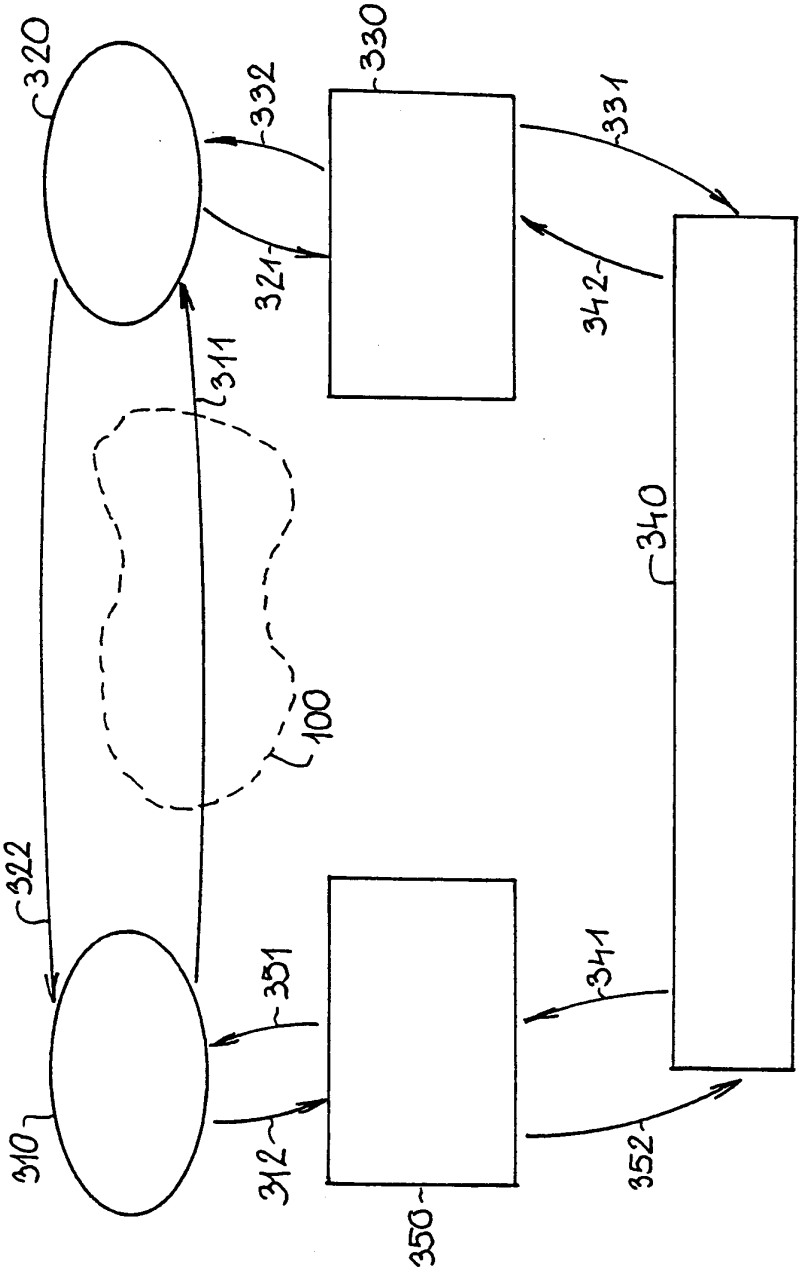


FIG 4.

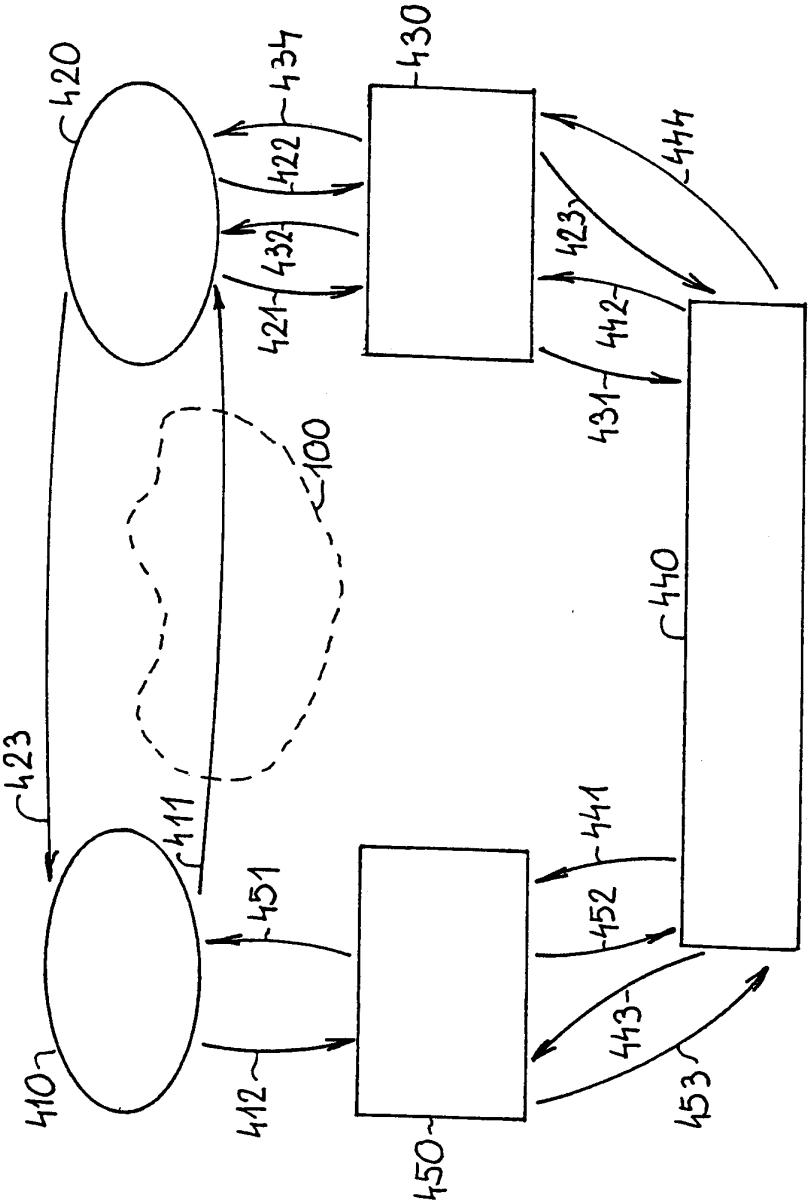

420
434
430
422
444
423
432
421
412
431
100
440
423
411
441
451
452
410
412
443
453
450

FIG 5.

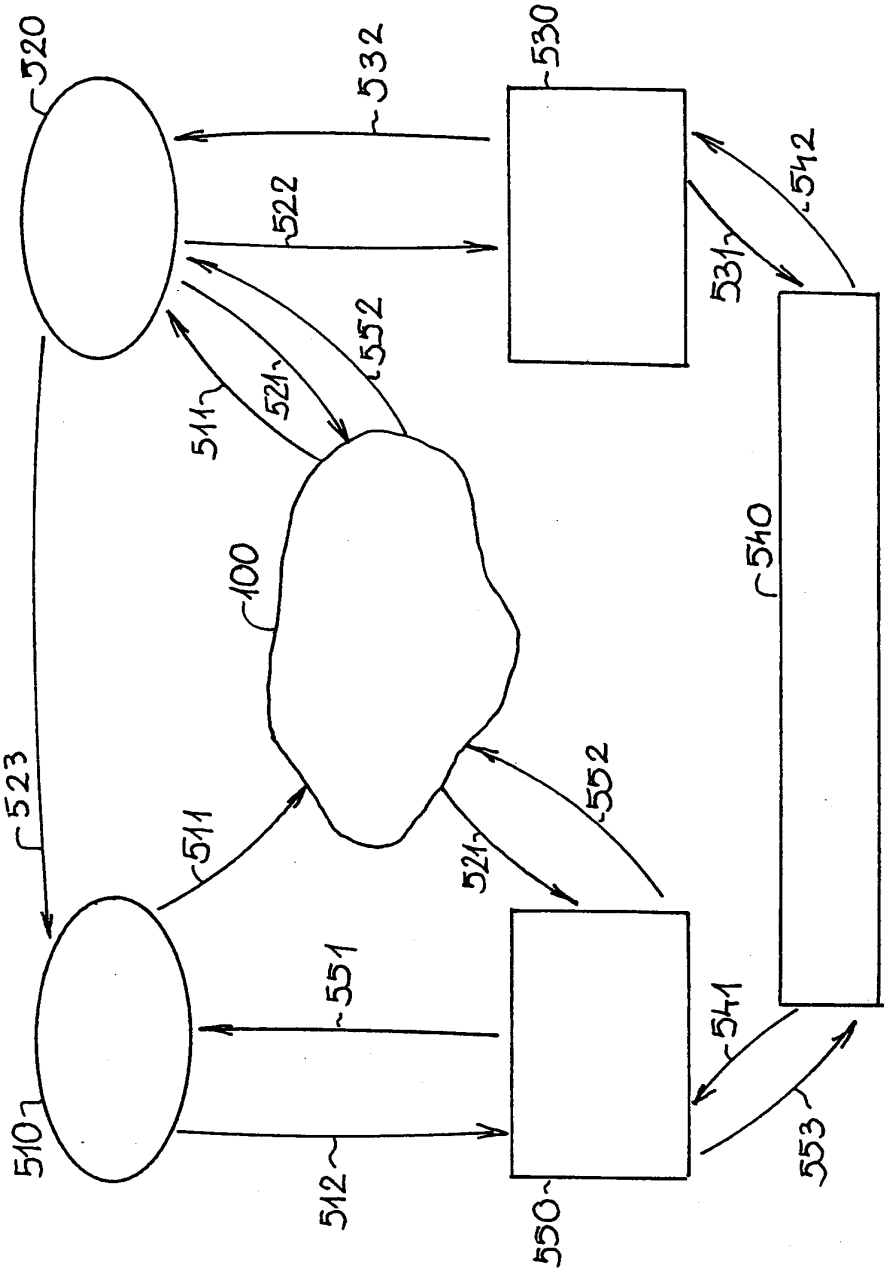

520
532
530
522
542
531
552
521
511
100
540
523
511
552
521
551
541
510
512
550
553

FIG 6.

FR2823882

Publication Title:

Commercial transaction using prepayment card over the Internet, uses personal computer or mobile phone, certification center validates data contained on prepayment card

Abstract:

Abstract of FR2823882

Method has stages as follows: (a) establish connection between the sale site and certification center; collect and send number series and associated secret code to certification center; verify validity of number and code; verify credit on prepaid card; send payment authorization from certification center to sale site if verification of code and credit is positive; notify user of purchase validation. Uses prepaid card having number series and associated secret code, to purchase service or object from sale site to which user has access via at least a partially public network. In second stage the connection to certification center is done automatically as son as the user selects the payment mode by prepaid card. The number series is composed of at least 10 alphanumeric characters and the secret code has at least 16 alphanumeric characters. In the first and last stages the data is transmitted in encrypted format. The user can access the sale site via a mobile phone via the certification center. The second stage is repeated a predetermined number of times in case of negative verification of number and code. An Independent Claim is also included for a prepaid card payment system.

Data supplied from the esp@cenet database - Worldwide

Courtesy of http://v3.espacenet.com

This Patent PDF Generated by Patent Fetcher(R), a service of Stroke of Color, Inc.

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 823 882**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **01 05423**

(51) Int Cl[7] : **G 06 F 17/60**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 23.04.01.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 25.10.02 Bulletin 02/43.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *NEW ACCESS SA Société anonyme suisse* — CH.

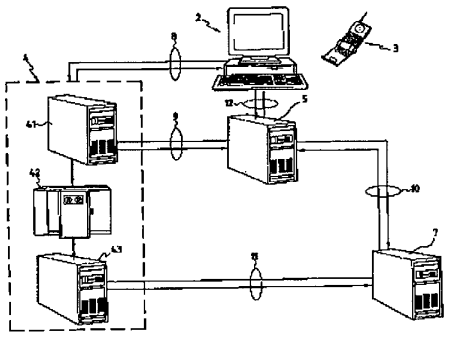
(72) **Inventeur(s) :**

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET BEAU DE LOMENIE.

(54) PROCEDE ET SYSTEME DE VALIDATION DE PAIEMENT.

(57) Pour limiter significativement les conséquences des fraudes dans le domaine des achats à distance via un réseau électronique, un utilisateur possède une carte prépayée à laquelle sont associés un numéro de série et un code secret qui est découvert par l'utilisateur. Lors d'une opération d'achat sur le réseau, l'utilisateur se connecte à un serveur (5) de site de vente en ligne qui, lorsque le mode de paiement par carte prépayée est sélectionné, établit une connexion (9) avec un centre certificateur (4). Le centre vérifie, dans un premier temps, la validité du numéro de série et du code secret puis le crédit disponible de la carte. Si la vérification du numéro de série, du code secret et du crédit disponible est positive, le centre certificateur envoi une autorisation de paiement au serveur (5) du site de vente qui valide l'achat de l'utilisateur.



FR 2 823 882 - A1

Petitioner Askeladden LLC
Exhibit 1002 - Page 184 of 350

2823882

Domaine de l'invention

La présente invention concerne le domaine des transactions commerciales effectuées sur des réseaux électroniques et plus particulièrement les méthodes de sécurisation et de validation du paiement lors de ces transactions.

Art antérieur

Le développement du commerce électronique, notamment sur le réseau Internet, est à l'heure actuelle ralenti par les problèmes de sécurité et de confidentialité rencontrés lors de la phase de paiement.

En effet, de récentes études ont montré que la majorité des utilisateurs du réseau Internet se refusent encore à effectuer des achats sur le réseau car le mode de paiement à distance le plus répandu à ce jour est celui qui consiste à transmettre les coordonnées de sa carte de crédit. Puisqu'il n'existe pas actuellement de méthode de cryptage éprouvée, la garantie de sécurité des données transmises contre toute interception frauduleuse reste très aléatoire. C'est pourquoi la plupart des utilisateurs préfèrent ne pas prendre un tel risque et, de ce fait, abandonnent l'achat faute d'autres alternatives de paiement plus sécurisées.

Outre le fait que ce mode de paiement est réservé aux utilisateurs qui possèdent une carte bancaire, il présente un certain nombre d'inconvénients. Si les coordonnées de la carte de crédit sont interceptées par un tiers qui souhaite les utiliser frauduleusement, les sommes prélevées peuvent être très importantes. De plus, la communication des coordonnées de la carte s'accompagne en général

Petitioner Askeladden LLC
Exhibit 1002 - Page 185 of 350

de l'identité du titulaire ce qui empêche toute confidentialité lors de l'achat. Enfin, ce mode de paiement n'est pas adapté pour des achats de faible montant en raison des frais de banque inhérents à ce type d'opération.

On connaît d'autres possibilités de paiement qui permettent de réaliser des achats à distance sans avoir à communiquer ses coordonnées bancaires ou de carte de crédit. Cependant, ces solutions présentent chacune des inconvénients spécifiques.

Par exemple, le paiement à la livraison, ne permet que l'achat d'articles livrables par colis et pas celui de services ou de produits directement téléchargeables à partir d'un site de vente.

D'autre part, certains sites marchands proposent à leurs utilisateurs d'ouvrir un compte préalablement approvisionné par envoi d'un chèque ou autre et qui sera ensuite débité au fur et à mesure des achats. Ce type de solution représente une charge de gestion supplémentaire non négligeable en complexité et en coût de fonctionnement pour la société qui souhaite vendre ses produits sur un site commercial. D'autre part, si l'utilisateur souhaite effectuer des achats sur d'autres sites marchands, il doit ouvrir ce type de compte dans chacun des sites où il souhaite effectuer ses achats. Etant donnée le nombre et la diversité des sites marchand aujourd'hui, une telle solution paraît déjà peu réaliste.

Objet et description succincte de l'invention

La présente invention vise à remédier aux inconvénients précités et à proposer une solution de paiement simple qui permet à un utilisateur d'effectuer des achats à distance, même de faible montant,

Petitioner Askeladden LLC
Exhibit 1002 - Page 186 of 350

tout en lui garantissant une limitation des risques en cas de fraude et une complète confidentialité lors du paiement.

Ces buts sont atteints grâce à un procédé de paiement pour permettre à un utilisateur, qui possède une carte prépayée comprenant au moins un numéro de série et un code secret associé, l'achat d'un bien ou service proposé sur un site de vente auquel l'utilisateur à accès via un réseau au moins partiellement public, caractérisé en ce qu'il comprend les étapes suivantes:

a) établissement d'une connexion entre le site de vente et un centre certificateur,

b) saisie et envoi du numéro de série et du code secret au site certificateur,

c) vérification de la validité du numéro de série et du code secret,

d) vérification du crédit disponible de la carte, et

e) envoi d'une autorisation de paiement par le centre certificateur au site de vente lorsque la vérification du code secret et crédit disponible est positive.

Par conséquent conformément au procédé de l'invention, le risque absolu pour l'utilisateur est de perdre la valeur de crédit associé à sa carte prépayée. De plus, le procédé offre une totale confidentialité lors de l'opération de paiement.

Dans l'étape a), la connexion au centre certificateur peut être établie automatiquement dès que l'utilisateur sélectionne le mode de paiement par carte prépayée sur le site de vente.

Selon une caractéristique de l'invention, le numéro de série est composé d'une suite d'au moins 10 caractères alphanumériques et le code secret est composé d'une suite d'au moins 16 caractères alphanumériques.

Petitioner Askeladden LLC
Exhibit 1002 - Page 187 of 350

Dans les étapes a) et e) les informations peuvent être transmises sous forme cryptée.

Selon un aspect de l'invention, le procédé est mis en œuvre sur le réseau Internet.

Si l'utilisateur possède un téléphone cellulaire ou similaire, il accède au site de vente via un réseau de téléphonie mobile.

Alternativement, l'utilisateur peut accéder au site de vente par l'intermédiaire du centre certificateur.

Le procédé selon l'invention comprend, en outre, une étape f) de notification de la validation de l'achat à l'utilisateur.

En cas de vérification négative du numéro de série et du code secret, l'étape b) peut être répétée un nombre prédéterminé de fois.

Selon une caractéristique de la présente invention, le procédé comprend, en outre, une étape de cumul du crédit de la carte avec le crédit d'au moins une carte prépayée.

Selon une autre caractéristique de l'invention, le procédé comprend, en outre, une étape d'envoi d'un ou plusieurs ordres de paiement à un service bancaire du site de vente.

La présente invention à également pour objet un système de paiement par carte prépayée pour effectuer des achats sur un réseau au moins partiellement public, la carte comprenant au moins un numéro de série et un code secret et ledit système comprenant un moyen d'accès à un serveur de site de vente via le réseau, caractérisé en ce qu'il comprend en outre un centre informatique en liaison via le réseau avec le serveur de vente, le centre comprenant au moins des moyens d'authentification du numéro de série et du code secret de la carte et des moyens de vérification du crédit disponible de la carte pour le paiement.

Petitioner Askeladden LLC
Exhibit 1002 - Page 188 of 350

Plus particulièrement, le centre informatique comprend un premier serveur en liaison via le réseau avec le serveur de vente, une unité de stockage de base de données et un second serveur en liaison via le réseau avec un serveur pour l'envoi des ordres de paiement.

Selon un aspect particulier de l'invention, le serveur de site de vente, le premier et le second serveurs du centre comprennent des moyens de cryptage et de décryptage pour la transmission des données.

Brève description des dessins

D'autres caractéristiques et avantages de l'invention ressortiront de la description suivante de modes particuliers de réalisation de l'invention, donnés à titre d'exemples non limitatifs, en référence aux dessins annexés, sur lesquels:

- la figure 1 est une vue schématique globale du système selon l'invention,
- la figure 2 est un organigramme illustrant les étapes du procédé selon l'invention,
- la figure 3 est un organigramme montrant des étapes additionnelles du procédé conformément à un mode de réalisation de l'invention, et
- la figure 4 est une vue schématique, en développée, d'un mode de réalisation d'une carte prépayée selon l'invention.

Description détaillée des modes de réalisation de l'invention

La présente invention est basée sur l'utilisation de cartes prépayées en tant que moyen de paiement pour l'achat de biens et/ou

Petitioner Askeladden LLC
Exhibit 1002 - Page 189 of 350

de services dits "en ligne", c'est-à-dire proposés à des utilisateurs d'un réseau public tel que le réseau Internet. Le principe de prépaiement des cartes qui est utilisé ici est sensiblement le même que celui déjà connu pour les cartes téléphoniques qui permettent de disposer d'un crédit de communications téléphoniques sans abonnement. En effet, la carte prépayée utilisée dans l'invention est une carte anonyme à laquelle est associée une valeur de crédit. Ainsi, comme pour une carte téléphonique, l'utilisateur achète une carte qui lui confère une valeur de crédit permettant d'effectuer des achats à distance sur un réseau.

A titre d'exemple non limitatif, les cartes pourraient être vendue pour des valeurs de crédit de l'ordre de 100, 200 ou 500 francs.

La valeur de crédit de la carte constitue le risque financier maximum pour l'utilisateur. En effet, dans le cas le plus défavorable pour l'utilisateur, c'est-à-dire la cas où il se fait dérober sa carte et ne le signale pas à la société qui gère ces dernières, seule la valeur de crédit de la carte peut être perdue et rien de plus contrairement au cas où les coordonnées de la carte de crédit de l'utilisateur sont interceptées, ce qui représente un intérêt très limité pour les éventuels fraudeurs. Ceci constitue un avantage important de la présente invention. En effet, comme il sera expliqué en détail dans la suite du texte, un utilisateur, muni d'une carte prépayée, ne communique aucune coordonnée bancaire, ni même son identité au moment du paiement selon le procédé de l'invention.

Pour garantir la cohérence et la sécurité du mode de paiement selon l'invention, il est préférable qu'une même société soit chargée de l'émission et de la gestion des cartes prépayées ainsi que de l'autorisation du paiement à partir de ces cartes.

La figure 4 illustre un mode de réalisation d'une carte prépayée selon l'invention. Une carte 100 comporte principalement sur une de ses faces 101 une zone 103 comprenant le code secret qui est

Petitioner Askeladden LLC
Exhibit 1002 - Page 190 of 350

recouvert d'un matériau d'occultation qu'il faut gratter pour découvrir le code et d'une zone 104 dans laquelle le numéro de série de la carte est inscrit sous forme visible. D'autres espaces non utilisés sur la carte 100 peuvent aussi comporter des zones 105 et 106 indiquant respectivement les coordonnées d'un service clientèle et l'adresse électronique du site de la société émettrice des cartes de prépayées. Les autres espaces libres sur les deux faces 101 et 102 de la carte 100 peuvent être notamment occupés par des illustrations publicitaires au bénéfice des sites de vente ou de la société émettrice des cartes.

Chaque carte comporte un numéro de série et un code secret qui lui sont propres. Le code secret de par sa nature est évidemment réservé à l'utilisateur pour s'authentifier lors de l'achat. Par contre, le numéro de série de chaque carte qui est enregistré dans la base de données de la société émettrice ne sera activé qu'une fois la carte livrée et payée par un revendeur qui va revendre à des utilisateurs les cartes au détail. Le terme activé signifie que le numéro de série stocké dans la base de donnée est indexé d'un code qui permet de définir si la carte détenue par un utilisateur à été valablement acquise. Ainsi, toute carte soustraite lors de la fabrication ou de la livraison ne sera jamais activée, ce qui la rend inutilisable. Par conséquent, aucune mesure de précaution particulière n'est nécessaire lors de la fabrication et du transport des cartes, celles-ci n'étant pas encore utilisables. Cette méthode peut être également utilisée lorsque l'utilisateur signal le vol de sa carte pour empêcher un tiers non autorisé d'utiliser cette dernière.

L'invention est donc destinée aux utilisateurs qui, non seulement, possèdent une ou plusieurs carte(s) prépayée(s) comme décrit ci-dessus mais aussi qui ont accès à un réseau ouvert ou public tel que, par exemple, le réseau Internet. Par souci de simplification, le réseau ouvert ou public à travers lequel les différentes parties

Petitioner Askeladden LLC
Exhibit 1002 - Page 191 of 350

interviennent dans l'opération d'achat sera simplement dénommé "réseau" dans la suite de la description. De même, la société qui a en charge la distribution, l'authentification et la gestion des cartes prépayées sera dénommée "société garante" par la suite.

La figure 1 est une vue globale du système montrant les relations entre les différentes parties intervenant selon le procédé de l'invention. Les parties qui interviennent principalement lors d'une opération d'achat sont un utilisateur, un site de vente de biens et/ou de services en ligne et un centre certificateur des cartes prépayées administré par la société garante. Le système peut comprendre en outre des liens entre un organisme bancaire du site de vente et un service de gestion des ordres de paiement de la société garante.

Pour avoir accès au réseau, l'utilisateur possède un terminal de connexion qui peut être fixe, tel qu'un ordinateur personnel 2 équipé d'un modem, ou bien mobile, tel qu'un téléphone cellulaire 3 dont l'opérateur propose un service d'accès au réseau ou similaire tel que les services "WAP" par exemple.

La société garante dispose d'un centre de stockage et de traitements informatique 4 qui comprend un premier serveur 41 essentiellement en charge de l'authentification et de la gestion des cartes prépayées en circulation, une unité de base de données 42 sur laquelle sont stockées et mises à jour toutes les informations relatives aux cartes, et un second serveur 43 en liaison, via une ligne 11, avec un serveur 7 de l'organisme bancaire du site de vente. Le centre certificateur de la société garante est principalement constitué par le serveur 41 en combinaison avec une partie de l'unité 42 qui comprend les bases de données sur lesquelles sont stockées les informations utiles (numéro de série, code secret, index d'activation...) pour la gestion des autorisations de paiement. Le site de vente à partir duquel l'utilisateur va effectuer son achat se trouve sur un serveur 5 qui peut

Petitioner Askeladden LLC
Exhibit 1002 - Page 192 of 350

être en liaison avec l'utilisateur, le centre 4, et le serveur 7 respectivement par des lignes 12, 9 et 10. Les serveurs 5, 7, 41 et 43 représentés dans le système de la figure 1 comprennent de manière conventionnelle des moyens de connexion au réseau, des moyens de stockage et des moyens de traitement. Les serveurs 5, 41 et 43 peuvent comprendre, en outre, des moyens de cryptage et de décryptage afin de réaliser des transmissions de données sous forme codée.

L'utilisateur se connecte au site de vente pour choisir un produit à acheter. Selon l'invention, l'utilisateur a deux possibilités: soit il se connecte directement au serveur 5 du site de vente par la ligne 12, soit il passe par le serveur 41 du centre 4 qui lui propose une liste de tous les sites de vente qui sont compatibles avec le paiement par carte prépayée. Dans ce dernier cas, le serveur 41 constitue aussi un "portail" d'accès pour les utilisateurs aux sites de vente adhérant au mode de paiement de l'invention. Le serveur 41 peut encore mettre à disposition de l'utilisateur, par exemple, des services de consultation pour renseigner l'utilisateur sur le crédit restant sur sa carte ainsi que sur l'historique des achats précédents.

Toutes les lignes de communication 8 à 12 peuvent être des lignes de transmissions bidirectionnelles de type filaire électrique ou optique. Néanmoins, les lignes 8 et 12 peuvent être également des liaisons radio fréquence (RF) dans le cas où l'utilisateur se connecte avec un téléphone cellulaire ou un terminal équipé de moyen d'accès au réseau sans fil.

Le procédé de l'invention qui est mis en œuvre dans le système de la figure 1 va être décrit en relation avec la figure 2.

Au début, l'utilisateur consulte les offres du site de vente soit en se connectant directement au serveur 5 soit en passant par un portail d'accès hébergé sur le serveur 41 qui se connecte ensuite au serveur 5.

Petitioner Askeladden LLC
Exhibit 1002 - Page 193 of 350

Après avoir choisi un article proposé à la vente sur le site, l'utilisateur en possession d'une ou plusieurs carte(s) prépayée(s) sélectionne le mode de paiement par carte prépayée dans une étape ST1. A ce moment, dans une étape ST2, le serveur 5 établit une connexion avec le serveur 41 du centre 4. Dans une étape ST3, l'utilisateur est invité à saisir le numéro de série de sa carte ainsi que le code secret qu'il aura découvert en grattant le revêtement d'occultation. Ces deux numéros sont alors envoyés au serveur 41 qui, dans une étape S4, interroge la base de données stockée sur l'unité 42 pour vérification. La vérification relative à la carte prépayée s'effectue en deux étapes ST5 et ST6. On vérifie d'abord l'authenticité de la carte en recherchant dans la base de données si le numéro de série et son code secret associé sont bien répertoriés comme correspondant à une carte valide, c'est-à-dire une carte vendue conformément aux exigences de sûreté décrites plus haut.

Si le numéro de série et/ou le code secret ne sont pas reconnus par la base de donnée, un refus d'autorisation de paiement est envoyé au serveur 5 du site de vente qui le notifie à l'utilisateur lors des étapes ST9 et ST10. Comme la non reconnaissance du numéro de série et du code secret associé peut provenir d'une erreur de saisie de l'utilisateur, il peut être prévu de donner à l'utilisateur un ou plusieurs essais avant de refuser l'autorisation de paiement. Ceci pourrait être mis en œuvre dans une étape ST51 où l'on vérifie que l'utilisateur a encore droit à un nouvel essai tant que le nombre T d'essais n'excède pas une valeur prédéterminée i. Si tel est le cas, on revient à l'étape de saisie ST3 en incrémentant au préalable le nombre T d'essais dans une étape ST52.

Si le numéro de série et le code secret de la carte sont reconnus dans la base de données, le crédit disponible sur la carte est comparé au montant de l'achat à effectuer. Le crédit disponible qui est

Petitioner Askeladden LLC
Exhibit 1002 - Page 194 of 350

mémorisé dans la base de donnée peut correspondre à la valeur initiale de la carte si celle-ci est utilisée pour la première fois ou bien au crédit restant sur la carte qui est calculé et actualisé dans la base de données après chaque opération d'achat effective.

Si le crédit disponible sur la carte est suffisant, le centre 4 via son serveur 41 envoi une autorisation de paiement au serveur du site de vente qui notifie à l'utilisateur que son paiement est validé respectivement dans des étapes ST7 et ST8. L'opération d'achat est ainsi terminée dans une étape ST11 où le serveur 5 est déconnecté du serveur 41. Le nouveau crédit disponible sur la carte est calculé et mis à jour immédiatement dans la base de données.

Par contre, si le crédit encore disponible sur la carte ne permet pas d'atteindre le montant de l'achat, un refus d'autorisation de paiement est envoyé au serveur du site de vente qui le notifie à l'utilisateur.

Pour accroître le niveau de sûreté dans le système, le numéro de série, le code secret de la carte et l'autorisation de paiement peuvent être transmis sous forme cryptée. Dans ce cas les serveurs qui envoient les données doivent comprendre au moins des moyens logiciels et/ou matériels de cryptage et les serveurs qui reçoivent ces données doivent comprendre au moins des moyens similaires de décryptage compatibles pour déchiffrer les données reçues.

Alternativement, l'utilisateur peut être en possession d'autres cartes qui ne permettent pas d'atteindre le montant de l'achat les unes indépendamment des autres mais qui cumulées entre elles présentent un crédit disponible suffisant.

A cet effet, l'invention propose une solution qui permet à l'utilisateur de cumuler le crédit de plusieurs cartes afin d'atteindre un crédit total suffisant pour l'achat. Cette solution est expliquée en relation avec les étapes ST61 à ST64 illustrées en figure 3. Lors de

Petitioner Askeladden LLC
Exhibit 1002 - Page 195 of 350

l'étape ST6, si le crédit de la première carte reconnue n'est pas suffisant, l'utilisateur peut être invité à indiquer s'il possède d'autres cartes. S'il ne possède pas de carte supplémentaire on retourne à l'étape ST9. Si l'utilisateur possède une ou plusieurs carte(s) supplémentaire(s), on mémorise le crédit initiale C1 de la première carte, on invite l'utilisateur à saisir le numéro de série et le code secret de la carte supplémentaire qui sont vérifiés selon la méthode déjà décrit en figure 2 et on calcule le nouveau crédit total Ctot disponible en additionnant le crédit C1 avec le crédit Csupp de la carte supplémentaire. Les étapes ST61 à ST64 peuvent être répétées plusieurs fois pour atteindre un crédit disponible suffisant sous réserve que l'utilisateur possède une ou plusieurs cartes qui permettent un cumul de crédit suffisant.

Le serveur 7 qui est en relation avec l'organisme bancaire du site de vente reçoit des ordres de paiement du serveur 43 du centre 4 de la société garante. Ainsi, la banque qui gère les comptes de la société propriétaire du site de vente peut recevoir un ordre de paiement dès qu'un achat est effectué et par conséquent créditer le compte du propriétaire du site de vente. Cependant, pour des raisons de coût et de pratique, il est préférable que le serveur 43 envoie les ordres de paiement groupés à des dates prédéterminés. Comme décrit plus haut, de tels envois de données peuvent se faire sous forme cryptée.

Par conséquent, la présente invention propose une solution de paiement confidentielle qui permet de limiter les risques à l'achat pour le consommateur d'une façon claire même pour de faible montant. Cette solution est donc de nature à convaincre les utilisateurs à réaliser des achats sur réseau. De plus, l'invention apporte également des garanties sur la solvabilité des clients aux

Petitioner Askeladden LLC
Exhibit 1002 - Page 196 of 350

entreprises qui vendent leurs produits et/ou services en ligne sans alourdir la charge de gestion pour ces dernières.

REVENDICATIONS

1. Procédé de paiement pour permettre à un utilisateur, qui possède une carte prépayée comprenant au moins un numéro de série et un code secret associé, l'achat d'un bien ou service proposé sur un site de vente auquel l'utilisateur à accès via un réseau au moins partiellement public, caractérisé en ce qu'il comprend les étapes suivantes:

a) établissement d'une connexion entre le site de vente et un centre certificateur,

b) saisie et envoi du numéro de série et du code secret au centre certificateur,

c) vérification de la validité du numéro de série et du code secret,

d) vérification du crédit disponible de la carte, et

e) envoi d'une autorisation de paiement par le centre certificateur au site de vente lorsque la vérification du code secret et crédit disponible est positive.

2. Procédé selon la revendication 1, caractérisé en ce que dans l'étape b), la connexion au centre certificateur est effectuée automatiquement dès que l'utilisateur sélectionne le mode de paiement par carte prépayée sur le site de vente.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce que le numéro de série est composé d'une suite d'au moins 10 caractères alphanumériques et en ce que le code secret est composé d'une suite d'au moins 16 caractères alphanumériques.

Petitioner Askeladden LLC
Exhibit 1002 - Page 198 of 350

4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce dans les étapes a) et e) les informations sont transmises sous forme cryptée.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ledit réseau est le réseau Internet.

6. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que l'utilisateur accède au site de vente via un réseau de téléphonie mobile.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que l'utilisateur accède au site de vente par l'intermédiaire du centre certificateur.

8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'il comprend en outre une étape f) de notification de la validation de l'achat à l'utilisateur.

9. Procédé selon l'une quelconque des revendications 1 à 8, caractérisé en ce que l'étape b) est répétée un nombre prédéterminé de fois en cas de vérification négative du numéro de série et du code secret.

10. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'il comprend en outre, une étape de cumul du crédit de la carte avec le crédit d'au moins une carte prépayée.

11. Procédé selon l'une quelconque des revendications 1 à 10, caractérisé en ce qu'il comprend en outre une étape d'envoi d'un ou plusieurs ordres de paiement à un service bancaire du site de vente.

12. Système de paiement par carte prépayée pour effectuer des achats sur un réseau au moins partiellement public, ladite carte comprenant au moins un numéro de série et un code secret et ledit système comprenant un moyen d'accès (2; 3) à un serveur (5) de site de vente via le réseau, caractérisé en ce qu'il comprend en outre un centre informatique (4) en liaison (9) via le réseau avec le serveur de vente, ledit centre comprenant au moins des moyens d'authentification du numéro de série et du code secret de la carte et des moyens de vérification du crédit disponible de la carte pour le paiement.

13. Système selon la revendication 12, caractérisé en ce que ledit centre (4) comprend un premier serveur (41) en liaison (9) via le réseau avec le serveur de vente (5), une unité de stockage de base de données (42) et un second serveur (43) en liaison (11) via le réseau avec un serveur (7) pour l'envoi des ordres de paiement.

14. système selon la revendication 13, caractérisé en ce que le serveur (5) de site de vente, le premier et le second serveur du centre (4) comprennent des moyens de cryptage et de décryptage pour la transmission des données.

Petitioner Askeladden LLC
Exhibit 1002 - Page 200 of 350

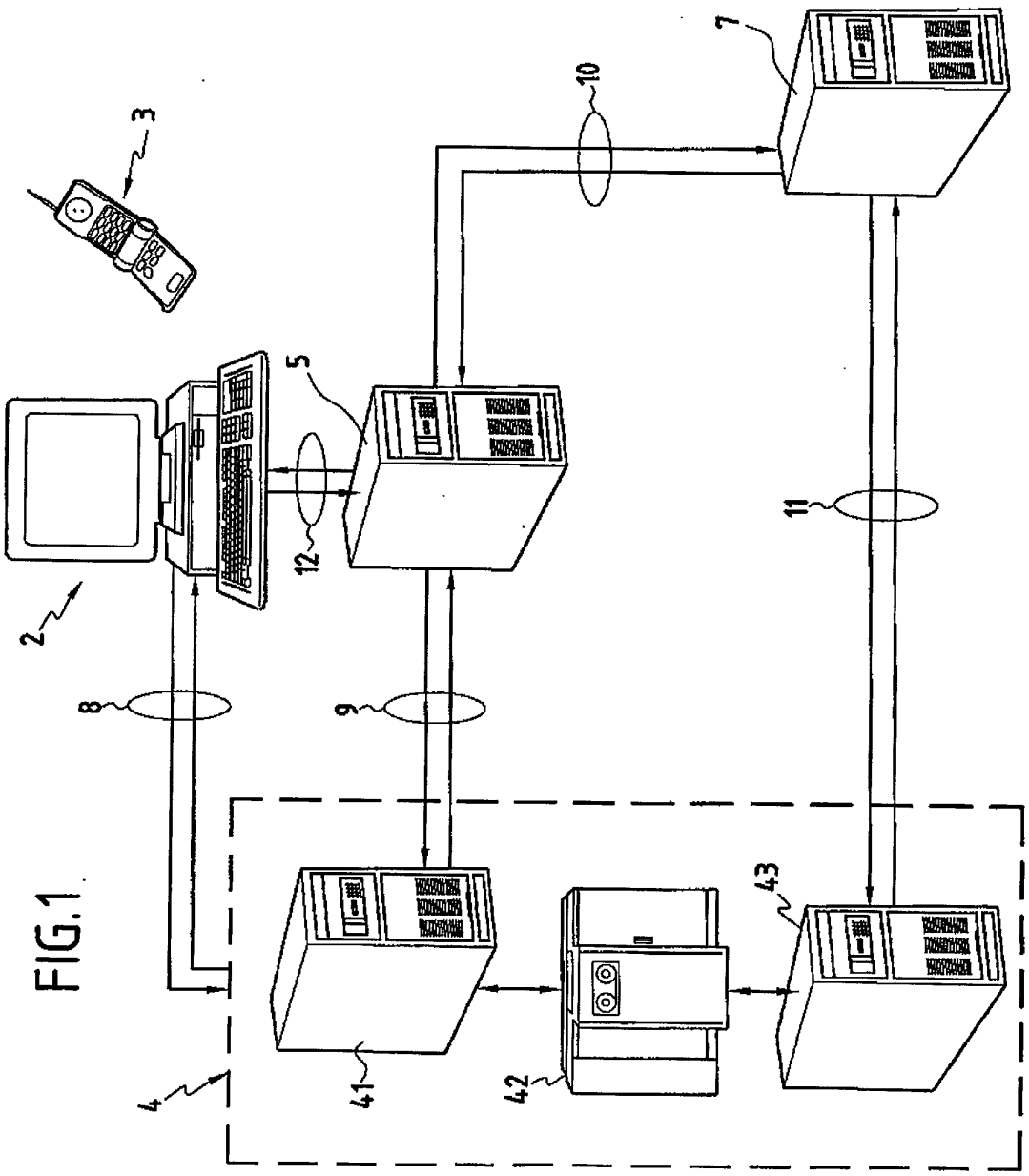


FIG.1

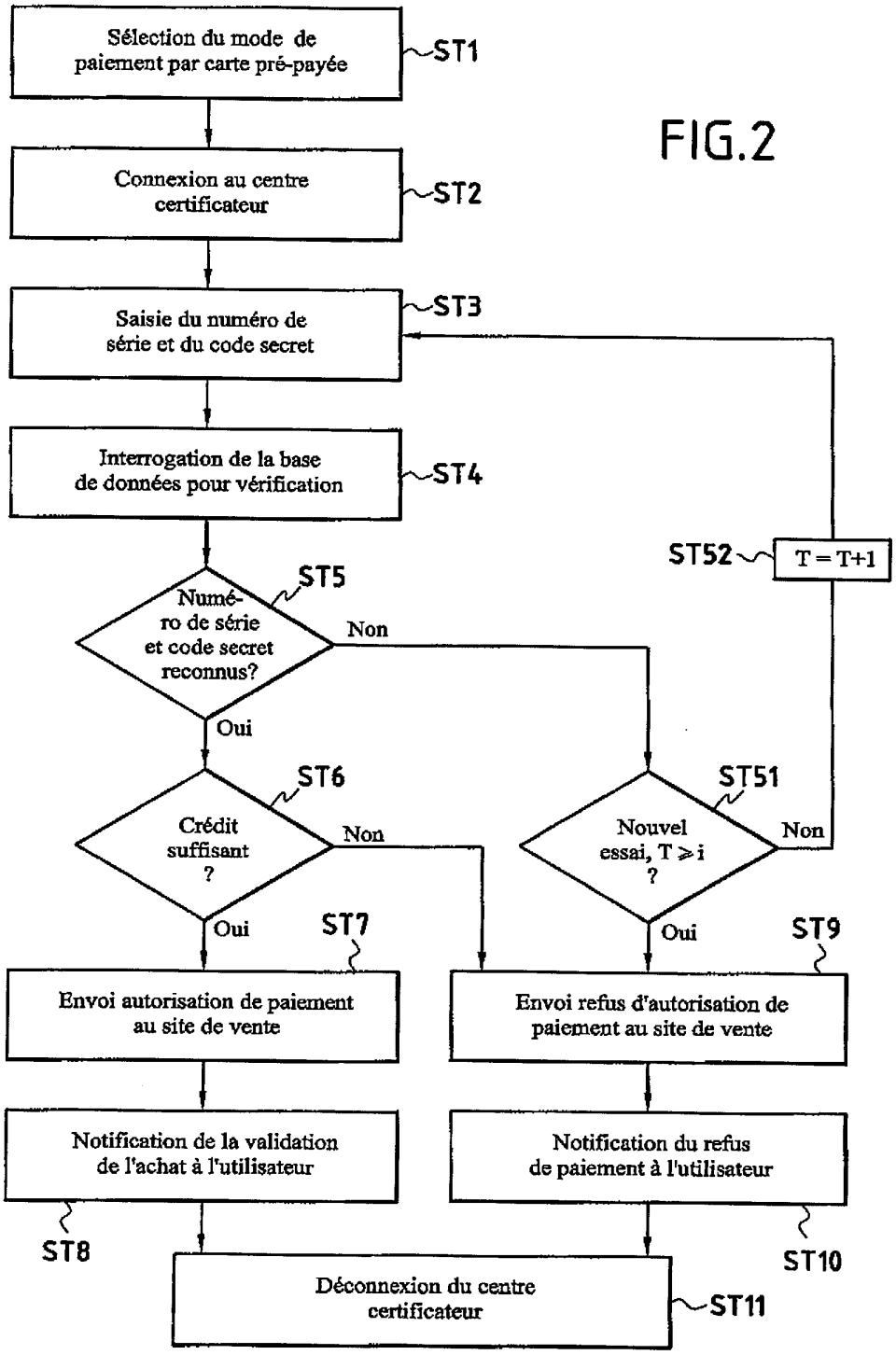

Sélection du mode de paiement par carte pré-payée
ST1
Connexion au centre certificateur
ST2
Saisie du numéro de série et du code secret
ST3
Interrogation de la base de données pour vérification
ST4
ST52
T = T+1
ST5
Numéro de série et code secret reconnus?
Non
Oui
ST6
Crédit suffisant ?
Non
Oui
ST51
Nouvel essai, T ⩾ i ?
Non
Oui
ST7
ST9
Envoi autorisation de paiement au site de vente
Envoi refus d'autorisation de paiement au site de vente
Notification de la validation de l'achat à l'utilisateur
Notification du refus de paiement à l'utilisateur
ST8
ST10
Déconnexion du centre certificateur
ST11

FIG.2

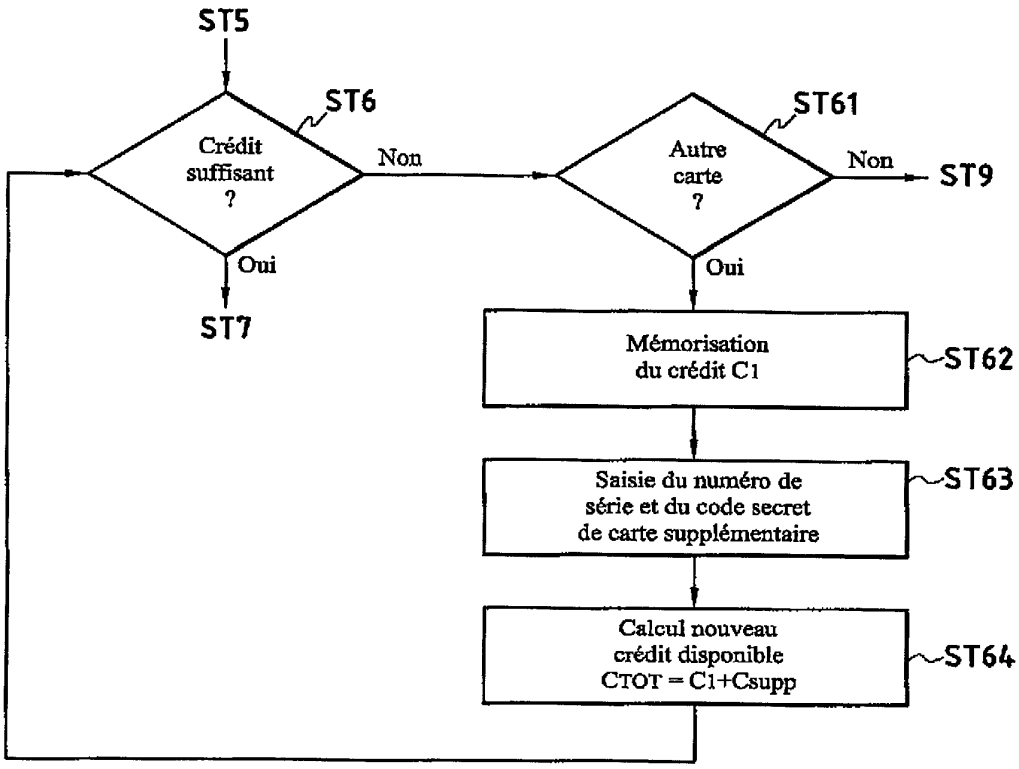

ST5
ST6
Crédit suffisant ?
Non
Oui
ST7
ST61
Autre carte ?
Non
ST9
Oui
Mémorisation du crédit C1
ST62
Saisie du numéro de série et du code secret de carte supplémentaire
ST63
Calcul nouveau crédit disponible CTOT = C1+Csupp
ST64

FIG.3

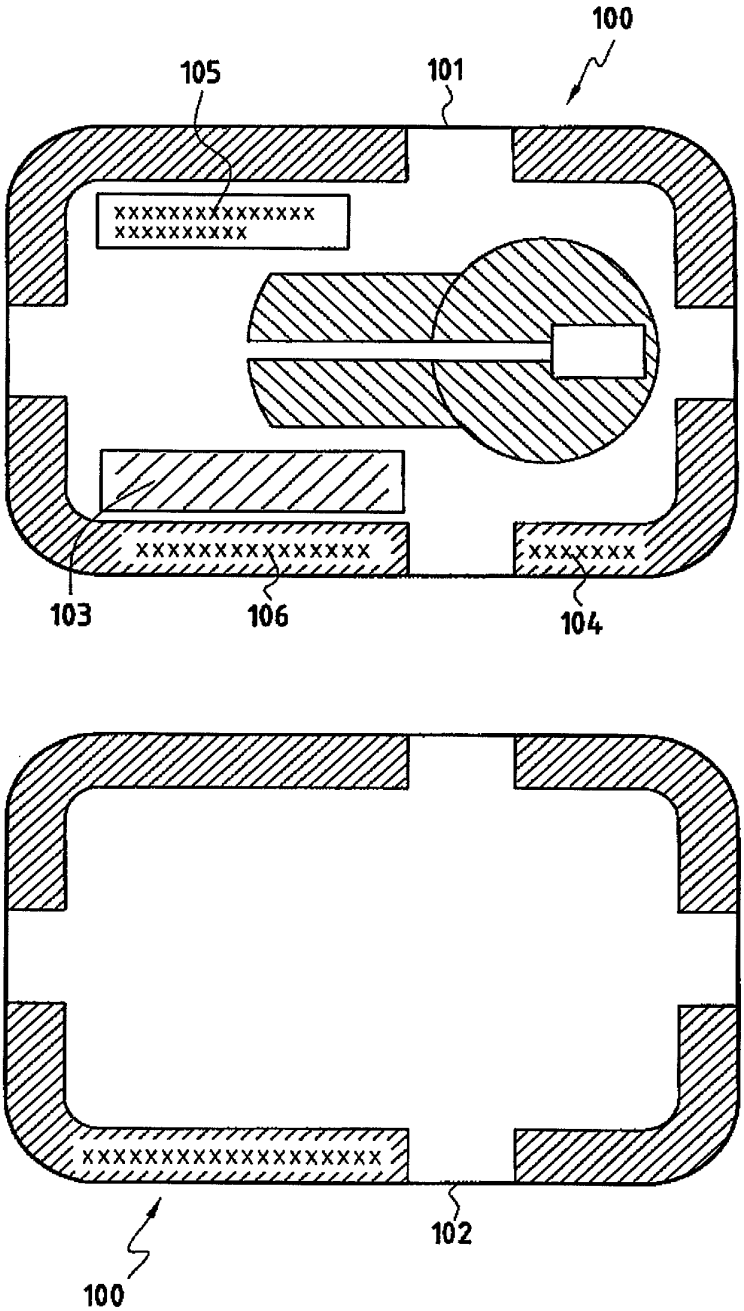

100
105
101
xxxxxxxxxxxxxxx
xxxxxxxxxx
xxxxxxxxxxxxxxx
xxxxxxx
103
106
104
xxxxxxxxxxxxxxxxxxx
102
100

FIG.4

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2823882

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 612236
FR 0105423

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
Y	FR 2 798 028 A (GEMPLUS CARD INT) 2 mars 2001 (2001-03-02)	1,4,5,12	G06F17/60
A	* page 5, ligne 7 - ligne 25 * * page 6, ligne 15 - page 7, ligne 38 * * revendications 1-3,7 *	8	
Y	FR 2 747 962 A (ITTAH AARON) 31 octobre 1997 (1997-10-31)	1,4,5,12	
A	* le document en entier *	3	
A	FR 2 780 679 A (ONGOUYA JEAN FELIX) 7 janvier 2000 (2000-01-07) * page 2, ligne 11 - ligne 16 * * page 4, ligne 3 - page 5, ligne 32 * * revendications 14-16,19; figure 9 *	1,3,5, 10,12	
A	WO 00 70514 A (COHEN GREGORY A ;CYBERMOOLA INC (US); FREEMAN ERIC S (US); RUIZ HE) 23 novembre 2000 (2000-11-23) * page 4, ligne 20 - page 8, ligne 20 *	1,2,5,8, 12-14	
A	WO 01 09853 A (SOFTWARE COM INC) 8 février 2001 (2001-02-08)		DOMAINES TECHNIQUES RECHERCHÉS (Int.Cl.7) G07F

1

Date d'achèvement de la recherche	Examinateur
10 mai 2002	Bocage, S

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

Petitioner Askeladden LLC
Exhibit 1002 - Page 205 of 350

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0105423 FA 612236

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 10-05-2002
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
FR 2798028	A	02-03-2001	FR	2798028 A1	02-03-2001
			AU	7015300 A	19-03-2001
			WO	0115095 A1	01-03-2001
FR 2747962	A	31-10-1997	FR	2747962 A1	31-10-1997
FR 2780679	A	07-01-2000	FR	2780679 A1	07-01-2000
WO 0070514	A	23-11-2000	AU	1833200 A	05-12-2000
			WO	0070514 A1	23-11-2000
WO 0109853	A	08-02-2001	AU	7135900 A	19-02-2001
			WO	0109853 A1	08-02-2001

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 April 2005 (07.04.2005)

PCT

(10) International Publication Number
WO 2005/031541 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2004/031537

(22) International Filing Date:
27 September 2004 (27.09.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/506,370 26 September 2003 (26.09.2003) US

(71) Applicant *(for all designated States except US)*: **MASTERCARD INTERNATIONAL INCORPORATED** [US/US]; 2000 Purchase Street, Purchase, NY 10577 (US).

(72) Inventors; and

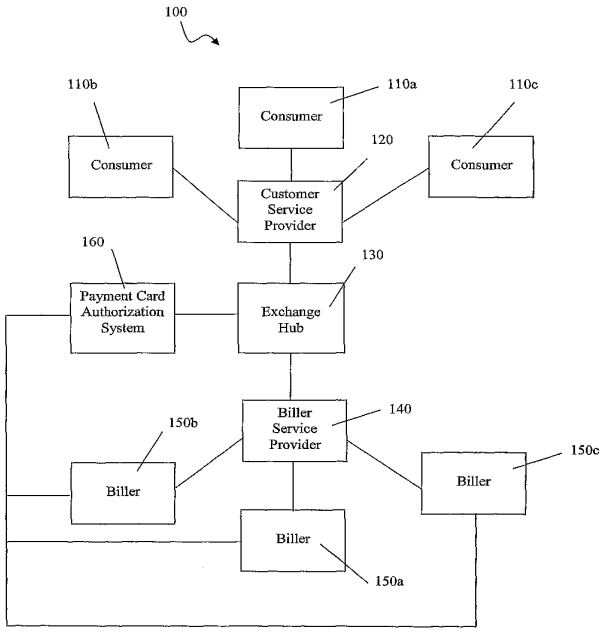
(75) Inventors/Applicants *(for US only)*: **CONFORTI, Cathleen, M.** [US/US]; 2404 Alexandra Court, Howell, NJ 07731 (US). **CAREY, Thomas** [US/US]; 239 West 260th Street, Riverdale, NY 10471 (US). **SULLIVAN, Dennis, H.** [US/US]; 1800 West Roscoe Street, #411, Chicago, IL 60657 (US). **SMITH, Thomas, D.** [US/US]; 4208 Austin View Court, St. Charles, MO 63304 (US).

(74) Agent: **SCHEINFELD, Robert, C.**; Baker Botts L.L.P., 30 Rockefeller Plaza, New York, NY 10112-4498 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, 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, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR USING PAYMENT CARDS AS A PAYMENT OPTION WITHIN AN ONLINE BILL PAYMENT AND PRESENTMENT SOLUTION



(57) Abstract: An exchange hub is provided that is programmed to receive by way of an open, standardized, secure messaging protocol, a payment card transaction request from a consumer's CSP. A consumer transmits to an EBPP system a request to pay a bill electronically using a payment card. The consumer's payment card transaction request is submitted to the consumer's CSP. The payment card transaction request is then submitted to the exchange hub of the EBPP system. The exchange hub parses the payment card transaction request, and generates a payment message to the biller's acquiring bank (the "acquirer"). The acquirer generates an authorization request message and transmits it to the issuer of the consumer's payment card. The issuer either approves or denies the consumer's payment card transaction request, and notifies the acquirer. The acquirer then, in turn, submits and appropriate approval or denial response to the exchange hub of the EBPP system. If the transaction is approved by the acquirer, the acquirer settles with the biller, and the consumer pays the payment card issuer when the consumer is eventually billed for the payment card transaction.

WO 2005/031541 A2

Petitioner Askeladden LLC
Exhibit 1002 - Page 207 of 350

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

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.

METHOD AND SYSTEM FOR USING PAYMENT CARDS AS A PAYMENT OPTION WITHIN AN ONLINE BILL PAYMENT AND PRESENTMENT SOLUTION

SPECIFICATION

CROSS-REFERENCE TO RELATED APPLICATION

This application claims priority to a United States Provisional Application entitled "Method and System For Using Payment Cards as a Payment Option Within an Online Bill Payment and Presentment Solution," Serial No. 60/506,370, which was filed on September 26, 2003, and is incorporated by reference into the present application.

FIELD OF THE INVENTION

The present invention relates generally to a method and system for electronic bill payment and presentment over a communications network, and more particularly to a method and system for enabling consumers to use payment cards and other non-cash vehicles to pay their bills in an electronic bill payment and presentation system.

BACKGROUND OF THE INVENTION

The process of presenting and paying bills online instead of using traditional paper-based methods is known as electronic bill payment and presentment ("EBPP"). EBPP is a fast growing segment of the e-commerce market. Increasingly, consumers are turning to EBPP systems to pay their bills electronically, preferring EBPP to the laborious and time consuming chore of writing checks, sealing envelopes, purchasing stamps, and walking their bill payment to the mailbox.

Currently, there are two basic EBPP models: the direct model, and the consolidator model. In the direct model, a biller presents its electronic bill to a consumer by way of the biller's own Web site. The consumer must visit the biller's Web site to view the bill, and then must pay it at the biller's Web site. The biller's Web site typically offers the consumer a number of payment options, including directly debiting the consumer's bank account, or using a payment card such as a credit card, debit card, pre-paid card, or other non-cash payment account vehicle.

The direct model has the disadvantage that it requires the consumer to individually visit a different Web site for each electronic bill that the consumer wishes to electronically pay. The consolidator EBPP model attempts to overcome this disadvantage by consolidating for the consumer multiple bills from multiple billers in aggregate for presentment on a single Web site, such as the consumer's online banking web site. In the consolidator model, the consumer need only visit a single Web site to electronically view and pay his bills. This consolidation is typically accomplished by using a centralized switching facility or "exchange hub," that routes aggregated electronic bills to a customer service provider ("CSP") for presentment to consumers who are enrolled with the CSP. The exchange hub also routes electronic payments of these bills by consumers to the appropriate biller service provider ("BSP"), which serves as the billing agent for the biller.

Currently, however, the consolidator EBPP model has the disadvantage that payment cards, such as credit cards, debit cards, prepaid cards, or other non-cash payment vehicles, are not available to consumers as a payment option.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide consumers with the ability to use payment cards to electronically pay electronic bills in an EBPP system.

In accordance with the present invention, an exchange hub is provided that is programmed to receive, by way of an open, standardized, secure messaging protocol, a payment card transaction request from a consumer's CSP. In an exemplary embodiment of the present invention, the consumer transmits to an EBPP system a request to pay a bill electronically using a payment card. The consumer's payment card transaction request is submitted to the consumer's CSP, along with all the details necessary for authorization processing (such as card-holder name, payment card account number, expiration date, etc.). The payment card transaction request may then be batched by the CSP and submitted to the exchange hub (*e.g.*, MasterCard's Remote Payment and Presentment System ("RPPS")) of the EBPP system. The exchange hub may then parse the payment card transaction request, and generate a payment message to the biller's acquiring bank (the "acquirer").

From here on, the conventional process of payment card authorization is utilized. The acquirer generates an authorization request message and transmits it

Petitioner Askeladden LLC
Exhibit 1002 - Page 210 of 350

to the issuer of the consumer's payment card. The issuer either approves or denies the consumer's payment card transaction request, and notifies the acquirer. The acquirer then, in turn, submits and appropriate approval or denial response to the exchange hub of the EBPP system. If the transaction is approved by the acquirer, the acquirer settles with the biller, and provides remittance data to the biller. The consumer pays the payment card issuer when the consumer is eventually billed for the payment card transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

Further objects, features and advantages of the invention will become apparent from the following detailed description taken in conjunction with the accompanying figures showing illustrative embodiments of the invention, in which:

FIG. 1 is a block diagram depicting an EBPP system with a payment card payment option, in accordance with an exemplary embodiment of the present invention;

FIG. 2 is a block diagram depicting the components of the EBPP system and a payment card authorization system in accordance with an exemplary embodiment of the present invention; and

FIG. 3 is a flow chart depicting a process by which a consumer pays an electronic bill in the EBPP system in accordance with an exemplary embodiment of the present invention.

Throughout the figures, the same reference numerals and characters, unless otherwise stated, are used to denote like features, elements, components or portions of the illustrated embodiments. Moreover, while the subject invention will now be described in detail with reference to the figures, it is done so in connection with the illustrative embodiments. It is intended that changes and modifications can be made to the described embodiments without departing from the true scope and spirit of the subject invention as defined by the appended claims.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 is a block diagram depicting the overall relationship of the main components in an EBPP system **100**, in accordance with an exemplary embodiment of the present invention. The components of the EBPP system **100**

Petitioner Askeladden LLC
Exhibit 1002 - Page 211 of 350

exchange data via a conventional computer network. The computer network may be, for example, the Internet, in which case the components may communicate using World Wide Web protocols such as HTTP and HTTPS. However those of ordinary skill in the art will appreciate that the various components of EBPP system **100** may alternatively communicate via virtual private networks (VPN), local area networks (LAN), private wide area networks (WAN), or any other conventional data communications network using any standard networking protocol.

The EBPP system **100** enables one or more consumers **110a-c** (three are shown) to use a computer to electronically view, and pay, bills for goods or services that are electronically presented to them by one or more billers **150a-c** (three are shown). For the purposes of this application, "computer" shall be deemed to include any computer capable of networked data communication with other components of the EBPP system **100**. Thus, "computer" includes not just desktop PCs, but laptop computers, server computers, handheld computers, personal digital assistants (PDAs), and cellular telephones. Preferably, the computers used by the consumers **110a-c** are programmed with conventional Web browsers, which provide the graphical user interface through which the consumers **110a-c** may view and pay their bills.

The customer service provider component **120** ("CSP") is preferably a bank with which the consumers **110a-c** have opened a financial account, but may also include non-financial third party bill processors with which consumers **110a-c** have enrolled for EBPP bill payment. The CSP **120** provides the consumers **110a-c** with the user interface for interacting with the EBPP system **100**. The CSP **120** delivers to the consumers' **110a-c** computers electronic billing data from the billers **150a-c**, which the consumers **110a-c** may view using a Web browser. Via the interface provided by the CSP **120**, the CSP **120** may also receive from consumers **110a-c** electronic bill payment requests (which include payment data) from the consumers **110a-c**. The electronic bill payment options made available to the consumers **110a-c** by their CSP **120** preferably include requests to directly debit the consumers' **110a-c** banks accounts, as well as requests to charge a payment card account.

As used in this application, a payment card may be any non-cash payment account vehicle – such as credit, debit, and prepaid cards – that may be used to provide payment for goods and/or services. These payment cards may be issued by individual card companies or by financial institutions that are members of a payment

Petitioner Askeladden LLC
Exhibit 1002 - Page 212 of 350

association (such as MasterCard® International). As used in this application, the term payment card includes not only physical payment cards, but also virtual payment cards in which the payment account information is stored in digital or electronic form, such as in a digital wallet.

The biller service provider **140** ("BSP") acts as the billing agent for the billers **150a-c** in the EBPP system. The BSP **140** receives billing data from the billers **150a-c** and transmits the billing data to the CSP **120** for presentment to the consumers **110a-c**. The BSP **140** also receives payment data from the CSP **120**, and credits the billers' **150a-c** accounts to settle the electronic bills. In an alternative body of the present invention, the acquirer **160** (discussed below in connection with **FIG. 2**) may play the role of the BSP.

The CSP **120** and BSP **140** communicate with each other by way of an exchange hub **130,** such as MasterCard's Remote Payment and Presentment System ("RPPS"), which is described in United States Patent Application Publication No. 2002/0049671A1 (incorporated herein by reference). The exchange hub **130,** routes electronic bills from the BSP **140** to the CSP **120**, and routes electronic bill payments from the CSP **120** to the BSP **140**. In accordance with the present invention, the exchange hub **130** also routes payment card bill payment requests to a payment card authorization system **160** for payment authorization, processing, and settlement in accordance with conventional payment card processing protocols.

Messages received by the exchange hub **130** are preferably parsed and its contents validated. Routing information and pertinent log data are preferably captured by the exchange hub **130**. The exchange hub **130** then rebundles the message, and delivers it to the intended recipient (either the CSP **120**, the BSP **140**, or the payment card authorization network **160**), preferably over secure lines.

FIG. 2 is a block diagram depicting the components of an EBPP system **100** and payment card authorization system **160** in accordance with an exemplary embodiment of the present invention. **FIG. 3** is a flow chart depicting the process by which the consumer **110a** (**FIG. 2**) pays an electronic bill in the EBPP system **100** in accordance with an exemplary embodiment of the present invention. Referring to both **FIG. 2** and **FIG. 3**, at step **305**, a consumer **110a** who has been presented with an electronic bill elects to pay the bill electronically using the EBPP system **100**. At step **310**, if the consumer **110a** does not wish to pay the bill using a payment card, a bill payment request is transmitted at step **315** from the consumer

Petitioner Askeladden LLC
Exhibit 1002 - Page 213 of 350

110a to the CSP **120**. The bill payment request preferably includes the biller's **150a** name, address, and account number, and a payment effective date.

At step **320**, the CSP **120** validates the bill payment request, batches it, and transmits it to the exchange hub **130**. At step **325**, the exchange hub **130** parses the data in the batched bill payment request, and captures routing information from the bill payment request. The exchange hub **130** then rebundles the bill payment message, and delivers it to the intended recipient biller's **150a** BSP **140**. At step **330**, the BSP **140** combines the bill payment messages it receives for the biller **150a**, credits the biller **150a** for net payment amounts, and finally prepares an accounts receivable file and transmits it to the biller **150a**.

Referring again to step **310** (**FIG. 3**), if the consumer **110a** elects to pay the bill electronically using a payment card, then at step **335** the consumer **110a** transmits a payment card transaction request to the CSP **120**. The payment card transaction request preferably contains all the information necessary to authorize the payment card transaction, such as card-holder name, payment card account number, and card expiration date. At step **340**, the CSP **120** transmits the payment card transaction request as a pre-notification in their batch file to the exchange hub **130**. All the details necessary for authorization processing are preferably contained in the IFX entry detail addendum record of the CSP's **120** message. At step **345**, upon receiving the batch file from the CSP **120**, the exchange hub **130** parses the payment card transaction request and generates a payment message to the biller's acquiring bank **160a** (the "acquirer") and transmits it to the acquirer **160a** in the payment card authorization system **160**.

From this point, the conventional process of payment card authorization is utilized, with the exchange hub **130** playing the same role that the merchant would play in a conventional credit card authorization process. At step **350**, the acquirer **160a** generates an 0200 Financial Request message, and transmits it to the payment card network **160b** with a destination of the consumer's **110a** payment card issuer **160c**. The issuer **160c** then, at step **355**, receives the bill payment transaction for processing, and either approves or denies the transaction, after which the issuer **160c** sends a 0210 response to the payment card network for routing back to the acquirer **160a**. At step **360**, the acquirer **160a** receives the 0210 response from the issuer, and based on that response transmits a message to the exchange hub **130** either approving or denying payment. If at step **365** the payment card transaction was

Petitioner Askeladden LLC
Exhibit 1002 - Page 214 of 350

approved, the acquirer **160a** settles with the biller **150a**, and provides remittance data to the biller **150a**. The exchange hub **130** logs at step **370** the approval message for historical purposes. The consumer **110a** eventually pays the issuer **160c** when he receives his payment card bill. If at step **365** the payment card transaction was denied, the exchange hub **130** logs at step **375** denial message and transmits a "denial" file to the CSP **120.** The CSP **120** then notifies the consumer **110a** of the denial.

Although the present invention has been described in connection with specific exemplary embodiments, it should be understood that various changes, substitutions and alterations can be made to the disclosed embodiments without departing from the spirit and scope of the invention as set forth in the appended claims.

Petitioner Askeladden LLC
Exhibit 1002 - Page 215 of 350

What is claimed is:

1. A system for paying an electronic bill in an electronic bill payment and presentment ("EBPP") system, the system comprising an exchange hub programmed to:

accept a payment card transaction request from a customer service provider ("CSP");

submit the payment card transaction request to a payment card authorization system;

receive an approval message or a denial message from the payment card authorization system in response to the submission of the payment card transaction request; and

transmit the received approval or denial message to the CSP.

2. The system of claim 1, further comprising a customer service provider programmed to submit the payment card transaction request to the exchange hub in response to an electronic request from a consumer to pay the electronic bill with a payment card.

3. The system of claim 2 wherein the payment card is a credit card.

4. The system of claim 2 wherein the payment card is a debit card.

5. The system of claim 2 wherein the payment card is a pre-paid card.

6. A method for paying an electronic bill in an electronic bill payment and presentment ("EBPP") system, comprising:

accepting at an exchange hub a payment card transaction request from a customer service provider ("CSP");

submitting the payment card transaction request to a payment card authorization system;

receiving an approval message or a denial message from the payment card authorization system in response to the submission of the payment card transaction request; and

transmitting the received approval or denial message to the CSP.

7. The method of claim 6 further comprising:

accepting at the CSP an electronic request from a consumer to pay the electronic bill with a payment card; and

Petitioner Askeladden LLC
Exhibit 1002 - Page 216 of 350

submitting the payment card transaction request to the exchange hub in response to the electronic request from the consumer to the CSP.

8. The method of claim 7 wherein the payment card is a credit card.

9. The method of claim 7 wherein the payment card is a debit card.

10. The method of claim 7 wherein the payment card is a pre-paid card.

Petitioner Askeladden LLC
Exhibit 1002 - Page 217 of 350

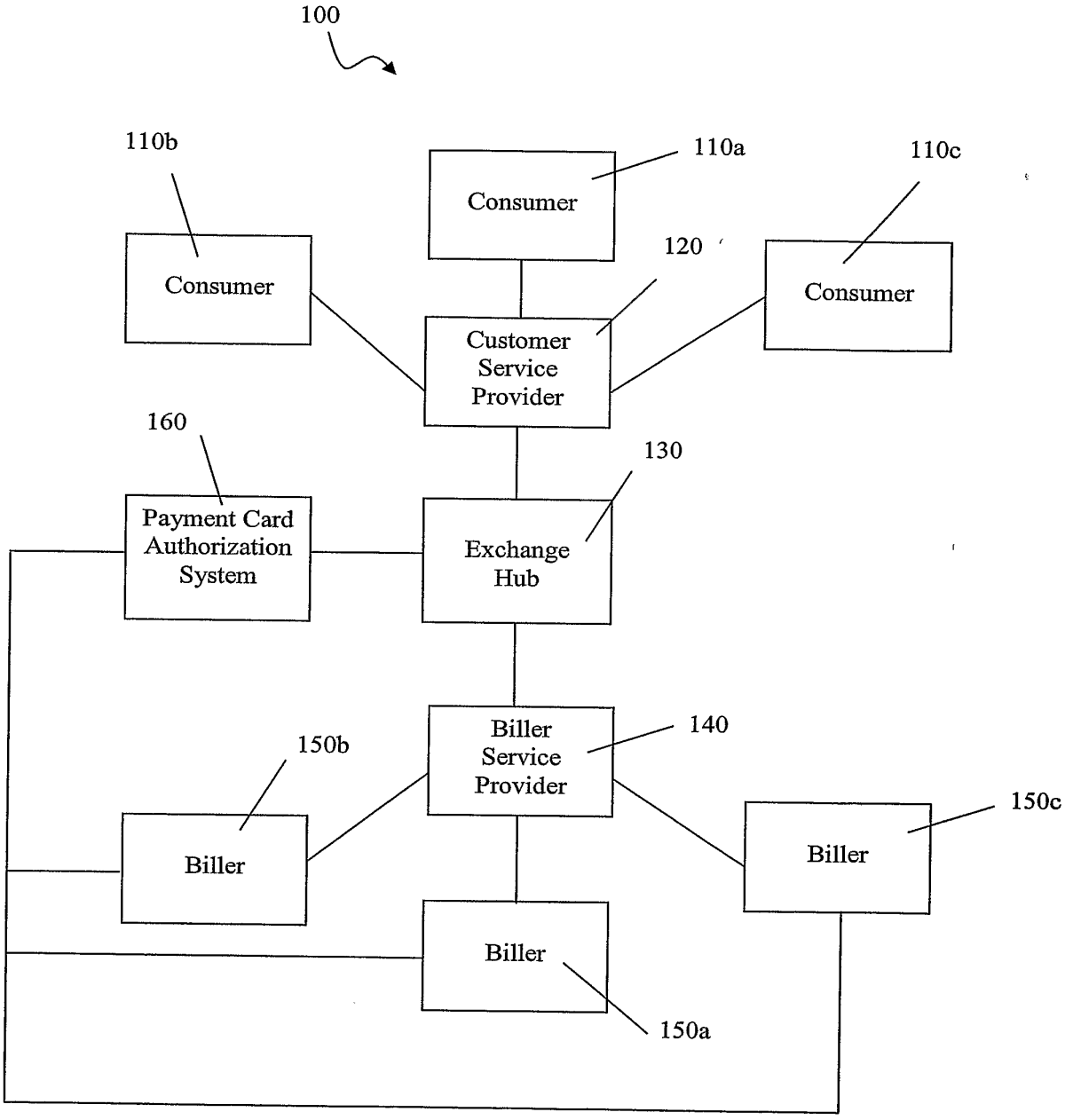

100
110b
Consumer
110a
Consumer
110c
Consumer
120
Customer Service Provider
160
Payment Card Authorization System
130
Exchange Hub
Biller Service Provider
140
150b
Biller
150c
Biller
Biller
150a

FIGURE 1

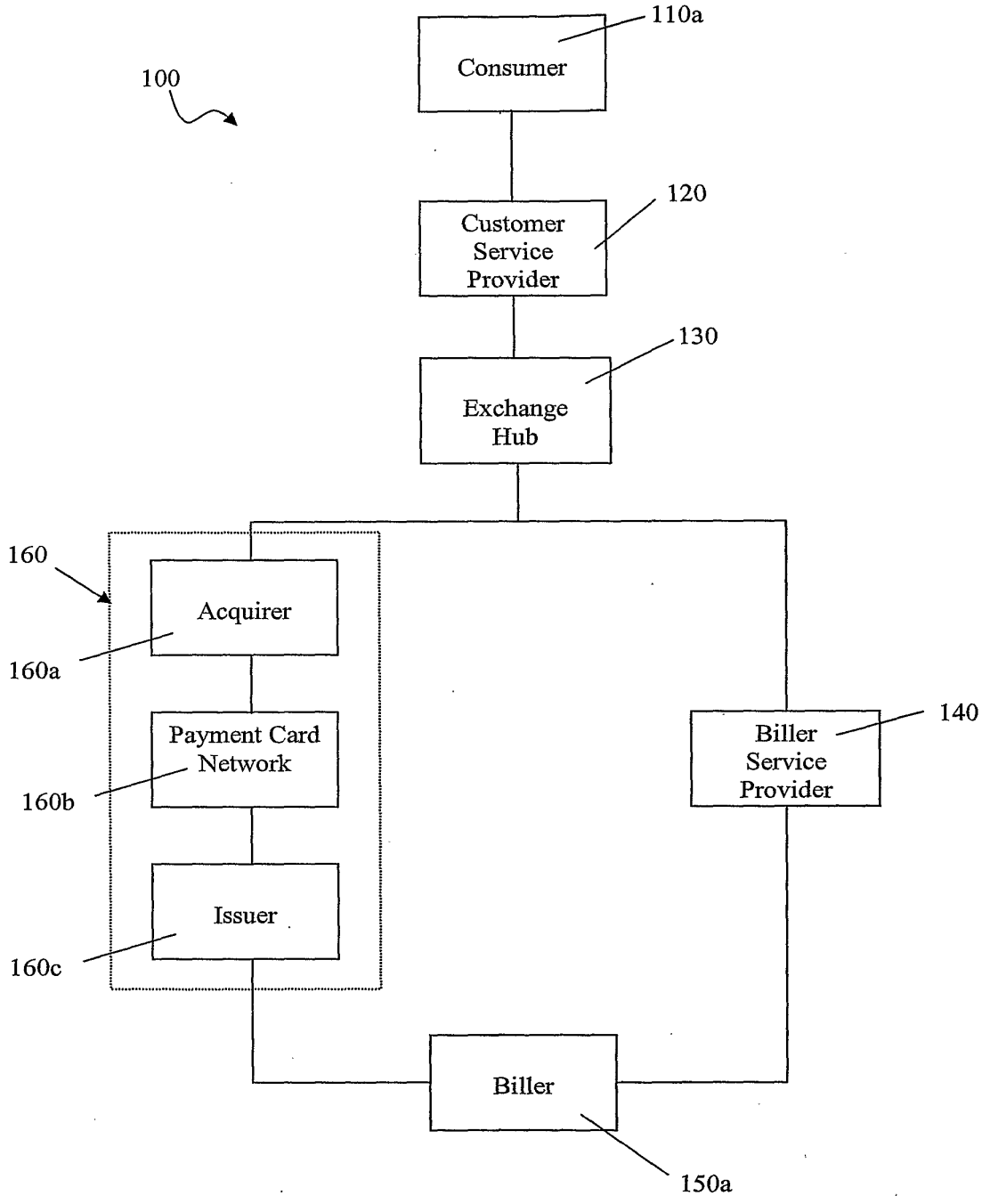

100
Consumer
110a
Customer Service Provider
120
Exchange Hub
130
160
Acquirer
160a
Payment Card Network
160b
Issuer
160c
Biller Service Provider
140
Biller
150a

FIGURE 2

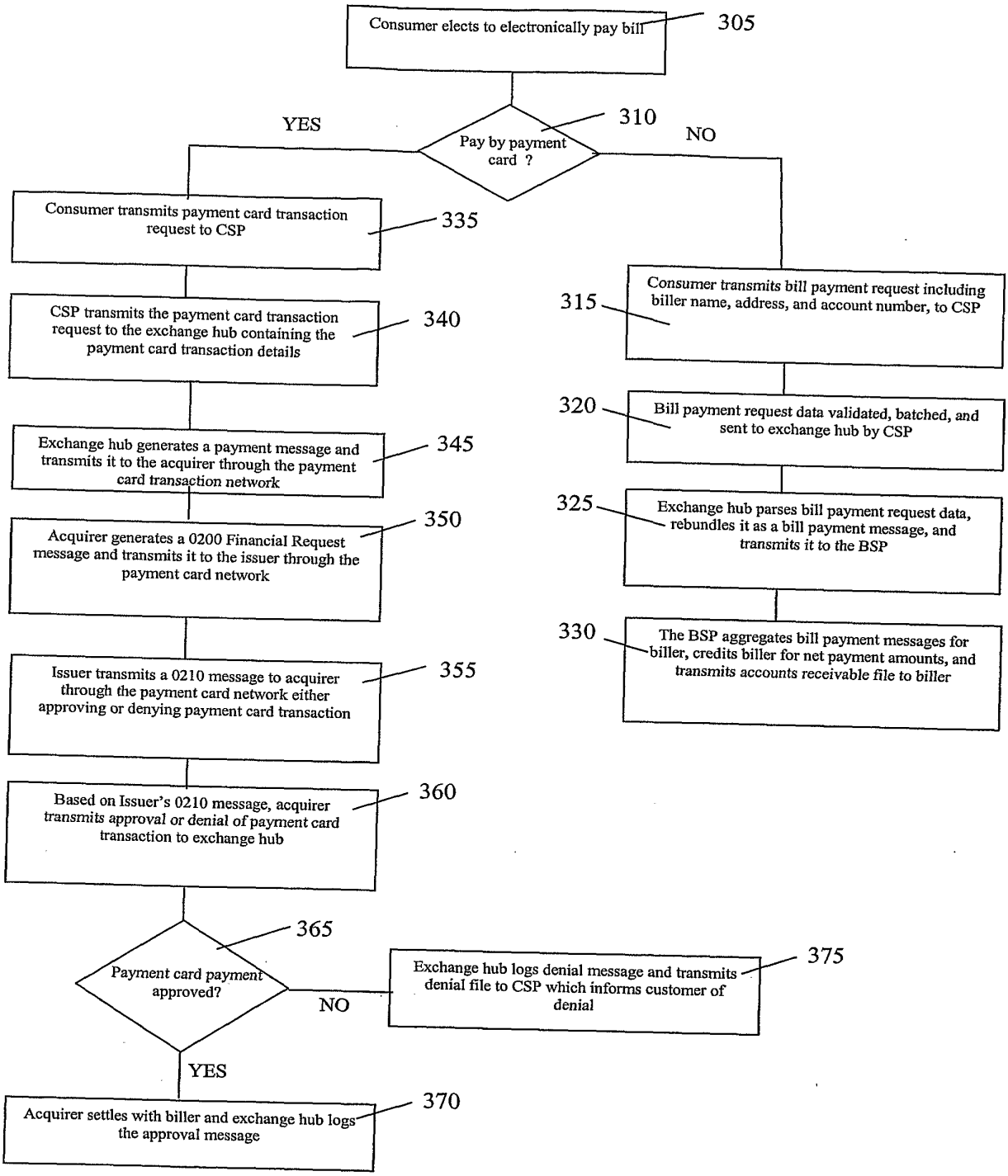


FIGURE 3

Petitioner Askeladden LLC
Exhibit 1002 - Page 220 of 350

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 067 492 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
17.01.2001 Bulletin 2001/03

(43) Date of publication A2:
10.01.2001 Bulletin 2001/02

(21) Application number: **00305196.8**

(22) Date of filing: **20.06.2000**

(51) Int. Cl.[7]: **G07F 19/00**, G06F 17/60, G07F 7/08

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **30.06.1999 US 343813**

(71) Applicant:
LUCENT TECHNOLOGIES INC.
Murray Hill, New Jersey 07974-0636 (US)

(72) Inventor: **Palmquist, John Mark**
Lilburn, Georgia 30247 (US)

(74) Representative:
Watts, Christopher Malcolm Kelway, Dr. et al
Lucent Technologies (UK) Ltd,
5 Mornington Road
Woodford Green Essex, IG8 0TU (GB)

(54) Transaction notification system and method

(57) A transaction notification system provides a transaction notification service for enabling early detection and prevention of consumer account fraud by providing a notification message to a subscriber of the service when a subscriber's account is used. Architecturally, an automated configuration of the transaction notification system includes one or more transaction devices to be monitored, a transaction processing center computer associated with a transaction processing center, and one or more transaction notification devices that are used to notify the subscriber. The transaction device 11 can be, for example, but not limited to, any of the following: a credit card point-of-sale (POS) device, a cellular telephone, an automated teller machine (ATM), a stockbroker computer, a shipment order computer, a utility company computer, a bank computer, a medical insurance company computer, *etc*. The subscriber notification device 15 can be, for example, but not limited to, any of the following: a computer having an electronic mail (e-mail) software program (e-mail computer), a pager, a facsimile machine, a computer maintaining a website on the World Wide Web (WWW) associated with the well known Internet (website computer), *etc*. The subscriber provides subscription information identifying the transaction device(s) to be monitored for usage and identifying a subscriber notification device(s) to be notified when the transaction device is used. In operation, a notification message is communicated to the subscriber notification device by the computer when the transaction device has been used, and the computer produces a bill that is sent to the subscriber for the transaction notification service.

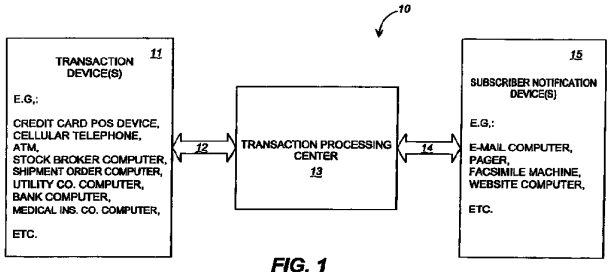


FIG. 1

EP 1 067 492 A3

Printed by Xerox (UK) Business Services
2.16.7 (HRS)/3.6

Petitioner Askeladden LLC
Exhibit 1002 - Page 221 of 350

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 30 5196

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X A	WO 98 06214 A (R.A. JOAO) 12 February 1998 (1998-02-12) * abstract; claims; figures * * page 21, line 28 - page 35, line 5 * ---	1-3,6,7 10-12, 15,16, 20,24-28	G07F19/00 G06F17/60 G07F7/08
A	EP 0 745 961 A (AT & T IPM) 4 December 1996 (1996-12-04) * abstract; claims; figures * * column 3, line 1 - column 11, line 28 * ---	1-3,6,7, 10-12, 15,16, 20,24-28	
A	US 5 530 438 A (R.S. BICKHAM) 25 June 1996 (1996-06-25) * the whole document * ---	1,10,27, 28	
A	WO 98 54943 A (T. HO KEUNG) 10 December 1998 (1998-12-10) -----		

TECHNICAL FIELDS SEARCHED (Int.Cl.7)
G07F H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	24 November 2000	David, J

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Petitioner Askeladden LLC
Exhibit 1002 - Page 222 of 350

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 30 5196

This annex lists the patent family membersrelating to the patent documents cited in the above–mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

24-11-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9806214 A	12-02-1998	US 5878337 A	02-03-1999
		US 5903830 A	11-05-1999
		AU 3977597 A	25-02-1998
		US 6047270 A	04-04-2000
EP 0745961 A	04-12-1996	US 5708422 A	13-01-1998
		CA 2176163 A,C	01-12-1996
		JP 8339407 A	24-12-1996
US 5530438 A	25-06-1996	NONE	
WO 9854943 A	10-12-1998	AU 8019698 A	21-12-1998

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Petitioner Askeladden LLC
Exhibit 1002 - Page 223 of 350

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 287 793 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
23.02.2011 Bulletin 2011/08

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

(21) Application number: **10184725.9**

(22) Date of filing: **05.03.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR

(30) Priority: **05.03.2002 US 93002**

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
03716368.0 / 1 485 846

(71) Applicants:
- **VISA U.S.A. Inc.**
  San Francisco, CA 94105 (US)
- **VISA INTERNATIONAL SERVICE ASSOCIATION**
  Foster City, CA 94404 (US)

(72) Inventors:
- **Kemper, Lynn**
  San Carlos, CA 94070 (US)
- **Vij, Akshey, Shawn**
  San Ramon, CA 94583 (US)
- **O'Connell, Robin**
  San Rafael, CA 94901 (US)

(74) Representative: **Eisenführ, Speiser & Partner**
Johannes-Brahms-Platz 1
20355 Hamburg (DE)

Remarks:
This application was filed on 30-09-2010 as a divisional application to the application mentioned under INID code 62.

(54) System for personal authorization control for card transactions

(57) An authorization system (10) allows for cardholder-provided parameters to a personal authorization subsystem (10). 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 (18) and a network operator (16), 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.

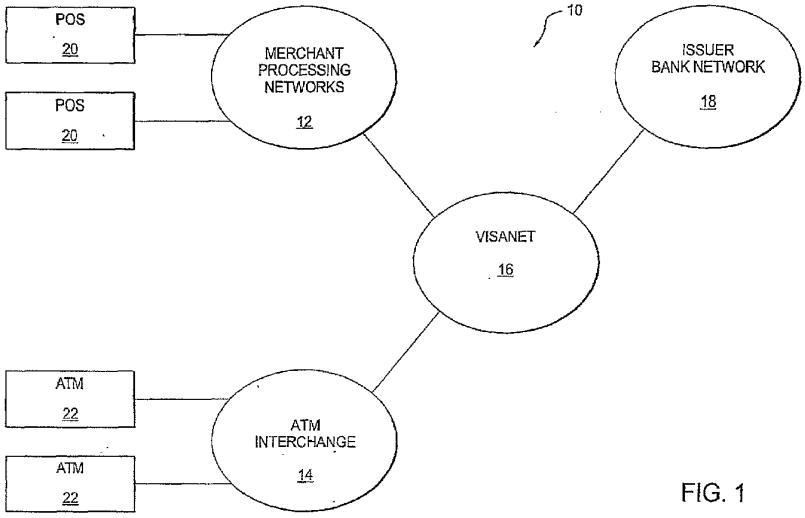


FIG. 1

EP 2 287 793 A1

Printed by Jouve, 75001 PARIS (FR)

Petitioner Askeladden LLC
Exhibit 1002 - Page 224 of 350

Description

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 jewellery might prompt the authorization system to deny the transaction as a suspect activity even if ultimately the cardholder is legitimately purchasing jewellery. 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

[0009] Fig. 1 is a block diagram of a transaction system wherein the present invention might be used.

[0010] Fig. 2 is a more detailed block diagram illustrating aspects of an authorization subprocessor and a cardholder's interaction with the subprocessor.

[0011] Fig. 3 is a flowchart illustrating a process of authorization control.

[0012] Figs. 4 (a) - (e) illustrate aspects of a user interface usable to set cardholder authorization parameters.

DETAILED DESCRIPTION OF THE INVENTION

[0013] 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

[0014] (ATM) interchange 14 coupled to a transaction network 16, such as the VISASNET network, which is in

Petitioner Askeladden LLC
Exhibit 1002 - Page 225 of 350

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.

[0015] 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.

[0016] 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.

[0017] 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.

[0018] In a typical operation, illustrated in Fig. 3, the cardholder (i.e., one of those ultimately responsible for nonfraudulent 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.

[0019] 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.

[0020] The authorization subprocessor is described above as acting to approve or deny a transaction. hi 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

[0021] 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:

[0022] Transaction Type

- Deny cash advances, but allow purchases.

[0023] Transaction Amount

- Allow a transaction below a set limit
- Allow transaction if total transactions would remain below a limit (personalized credit limit)
- Allow transaction if total transactions in a set time period are below a limit
- Daily Limits

Petitioner Askeladden LLC
Exhibit 1002 - Page 226 of 350

- Limit on number of transactions

[0024] Transaction Details

- 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)
- Allow transaction only during set times of the week (e. g. , movie purchases not allowed during the week)
- Allow offline transactions, but not online (telephone, Internet, etc.) transactions
- Allow online transactions, but only from prespecified IP addresses
- Allow transactions based on geographic location (e.g., block purchases outside U. S.)
- Allow transactions based on the merchant category type (e. g. , restaurants and hotels but not retail stores)

[0025] Other Limits

- Preauthorization for one-time transactions
- Recurring Payment Authorization
- Varying controls from card carrier to card carrier
- 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.)

[0026] 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.

[0027] 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

[0028] 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

[0029] 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.

[0030] 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.

[0031] 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.

[0032] 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 cardhold-

Petitioner Askeladden LLC
Exhibit 1002 - Page 227 of 350

er (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.

[0033] 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.

[0034] 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.

Claims

1. A card transaction system (10), wherein a cardholder effects transactions in the card transaction system, the system comprising:

   a Web server (34) for receiving authorization parameters from the cardholder through a Web interface accessible from a web page;
   an authorization parameters table (32) for storing the authorization parameters received through the Web server;
   a transaction network (16) coupled to merchant terminals (20, 22) for receiving requests for authorization from merchants, the transaction network receiving requests for authorization of transactions using cards issued by a plurality of issuer financial institutions;
   an authorization subprocessor (30) configured to retrieve the authorization parameters associated with the cardholder from the authorization parameter table (32), the authorization subprocessor being further operable to make an authorization determination based on the authorization parameters, the transaction network (16) using said authorization determination to determine whether to deny the authorization request, the transaction network further operable to send the authorization request to an authorization server at a issuer financial institution for an other authorization determination based on criteria set by the issuer financial institution that issued the card to the cardholder, the transaction network denying the transaction based on one of said two authorization determination.

2. The system of claim 1 wherein the card is one of a credit card and a debit card.

3. The system of any of the preceding claims wherein the authorization parameter comprises a geographic limitation on authorized transactions.

4. The system of any of the preceding claims wherein the authorization parameter comprises a per merchant category transaction limit.

5. The system of any of the preceding claims wherein the authorization parameter comprises an instant cutoff limit, the instant cutoff limit denying authorization for all transactions.

6. The system of any of the preceding claims wherein the web interface is in the form of a calendar view.

7. The system of any of the preceding claims wherein the authorization subprocessor sends a transaction notification message to the cardholder.

8. A method of using the system of claim 1 for authorizing use of a card for a transaction, the card being associated with a cardholder account, the method comprising:

   generating a Web interface accessible from a web page that allows a cardholder to input at least one authorization parameter;
   receiving through the Web interface the at least one authorization parameter and storing the at least one authorization parameter in an authorization parameters table;
   receiving a request for authorization to use the card for the transaction, the request received over a transaction network that receives requests for authorization of transactions for cards issued by a plurality of issuer financial institutions;
   retrieving the at least one authorization parameter from the authorization parameter table by an authorization subprocessor;
   making an authorization determination with the authorization subprocessor based on the at least one authorization parameter;
   receiving an other authorization determination at the transaction network from a issuer financial

Petitioner Askeladden LLC
Exhibit 1002 - Page 228 of 350

institution, said other authorization determination using an authorization server to authorize the transaction based on criteria set by the issuer financial institution that issued the card to the cardholder; and
denying the transaction if any of the two authorization determinations indicate the transaction is not authorized.

9. The method of claim 8 wherein the card is one of a credit card and a debit card.

10. The method of any of claims 8 and 9 wherein the authorization parameter comprises a geographic limitation on authorized transactions.

11. The method of any of claims 8-10, wherein the geographic limitation includes denying international transactions.

12. The method of any of claims 8-11 wherein the authorization parameter comprises a per merchant category transaction limit.

13. The method of any of claims 8-12 wherein the authorization parameter comprises an instant cutoff limit, the instant cutoff limit denying authorization for all transactions.

14. The method of any of claims 8-13 wherein the web interface is in the form of a calendar view.

15. The method of any of claims 8-14 wherein the authorization subprocessor sends a transaction notification message to the cardholder.

Petitioner Askeladden LLC
Exhibit 1002 - Page 229 of 350

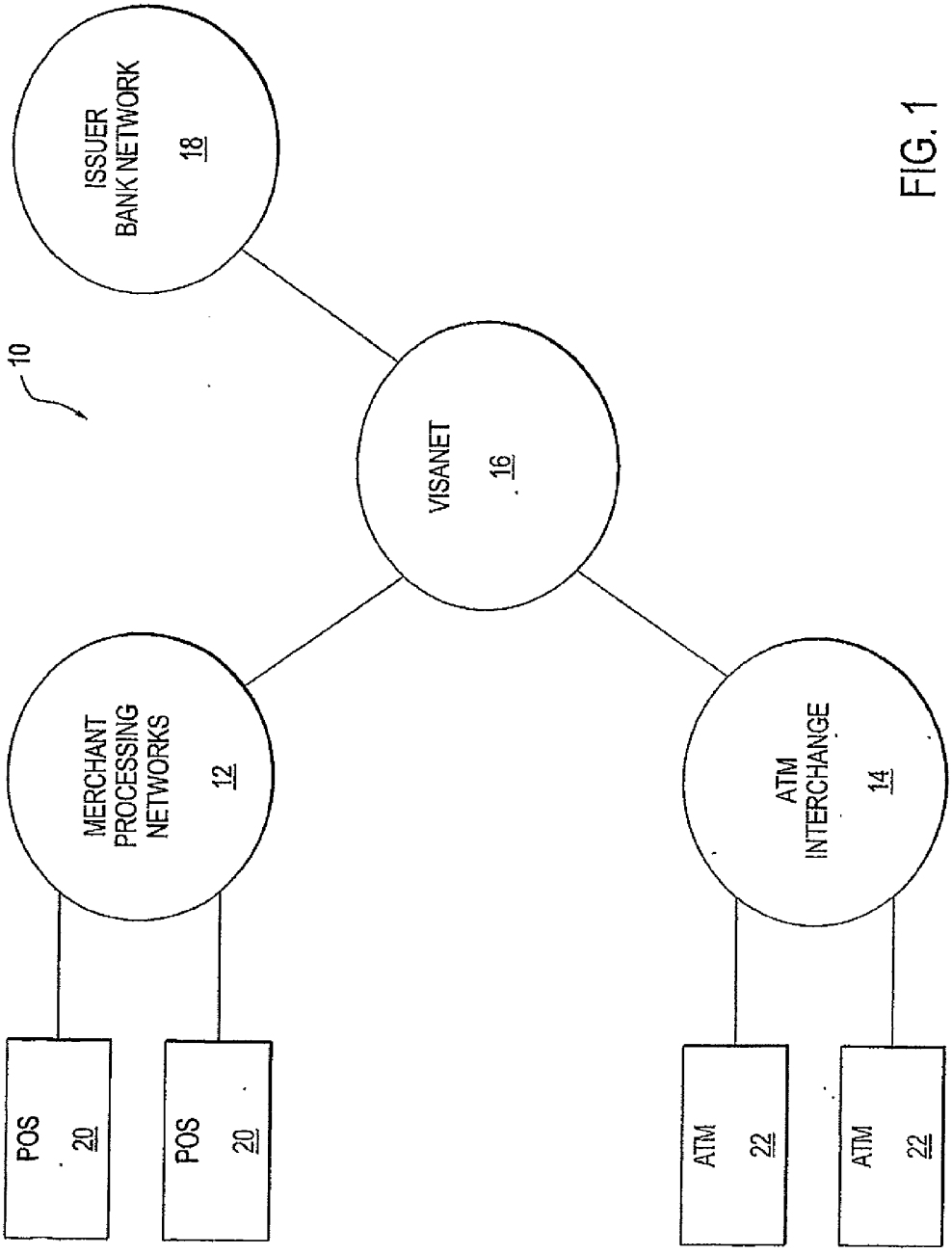


FIG. 1

Petitioner Askeladden LLC
Exhibit 1002 - Page 230 of 350

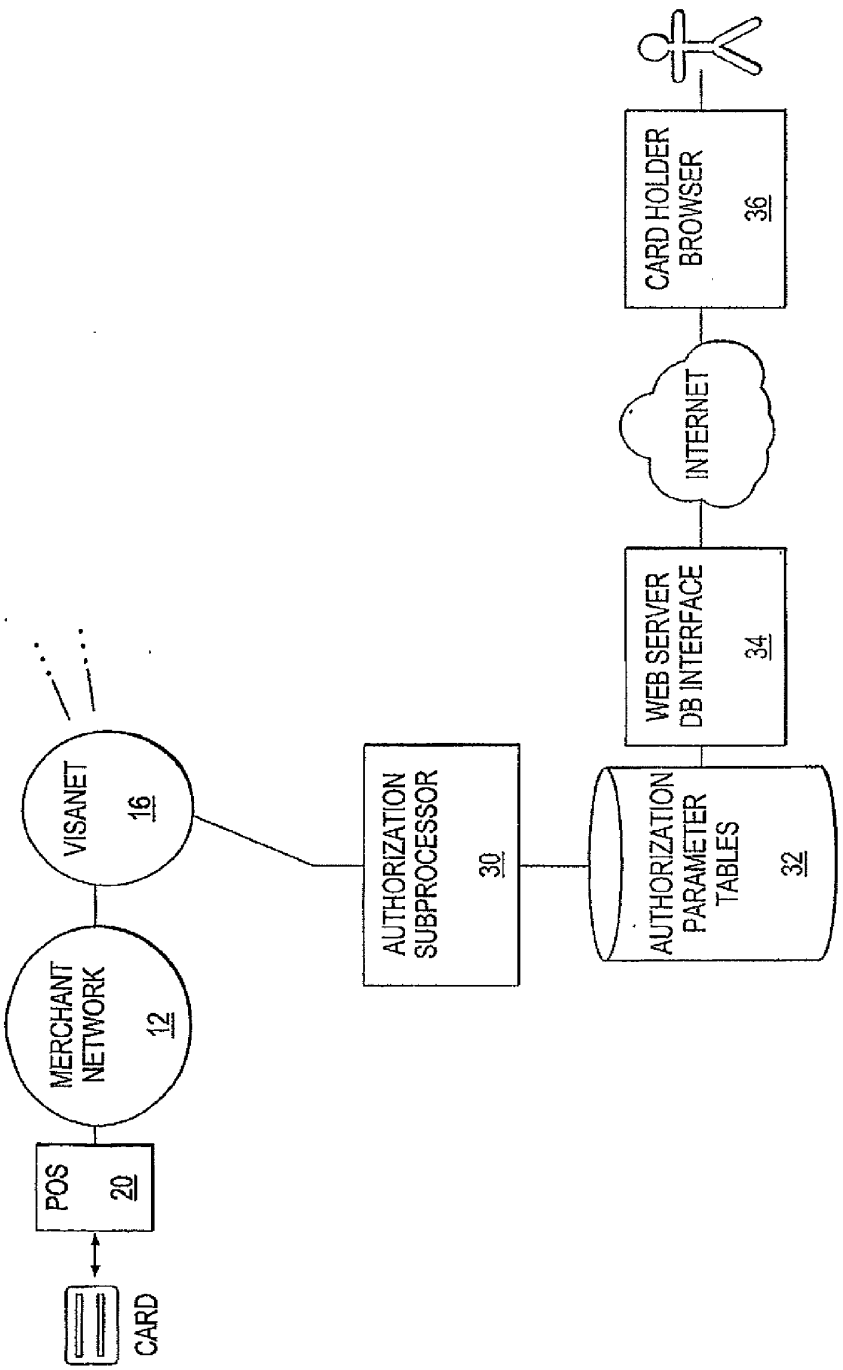


FIG. 2

Petitioner Askeladden LLC
Exhibit 1002 - Page 231 of 350

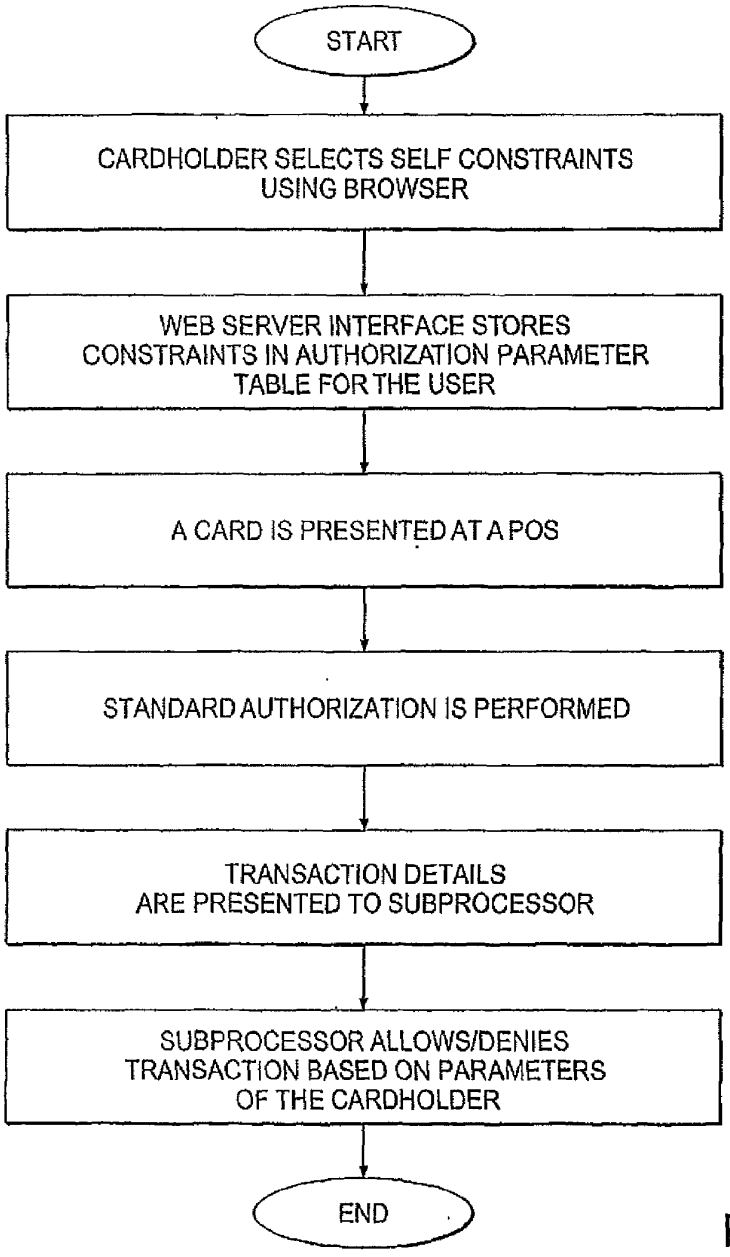


FIG. 3

Petitioner Askeladden LLC
Exhibit 1002 - Page 232 of 350

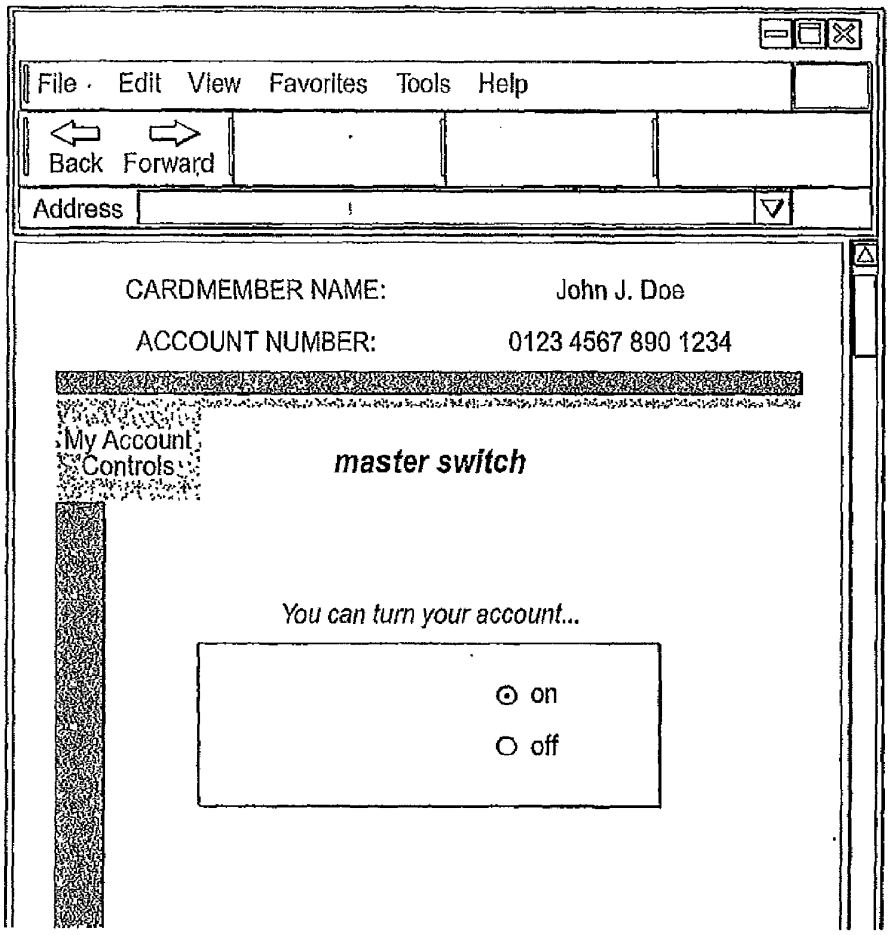


FIG. 4(a)

Petitioner Askeladden LLC
Exhibit 1002 - Page 233 of 350

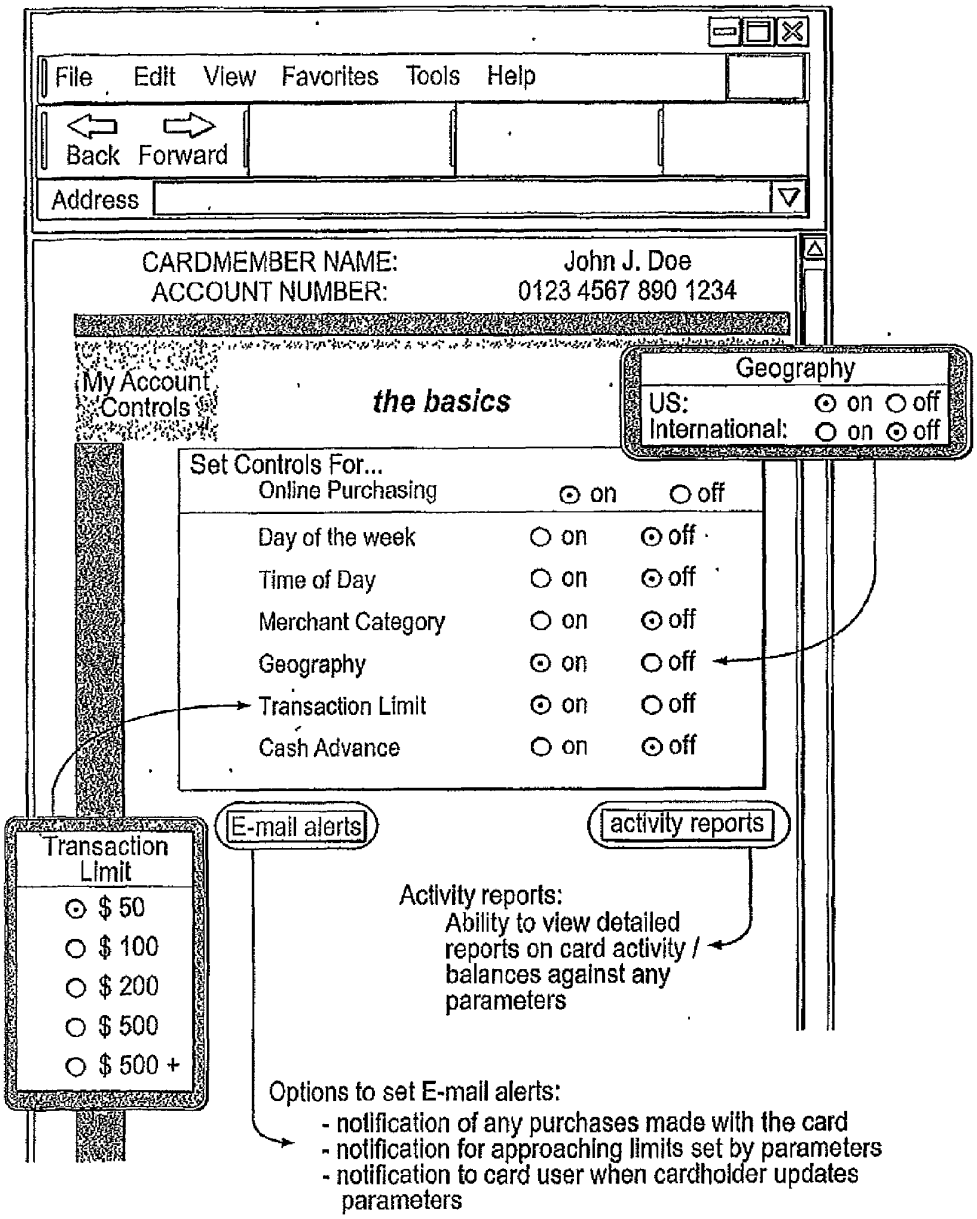


FIG. 4(b)

Petitioner Askeladden LLC
Exhibit 1002 - Page 234 of 350

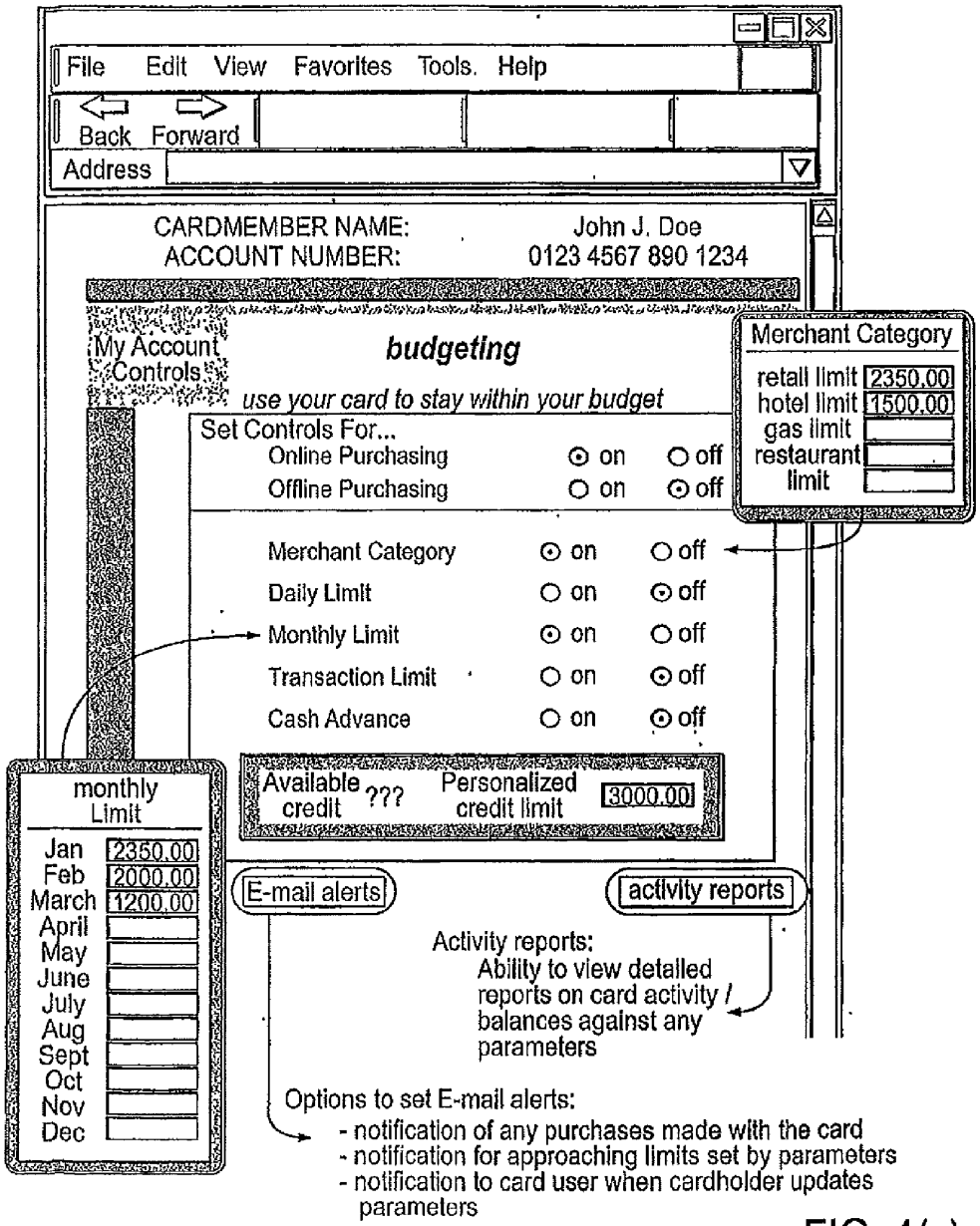


FIG. 4(c)

Petitioner Askeladden LLC
Exhibit 1002 - Page 235 of 350

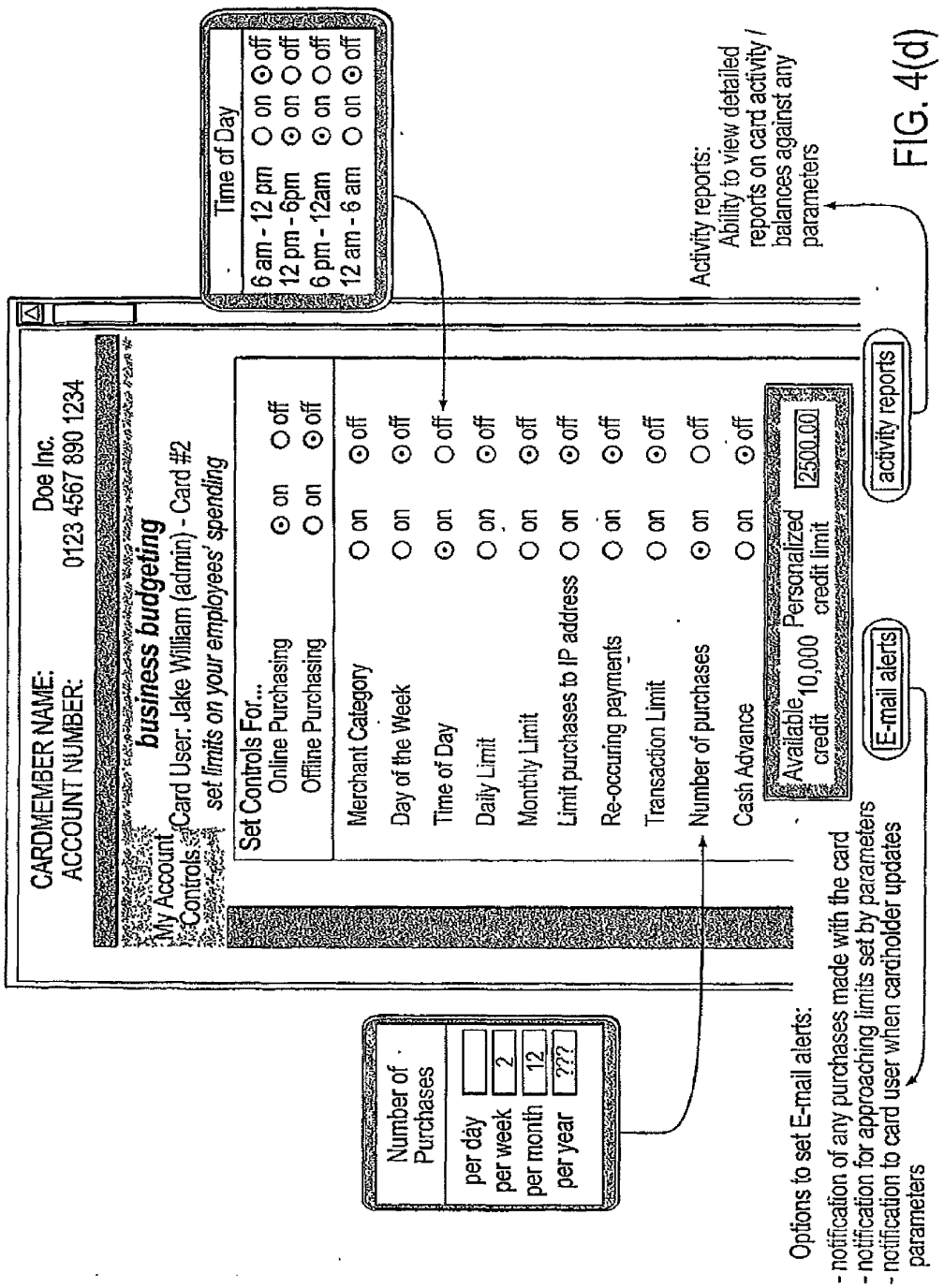


FIG. 4(d)

Petitioner Askeladden LLC
Exhibit 1002 - Page 236 of 350

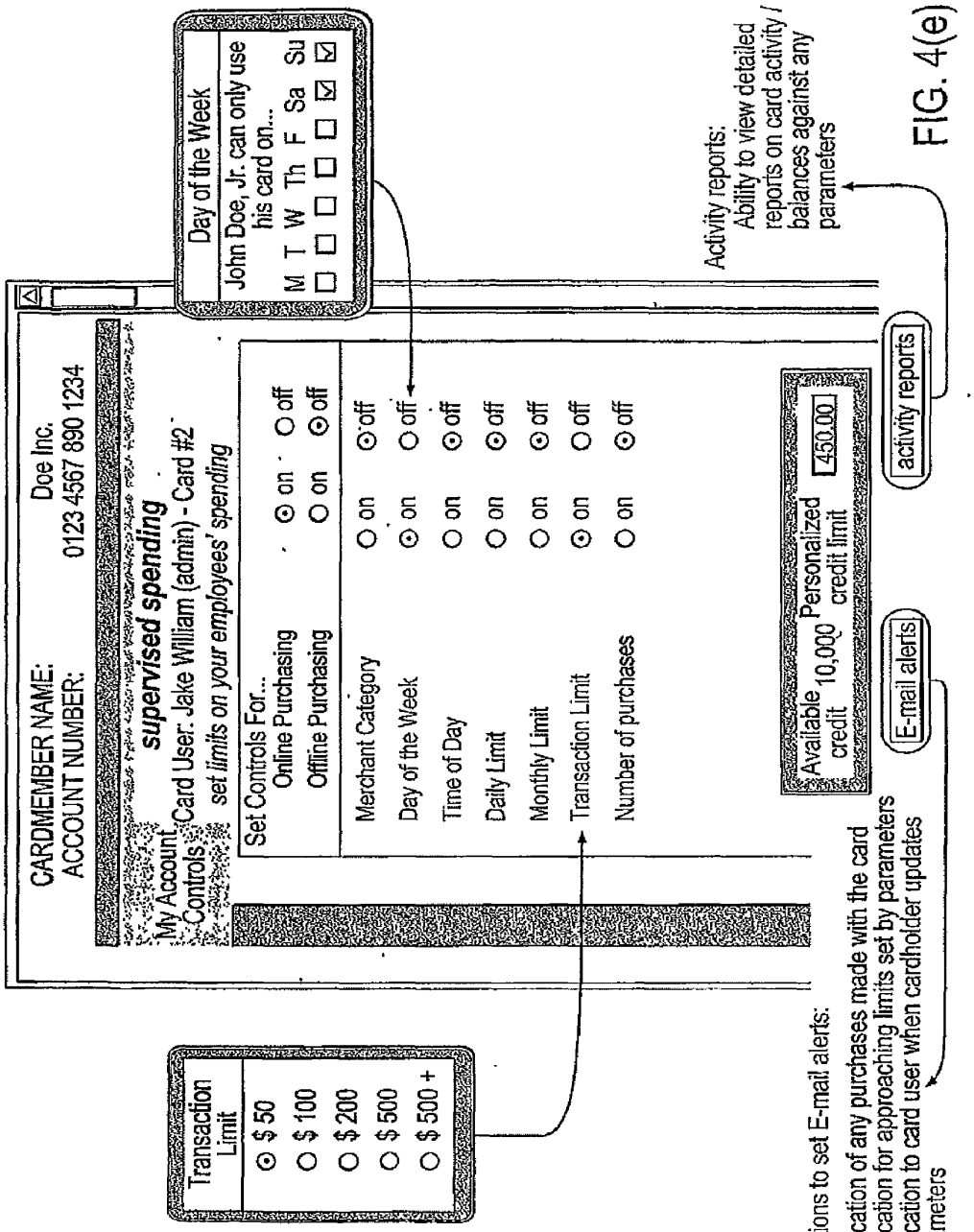


FIG. 4(e)

Petitioner Askeladden LLC
Exhibit 1002 - Page 237 of 350

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 10 18 4725

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 5 655 007 A (MCALLISTER ET AL) 5 August 1997 (1997-08-05) * column 12, line 40 - line 54 * * column 13, line 19 - column 17, line 16 * * column 18, line 25 - line 39 * * figure 5 * * claims 1-8 *	1-15	INV. G06Q20/00
X	WO 00/46769 A1 (TOMAN, PAUL, M; KOEHLER, STEVEN, M) 10 August 2000 (2000-08-10) * page 3, line 7 - line 20 * * page 5, line 30 - page 8, line 33 * * page 11, line 5 - line 11 * * page 11, line 25 - page 12, line 23 *	1-15	
X	EP 0 745 961 A2 (AT&T IPM CORP; AT&T CORP) 4 December 1996 (1996-12-04) * column 5, line 28 - column 9, line 8 * * column 13, line 45 - column 16, line 1 * * figure 1 *	1-15	TECHNICAL FIELDS SEARCHED (IPC)
X,P	WO 03/001866 A1 (SNAPCOUNT LIMITED; DAVANAGH, STEPHEN; CLARKE, CONOR; GUILFOYLE, KIERON) 9 January 2003 (2003-01-09) * page 8, line 10 - page 10, line 14 * * page 15, line 24 - page 16, line 2 * * page 21, line 5 - line 25 * * page 27, line 14 - page 28, line 3 * * figures 1-3 *	1-15	G07F
A	EP 0 540 234 B1 (AMERICAN TELEPHONE & TELEGRAPH [US] AMERICAN TELEPHONE & TELEGRAPH [DE]) 4 March 1998 (1998-03-04) * col. 3, line 58 - col. 4, line 34; column 3, line 58 - column 4, line 34 * * figure 2 *	1-15	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	16 December 2010	Rachkov, Vassil

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Petitioner Askeladden LLC
Exhibit 1002 - Page 238 of 350

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 10 18 4725

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

16-12-2010

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5655007 A	05-08-1997	US 5513250 A	30-04-1996
WO 0046769 A1	10-08-2000	AU 3355900 A	25-08-2000
EP 0745961 A2	04-12-1996	CA 2176163 A1	01-12-1996
		DE 69617097 D1	03-01-2002
		DE 69617097 T2	20-06-2002
		JP 8339407 A	24-12-1996
		US 5708422 A	13-01-1998
WO 03001866 A1	09-01-2003	EP 1402486 A1	31-03-2004
		IE 20020534 A1	30-12-2002
		US 2010017328 A1	21-01-2010
		US 2007198411 A1	23-08-2007
		US 2004128243 A1	01-07-2004
EP 0540234 B1	04-03-1998	CA 2076433 A1	01-05-1993
		DE 69224585 D1	09-04-1998
		DE 69224585 T2	10-09-1998
		EP 0540234 A2	05-05-1993
		JP 3245834 B2	15-01-2002
		JP 6290195 A	18-10-1994
		US 5450477 A	12-09-1995

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Petitioner Askeladden LLC
Exhibit 1002 - Page 239 of 350

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 June 2003 (05.06.2003)

PCT

(10) International Publication Number
WO 03/046778 A2

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/EP02/12851

(22) International Filing Date:
15 November 2002 (15.11.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/996,576 30 November 2001 (30.11.2001) US

(71) Applicant: **ACTIVCARD** [FR/FR]; 24-28 avenue du Général de Gaulle, F-92156 Suresnes Cedex (FR).

(72) Inventors: **AUDEBERT, Yves**; 237 Forrester Road, Los Gatos, CA 95032 (US). **BECQUART, Jérôme**; 618 Barcelona Drive, Fremont, CA 94536 (US).

(74) Agent: **CABINET JP COLAS**; 37, avenue Franklin D. Roosevelt, F-75008 Paris (FR).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

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

Published:
— *with declaration under Article 17(2)(a); without abstract; title not checked by the International Searching Authority*

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.

WO 03/046778 A2

(54) Title: FINANCIAL RISK MANAGEMENT SYSTEM AND METHOD

(57) Abstract:

Petitioner Askeladden LLC
Exhibit 1002 - Page 240 of 350

Financial Risk Management System and Method

FIELD OF INVENTION

The present invention relates to a data processing method and system for reducing fraudulent financial transactions and provides the ability to authenticate transactions exceeding specified limits.

BACKGROUND OF INVENTION

Consumers are largely reliant on the financial services industry to validate financial transactions such as credit card charges. However, a fraudulently obtained credit card may be used before the financial services industry and/or the card's owner becomes aware that an unauthorized entity is charging to the credit card. While the financial services industry does have elaborate fraud prevention mechanisms in place, fraud detection usually occurs after one or more initially successful fraudulent transactions. There currently is no mechanism available which alerts the consumer to a potentially fraudulent transaction involving a credit card.

In addition, spending limits are determined by the consumer's credit rating rather than by personal choices made by the consumer. Some card issuers have introduced low spending limit credit cards for use by adolescents. The purported intent of these low spending limits cards is to develop responsible spending habits by early exposure to using credit cards. The basic premise being that exceeding the maximum spending limit prevents further use.

Online financial management systems are known in the art. For example, US patent 6,131,115 by Anderson, et al. describes an online system for viewing a multitude of customer accounts available from a number of service providers. No provisions are available for the customer to receive transaction notifications or to set transactions limits.

In another approach, US patent 6,285,991 by Powar describes an interactive bill payment system, which allows a customer to pay bills online to a variety of service providers. Again, no provisions are available for the customer to receive transaction notifications or to set transactions limits.

In another approach, US patent 6,230,145 by Verderamo, et al., describes a method of providing financial transaction information to a merchant. The system

Petitioner Askeladden LLC
Exhibit 1002 - Page 241 of 350

described is oriented for use by a merchant for consolidation of a large number of financial transactions into a statement available over the Internet. Limited interactive capabilities are included, however, the patent does not allow the customer to receive transaction notifications or to set transactions limits and is intended for a merchant rather than a consumer.

In yet another approach, US patent 5,590,197 by Chen, et al. describes an online bill payment system, which incorporates the use of an electronic purse or wallet for conducting E-commerce transactions. Again, no provisions are available for the customer to receive transaction notifications, set transaction limits or to authorize transactions exceeding a predetermined amount.

Thus it is apparent that a system which allows a customer to set transaction limits and provides notifications of transactions, allows authorization of transaction and performs account suspensions when transactions exceed authorized limits is highly desirable.

BRIEF SUMMARY OF THE INVENTION

This invention describes a web-based system that allows a customer to enter preset spending limits and includes telecommunications information that provides notification to the customer when the preset spending limits are being exceeded. A second feature of this invention provides the ability to authorize transactions, which exceed the preset spending limits thus providing even greater control of a consumer's credit transactions. A third feature of this invention provides account suspension if spending exceeds, preset spending limits either in a single transaction or cumulatively over a pre-established period of time.

Robust authentication procedures should be established to ensure that only the customer is permitted access to his or her account. Common procedures including entry of an account number, user name and password, PIN (Personal Identity Number) entry, authentication token, biometric entry, and digital certificate exchange should be sufficient for accessing the customer's account and entering the notification and transaction information.

The transaction notification methods may include sending an email to an entered email address, calling a designated phone number (either POTS or cellular), interactive television (set top box) or calling a pager number. A further enhancement includes the ability to approve pending transactions; for example, an SMS (Short

Petitioner Askeladden LLC
Exhibit 1002 - Page 242 of 350

Messsage Service) message may request that a user formally authenticate the transaction using pre-established cryptographic methods etc. Other methods may request the user to call a telephone number that prompts the user for a PIN or other alphanumeric sequence in order to authorize the transaction.

Account suspension features allow the customer's account to be blocked from further use if pre-established transaction limits are exceeded. This feature includes sending notification of the account's suspended status to the customer using one or more of the notification methods described above. The suspended account requires the customer to contact his or her financial institution in order to reactivate the account.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the present invention may be accomplished by referring to the following Detailed Description and Claims, when viewed in conjunction with the following drawings:

FIG. 1 is a block diagram providing an overview of the notifications and authorization systems available for implementing the invention.

FIG. 2 is a flow chart for establishing the cardholder's preferences.

FIG. 3 depicts a simulated web data entry screen for establishing the cardholder's preferences.

FIG. 4 is a flow chart for evaluating transactions by a financial institution.

DETAILED DESCRIPTION OF THE INVENTION

This patent describes a new procedure, which allows a customer to approve financial service transactions based on preset spending limits. When a single or cumulative number of transactions exceed a preset limit, notifications are sent to one or more devices prearranged by the customer. This allows a customer to monitor expenditures and control spending habits. Another benefit of this patent is the ability to detect fraudulent transactions. Since the customer presumably is aware of the usage of his or her account, unauthorized transactions, which exceed the pre-established transaction limits, will alert the customer to fraudulent transactions that are occurring generally before the financial institution becomes aware that the customer's account has been compromised.

Referring to FIG.1, a generalized diagram is shown which includes the various network interactions and notification devices available. In FIG.1, a financial services server 100 is interconnected with a plurality of telecommunications networks including the public telephone system network 110, the Internet 120, wireless network 130 and cable television network 140.

A customer has the option of including transaction notification devices such as a normal telephone 145, email messages to a web enabled computer 155, cellular telephone 165, pager 175, personal data assistant (PDA) 185 or television set 195. Point of sales (POS) terminals 20, 40, 60, 80 may be connected on one or more of the plurality of networks, which perform financial transactions with the financial services server 100.

Referring to FIG. 2, a current customer at a local client initiates 200 a connection with a financial services server. Once a connection is established 210 between the client (customer) and the financial services server, the customer is authenticated 220 using a preferably robust authentication mechanism: examples include entry of an account number, user name and password, PIN entry, authentication token, biometric entry, and digital certificate exchange. Robust authentication methods are well known in the art and will not be described further. In the preferred embodiment of the invention, secure communications are maintained between the client and the financial services server. High-level encryption methods such as SSL, IPSEC, etc., using at least 128-bit encryption should be employed.

Once the customer is properly authenticated 220, the customer is allowed access to the data input screen which allows entry of the customer's preferences related to notification methods 230, transaction limits 240, authorization limits 250 and account suspension limits 260. After the customer has completed entry of the information processing is ended 270.

Referring to FIG. 3, an example screen which illustrates the data entry blocks for the various notification methods, transaction limits, authorization limits and account suspension limits. Optionally, the customer has the ability to utilize the entered information for all accounts linked to his or her current account. The customer input screen may be programmed in any common language such as HTML, XML, XHTML, etc.

Notification methods includes the ability to send email to a specified email address, call a cellular telephone number, call a work phone number, call a digital

Petitioner Askeladden LLC
Exhibit 1002 - Page 244 of 350

pager, call a home number or call an alternative number. The notification methods that allow return of a response may also be used to perform authorizations.

The notification transaction limits includes the ability to specify single transaction and/or cumulative transaction levels which when exceeded will cause notifications to be issued using the customer notification method(s) selected above. Cumulative transaction limits may be specified over an appropriate period of time including transactions occurring daily, weekly, monthly, per billing period or a customer specified period (e.g. quarterly.)

The authentication transaction limits includes the ability to specify single transaction and/or cumulative transaction levels which when exceeded will require authorization to be received following issuance of a notification message as described above. The authorization may include entry of a PIN, biometric result, and user name/password, etc. which is returned to the customer notification method(s) selected above. Again, cumulative transaction limits may be specified over an appropriate period of time including transactions occurring daily, weekly, monthly, per billing period or a customer specified period (e.g. quarterly.)

The account suspension transaction limits includes the ability to specify single transaction and/or cumulative transaction levels which when exceeded will suspend the customer's account from receiving any further financial transactions until reset by the financial institution in accordance with their internal policies. As before, cumulative transaction limits may be specified over an appropriate period of time including transactions occurring daily, weekly, monthly, per billing period or a customer specified period (e.g. quarterly.)

Referring to FIG. 4, a flow chart depicts the financial institution's processing of financial transactions received from one or more point of sale terminals. Processing is initiated 400 by receipt of a financial transaction 405 associated with a customer's account number by the financial services server. The transaction amount is compared with the preset notification limits. If the transaction amount is below the preset notification limits, the transaction is processed 430 without performing notifications and processing ends 455 for this transaction.

If the transaction amount is greater than the preset notifications limits, the transaction is compared with the authorization limits 415. If the transaction amount is below the preset authorization limits, notifications are issued 435, the transaction is processed 430 and processing ends 455 for this transaction.

Petitioner Askeladden LLC
Exhibit 1002 - Page 245 of 350

If the transaction amount is greater than the preset authorization limits, the transaction is compared with the account suspension limits 420. If the transaction amount is below the preset account suspension limits, authorization 440 is required using the preset notification methods. If a proper authorization is received 445, the transaction is processed 430 and processing ends 455 for this transaction. If no authorization or an invalid authorization is received, a warning message is sent 450 to the preset notification methods and processing ends 455 for this transaction.

Lastly, if the transaction amount is greater than the preset account suspension limits, the customer's account is blocked 425 from further use, a warning message is sent 450 using the preset notification methods and processing ends 455 for this transaction.

The foregoing described embodiments of the invention are provided as illustrations and descriptions. They are not intended to limit the invention to precise form described. In particular, it is contemplated that functional implementation of the invention described herein may be implemented equivalently in hardware, software, firmware, and/or other available functional components or building blocks. Other variations and embodiments are possible in light of above teachings, and it is not intended that this Detailed Description limit the scope of invention, but rather by the Claims following herein.

CLAIMS

What is claimed:

1. A network enabled online transaction risk management system comprising;

at least one financial services server (100) for processing financial transaction requests received over said network for at least one customer account wherein preferences for said at least one customer account are remotely configurable over said network;

at least one client in processing communications with said at least one financial services server (100) over said network including means for remote configuration (230, 240, 250, 260) of said at least one customer account using one or more customer preferences;

at least one point of sales terminal in processing communications with said at least one financial services server (100) including means for performing financial transactions with said financial services server.

2. The system according to claim 1 wherein said one or more customer preferences includes notification methods (230) and said system comprises notification means for performing said notification methods.

3. The system according to claim 2 wherein said notification methods further includes authorization methods and said system further comprises authorization means for performing said authorization methods.

4. The system according to claim 3 wherein said one or more customer preferences includes transaction limits (240).

5. The system according to claim 4 wherein said one or more customer preferences includes authorization limits (250).

6. The system according to claim 5 wherein said one or more customer preferences includes account suspension limits (260).

7. The system according to claim 6 wherein said one or more customer preferences includes single transactions.

8. The system according to claim 7 wherein said one or more customer preferences includes cumulative transactions.

9. The system according to claim 8 wherein said one or more customer preferences includes an applicable time period.

10. The system according to claim 1 wherein said at least one financial services server authenticates (220) said at least one customer before allowing said at least one customer access to said at least one customer account.

11. The system according to claim 1 wherein said communication is performed using a secure messaging protocol.

12. The system according to claim 1 wherein said network includes the Internet (120).

13. The system according to claim 1 wherein said network includes a public telephone service network (110).

14. The system according to claim 1 wherein said network includes a cellular telephone network (130).

15. The system according to claim 1 wherein said network includes a cable television network (140).

16. The system according to claim 2 wherein said notification means includes a cellular telephone (165).

17. The system according to claim 2 wherein said notification means includes a pager (175).

18. The system according to claim 2 wherein said notification means includes a regular telephone (145).

19. The system according to claim 2 wherein said notification means includes electronic mail.

20. The system according to claim 2 wherein said notification means includes a personal data assistant (185).

21. The system according to claim 2 wherein said notification means includes a television (195) equipped with a set top box.

22. The system according to claim 9 further including comparator means wherein said comparator means compares (410, 415, 420) financial transactions received from said at least one point of sales terminal to said one or more customer preferences.

23. The system according to claim 22 wherein notifications (435, 450) are sent to said at least one customer using said notification means if said financial transactions exceeds said one or more customer preferences.

24. The system according to claim 23 wherein authorization requests are sent (440) to said at least one customer using said notification means if said financial transactions exceeds said one or more customer preferences.

25. The system according to claim 24 wherein said at least one customer account belonging to said at least one customer is suspended (425) if said financial transactions exceeds said one or more customer preferences.

26. A method for reducing financial transaction risk comprising;

establishing (210) networking communications between a client and a financial services server (100) by at least one customer wherein said financial services server (100) is in processing communications with at least one point of sales terminal,

accessing an account on said financial services server owned by said at least one customer,

entering one or more customer preferences (230, 240, 250, 260),

comparing (410, 415, 420) financial transactions received from said at least one point of sales terminal to said one or more customer preferences,

sending (435, 450) notifications to said at least one customer if said financial transactions exceed said one or more customer preferences,

requesting (440) authorization of said at least one customer if said financial transactions exceed said one or more customer preferences,

suspending (425) further financial transactions of said at least one customer if said financial transactions exceed one or more customer preferences.

27. The method according to claim 26 further including the step of authenticating (220) said customer to said financial services server.

28. The method according to claim 26 wherein said networking communications includes using the Internet (120).

29. The method according to claim 26 wherein said networking communications includes using a public telephone service network (110).

30. The method according to claim 26 wherein said networking communications includes using a cellular telephone network (130).

31. The method according to claim 26 wherein said networking communications includes using a cable television network (140).

32. The method according to claim 26 wherein said one or more customer preferences includes transaction limits (240).

33. The method according to claim 26 wherein said one or more customer preferences includes authorization limits (250).

34. The method according to claim 26 wherein said one or more customer preferences includes account suspension limits (260).

35. The method according to claim 26 wherein said one or more customer preferences includes single transactions.

36. The method according to claim 26 wherein said one or more customer preferences includes cumulative transactions.

37. The method according to claim 26 wherein said one or more customer preferences includes an applicable time period.

38. The method according to claim 26 wherein said notification methods includes a cellular telephone (165).

39. The method according to claim 26 wherein said notification methods includes a pager (175).

40. The method according to claim 26 wherein said notification methods includes a regular telephone (145).

41. The method according to claim 26 wherein said notification methods includes electronic mail.

42. The method according to claim 26 wherein said notification methods includes a personal data assistant (185).

43. The method according to claim 26 wherein said notification methods includes a television (195) equipped with a set top box.

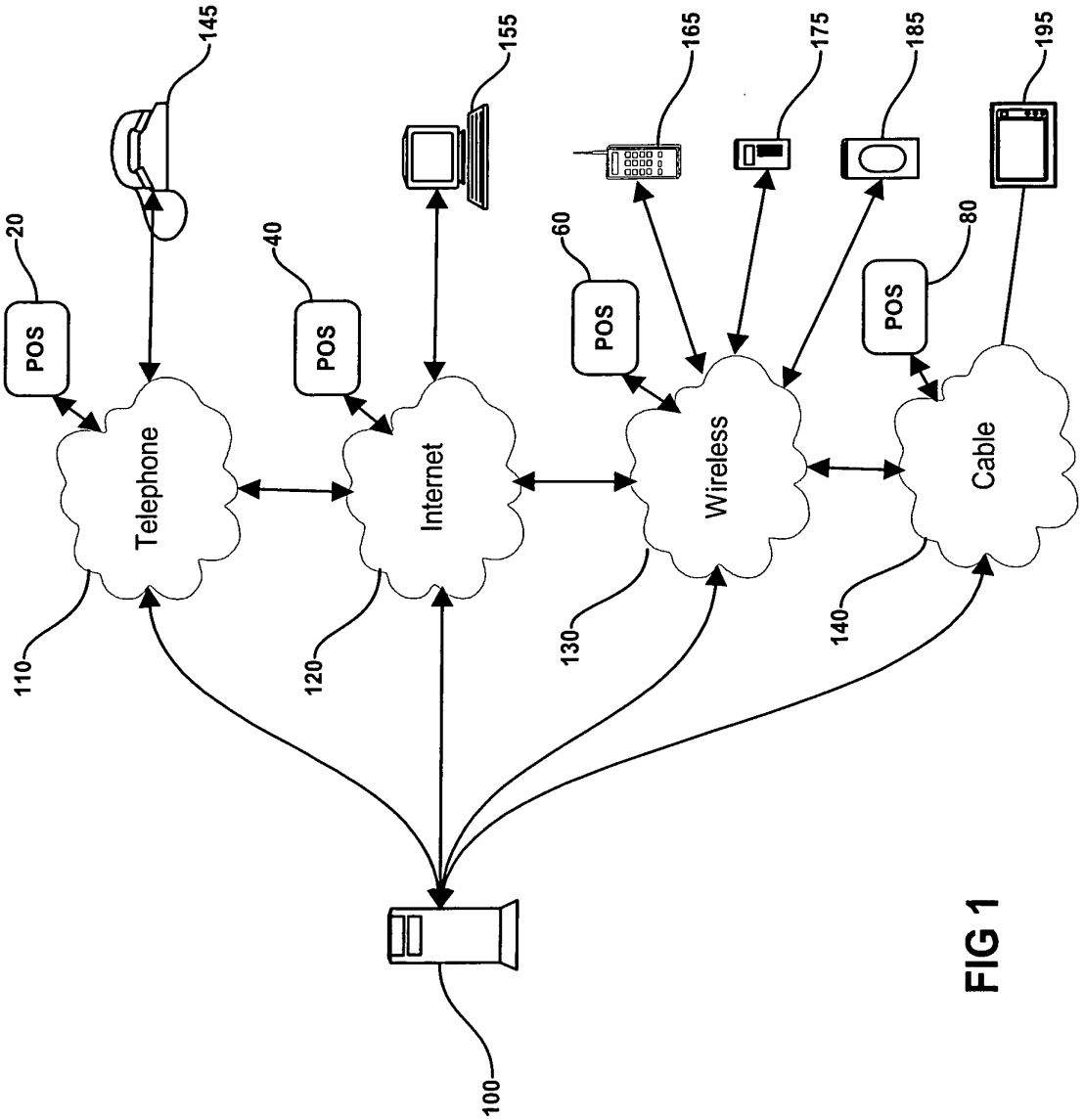

145
155
165
175
185
195
20
40
60
80
POS
POS
POS
POS
Telephone
Internet
Wireless
Cable
110
120
130
140
100

FIG 1

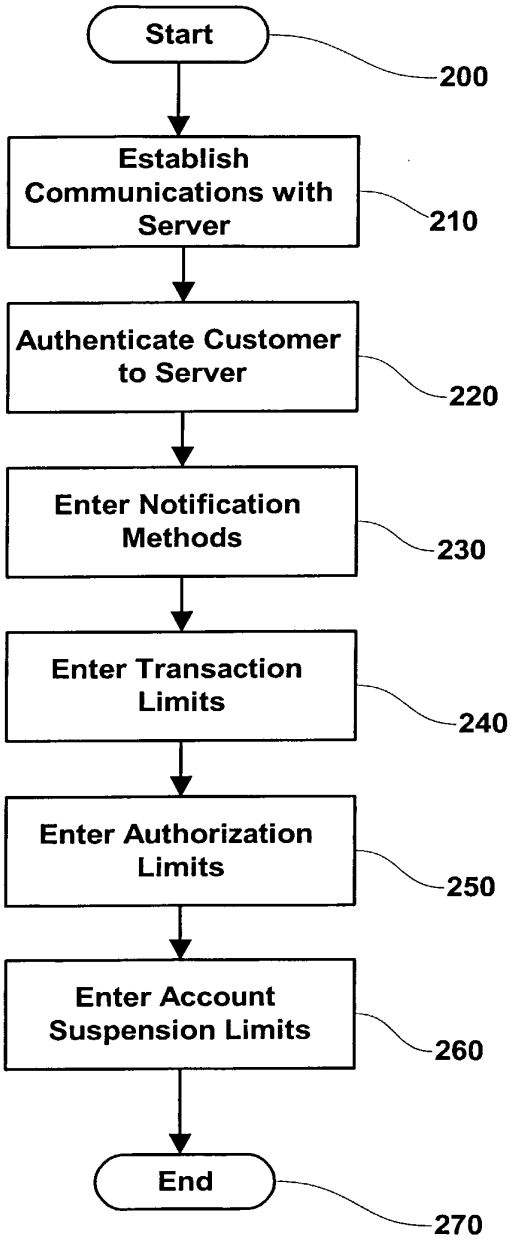

Start
200
Establish Communications with Server
210
Authenticate Customer to Server
220
Enter Notification Methods
230
Enter Transaction Limits
240
Enter Authorization Limits
250
Enter Account Suspension Limits
260
End
270

FIG. 2

Personal Credit Manager

Set Notification Method

☐ Email ☐ Pager

☐ Cell phone ☐ Home phone

☐ Work phone ☐ Alternate phone

Set Transaction Limits

☐ Notify me if any single transaction exceeds:

☐ Notify me if the total $ value of transactions exceeds:

In a ☐ Day ☐ Week ☐ Month ☐ Billing period ☐ Other

Set Authorization Limits

☐ Require authorization if any single transaction exceeds:

☐ Require authorization if the total $ value of transactions exceeds:

In a ☐ Day ☐ Week ☐ Month ☐ Billing period ☐ Other

Set Suspension Limits

Suspend card usage if:

☐ A single transaction exceeds:

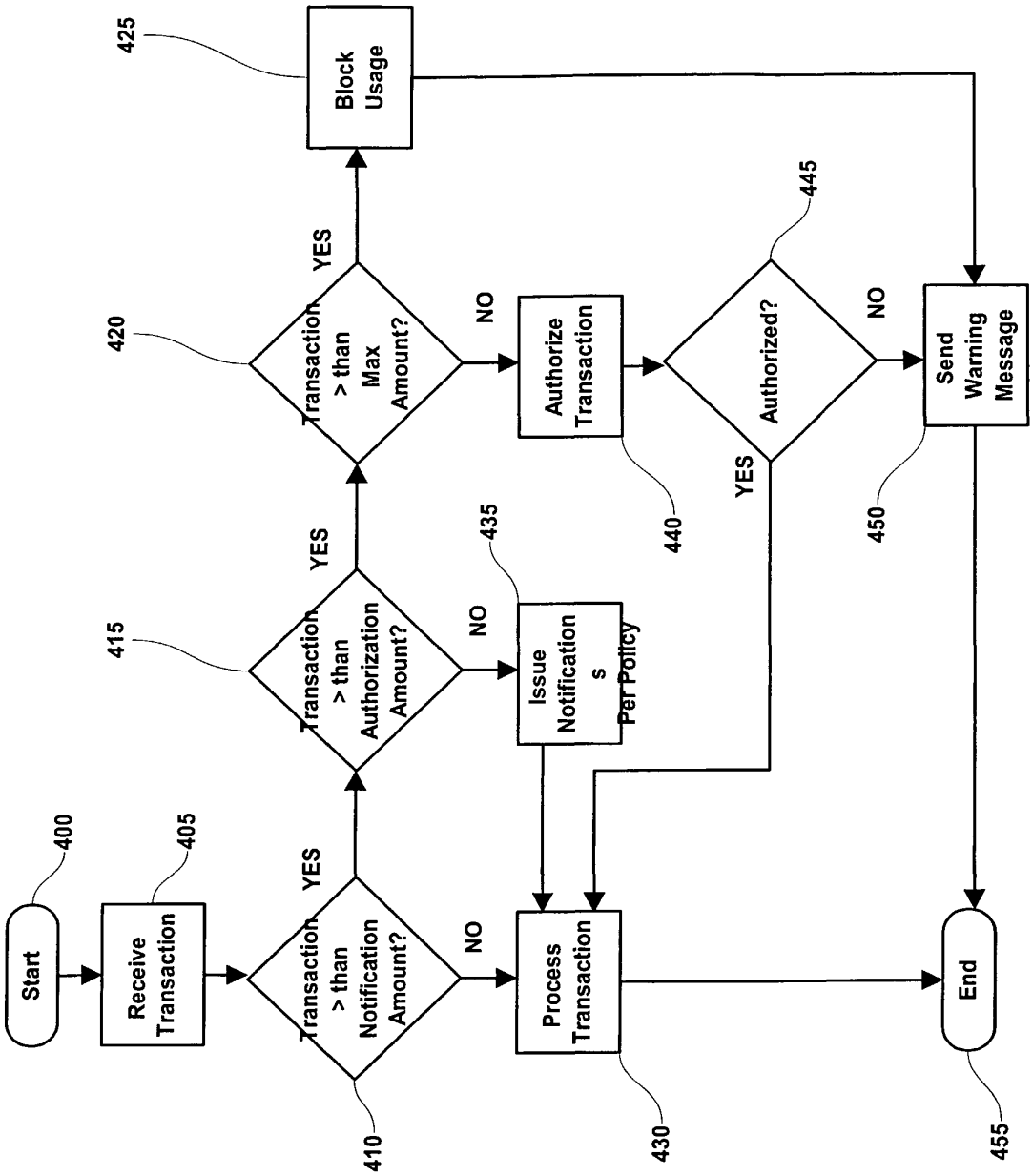
☐ If the total $ value of all transactions exceeds:

In a ☐ Day ☐ Week ☐ Month ☐ Billing period ☐ Other

☐ Include all linked accounts

FIG.3

FIG.4


Start
400
Receive Transaction
405
Transaction > than Notification Amount?
410
YES
NO
Process Transaction
430
Transaction > than Authorization Amount?
415
YES
NO
Issue Notification s Per Policy
435
Transaction > than Max Amount?
420
YES
NO
Block Usage
425
Authorize Transaction
440
Authorized?
445
YES
NO
Send Warning Message
450
End
455

PATENT COOPERATION TREATY

PCT

DECLARATION OF NON-ESTABLISHMENT OF INTERNATIONAL SEARCH REPORT

(PCT Article 17(2)(a), Rules 13ter.1(c) and Rule 39)

Applicant's or agent's file reference	IMPORTANT DECLARATION	Date of mailing *(day/month/year)*
DB3158/JPC		17/04/2003
International application No.	International filing date *(day/month/year)*	(Earliest) Priority date *(day/month/year)*
PCT/EP 02/12851	15/11/2002	30/11/2001
International Patent Classification (IPC) or both national classification and IPC	G06F17/60	
Applicant		
ACTIVCARD		

This International Searching Authority hereby declares, according to Article 17(2)(a), that **no international search report will be established** on the international application for the reasons indicated below

1. ☐ The subject matter of the international application relates to:
   - a. ☐ scientific theories.
   - b. ☐ mathematical theories
   - c. ☐ plant varieties.
   - d. ☐ animal varieties.
   - e. ☐ essentially biological processes for the production of plants and animals, other than microbiological processes and the products of such processes.
   - f. ☒ schemes, rules or methods of doing business.
   - g. ☐ schemes, rules or methods of performing purely mental acts.
   - h. ☐ schemes, rules or methods of playing games.
   - i. ☐ methods for treatment of the human body by surgery or therapy.
   - j. ☐ methods for treatment of the animal body by surgery or therapy.
   - k. ☐ diagnostic methods practised on the human or animal body.
   - l. ☐ mere presentations of information.
   - m. ☐ computer programs for which this International Searching Authority is not equipped to search prior art.

2. ☐ The failure of the following parts of the international application to comply with prescribed requirements prevents a meaningful search from being carried out:
   ☐ the description ☐ the claims ☐ the drawings

3. ☐ The failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions prevents a meaningful search from being carried out:
   ☐ the written form has not been furnished or does not comply with the standard.
   ☐ the computer readable form has not been furnished or does not comply with the standard.

4. Further comments:

Name and mailing address of the International Searching Authority	Authorized officer
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	María Rodríguez Nóvoa

Form PCT/ISA/203 (July 1998)

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 203

The claims relate to subject matter for which no search is required according to Rule 39 PCT. Given that the claims are formulated in terms of such subject matter or merely specify commonplace features relating to its technological implementation, the search examiner could not establish any technical problem which might potentially have required an inventive step to overcome. Hence it was not possible to carry out a meaningful search into the state of the art (Art. 17(2)(a)(i) and (ii) PCT; see Guidelines Part B Chapter VIII, 1-6).

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure. If the application proceeds into the regional phase before the EPO, the applicant is reminded that a search may be carried out during examination before the EPO (see EPO Guideline C-VI, 8.5), should the problems which led to the Article 17(2) declaration be overcome.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 December 2001 (06.12.2001)

PCT

(10) International Publication Number
WO 01/93213 A2

(51) International Patent Classification[7]: G07F 7/08

(21) International Application Number: PCT/US01/40774

(22) International Filing Date: 21 May 2001 (21.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/580,811 26 May 2000 (26.05.2000) US

(71) Applicant: **ALCATEL USA SOURCING, L.P.** [US/US]; 1000 Coit Road, Mail Stop LEGL2, Plano, TX 75075 (US).

(72) Inventors: **MANI, Babu, V.**; 2325 Terping Place, Plano, TX 75025 (US). **STEVENS, Gilman, R.**; 850 Quail Rise, Fairview, TX 75069 (US).

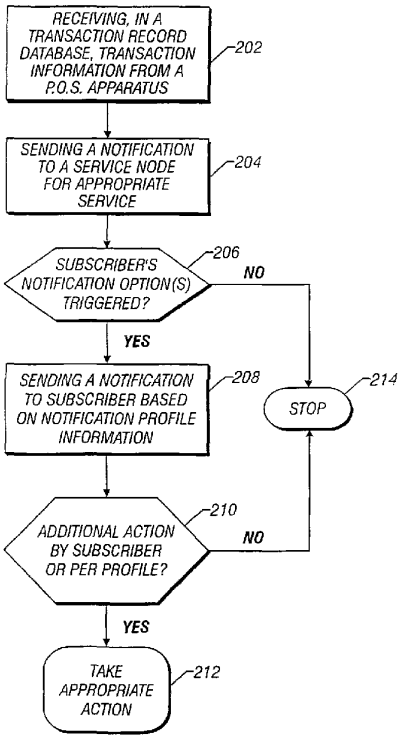
(74) Agent: **DANAMRAJ, Shreen, K.**; Smith, Danamraj & Youst, P.C., Suite 1200, LB-15, 12900 Preston Road, Dallas, TX 75230-1328 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, 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).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR REPORTING TRANSACTION INFORMATION IN A CARD-BASED TRANSACTION



(57) Abstract: A method and system for notifying a subscriber of a transaction that is based on a card issued to the subscriber. A service profile comprising various notification service options is provided for the subscriber. Notification mode, i.e., real-time versus delayed notification, type of notification (e.g., email, voice mail, fax, et cetera), frequency of notification, notification based on frequency of transactions and other options are provided so that a subscriber can elect a particular combination of the notification service options that the subscriber desires. The service profile may be co-located at a transaction record database associated with the card or may be provided as part of an IN-capable Service Control Point (SCP). When an indication from a Point-Of-Sale (POS) apparatus is received in the card transaction record database with respect to a card-based transaction effectuated by a user, a determination is made, based upon the service options available for the subscriber, if the indication contains transaction information that can trigger a notification service for the subscriber. If so, an appropriate notification type is effectuated to inform the subscriber of the transaction.

WO 01/93213 A2

Petitioner Askeladden LLC
Exhibit 1002 - Page 258 of 350

Published:
— *without international search report and to be republished upon receipt of that report*

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.

SYSTEM AND METHOD FOR REPORTING TRANSACTION INFORMATION IN A CARD-BASED TRANSACTION

BACKGROUND OF THE INVENTION

Technical Field of the Invention

The present invention relates to transaction cards and, more particularly, to a system and method for providing transaction information to a cardholder based on a subscriber service profile.

Description of Related Art

Transaction card fraud is a major issue with consumers (i.e, legitimate cardholders) as well as card issuing companies. Several access control schemes are available today for fraud deterrence. For example, as is well known, calling/phone cards, credit cards, automated teller machine (ATM) cards or debit cards, et cetera, typically require entering a correct Personal Identification Number (PIN) as an access control mechanism. To further increase security, some transaction cards have an integrated circuit (e.g., smart cards) which facilitates encryption of a legitimate cardholder's personal identity information and other data.

Although there have been impressive advances in the existing access control schemes designed to reduce costs to a card-issuing entity and its customers, current solutions are not entirely satisfactory. First, there is no sure way that any current system can guard against all forms of fraud, and there is no tangible means of determining what the actual fraud-related costs are. Moreover, the same technological advances that have increased security by means of encryption are also making it possible for illegitimately deciphering access codes etc.

Petitioner Askeladden LLC
Exhibit 1002 - Page 260 of 350

Some of the current authorization/validation schemes require that when a transaction involving a substantial amount of money takes place, the cardholder be contacted directly over the phone. However, unauthorized users may be clever enough to limit the transactions to smaller amounts so that the pattern of fraud does not trigger reporting back to the cardholder.

In addition, although access control schemes such as photo ID, fingerprinting, etc. are useful in preventing fraud where the user is required to be physically present at the site of transaction, such schemes are ineffective for transactions that take place over the phone or via the Internet.

Those skilled in the art should appreciate that despite various on-going developments, transaction card-related fraud is still possible primarily because of the following factors. First, cards and their PINs can still be easily stolen or misplaced. And, second, most access control schemes used in connection with transaction cards can be reverse-engineered with luck and perseverance. Furthermore, once a card and its access control mechanism is misappropriated, the cardholder (or the card-issuing entity) is typically not aware of subsequent, unauthorized transactions until the subscriber receives a billing statement or an appropriate transaction report at the end of a billing/report cycle.

SUMMARY OF THE INVENTION

Accordingly, the present invention is directed to a scheme for informing a cardholder/subscriber as expeditiously as possible of a card-based transaction in a subscriber-selectable manner. A service profile is maintained for the subscriber that comprises various notification service options relative to the time, place, and manner of the transaction notification

Petitioner Askeladden LLC
Exhibit 1002 - Page 261 of 350

which the subscriber wishes to receive. Notification mode, i..e, real-time versus delayed notification, type of notification (e.g., email, voice mail, fax, phone, et cetera), frequency of notification, notification based on frequency of transactions (with or without a dependency on the amount per each transaction), and other options are provided so that a subscriber can elect a particular combination of the notification service options from a plurality of combinations that the subscriber desires. The service profile may be co-located at a transaction record database associated with the card or may be provided as part of an Intelligent Network (IN)-capable Service Control Point (SCP). The SCP can be alerted by the card transaction record database or, in other exemplary embodiments, the SCP may periodically poll the card transaction record database for service status determination. When an indication from a Point-Of-Sale (POS) apparatus is received in the card transaction record database with respect to a card-based transaction effectuated by a user, a determination is made, based upon the service options available for the subscriber, if the indication contains transaction information that can trigger a notification service for the subscriber. If so, an appropriate notification type is effectuated to inform the subscriber of the transaction.

Exemplary embodiments of the POS apparatus include, for example, card readers provided at merchants' locations, interactive televisions (ITVs) and Internet appliances capable of accepting transaction cards by means of Set-Top Boxes (STBs), card receptacles for swiping, optical scanning, etc. Further, based on the service profile options and/or subscriber interaction subsequent to the notification, a law enforcement agency and/or the card company may also be informed of a transaction.

In another aspect, the present invention relates to a method for

Petitioner Askeladden LLC
Exhibit 1002 - Page 262 of 350

notifying a subscriber of a transaction that is based on a card issued to said subscriber. The method commences upon receiving from a POS apparatus an indication in a transaction record database associated with the card with respect to the transaction. Preferably, the indication includes transaction information associated with the transaction such as, for example, the amount of money (credit or debit) involved in the transaction, transaction's time/date stamp, card number (or its alias), etc. Thereafter, a determination is made based at least in part on a service profile associated with the subscriber whether at least a portion of the transaction information triggers a notification service for which the subscriber has a subscription. If so, the notification service is invoked to inform the subscriber of the transaction, wherein the time, place and manner of notification is based on the service profile options provided for the subscriber.

In yet another aspect, the present invention is directed to a computer-accessible medium associated with a service node or a transaction card record database, wherein the computer-accessible medium carries a sequence of instructions provided for executing service logic which, when executed by a processor, causes the processor to perform the following steps. Upon receiving an indication in the transaction record database with respect to a POS transaction that is based on a card issued to a subscriber, a determination is made based at least in part on a service profile associated with the subscriber if at least a portion of the indication triggers a notification service for which the subscriber has a subscription. Responsive to the determination step, the notification service is invoked to inform the subscriber of the transaction based on the service profile.

Petitioner Askeladden LLC
Exhibit 1002 - Page 263 of 350

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the present invention may be had by reference to the following Detailed Description when taken in conjunction with the accompanying drawings wherein:

FIG. 1A depicts an exemplary embodiment of the present invention;

FIG. 1B depicts another exemplary embodiment of the present invention; and

FIG. 2 depicts a flow chart which illustrates the steps involved in an exemplary notification method provided in accordance with the teachings of the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

In the drawings, like or similar elements are designated with identical reference numerals throughout the several views thereof, and the various elements depicted are not necessarily drawn to scale. Referring now to FIG. 1A, depicted therein is an exemplary communications network arrangement 100A for notifying a subscriber 101 in accordance with the teachings of the present invention when a card-based transaction is effectuated by a user 102. It is contemplated herein that the card may be of any type that can be used for a Point-Of-Sale (POS) transaction (e.g., purchase of goods and/or services, withdrawal or transfer of money, cash equivalents, or indicia/instruments of value) at a facility (i.e., a merchant's premises, a financial facility, sites of automated teller machines (ATMs), service provider's offices, etc.) or over a network (voice, data, hybrid, and the like). Accordingly, the teachings of the present invention may be practiced in any arrangement which involves the use of cards such as credit cards, debit

Petitioner Askeladden LLC
Exhibit 1002 - Page 264 of 350

cards, phone/calling cards, charge cards, bank cards, ATM cards, smart cards, cards with integrated circuits (ICs) and/or photo IDs, et cetera (hereinafter collectively referred to as "transaction cards").

Upon obtaining a transaction card, user 102 (including but not limited to, for example, persons authorized by the subscriber to whom the card is issued, i.e., cardholder; unauthorized or fraudulent users; etc.) engages in a POS transaction using a suitable POS apparatus 104. As exemplified in FIG. 1A, the POS apparatus 104 may comprise, for example, a card reader terminal 106 located at a facility. Also, in other exemplary embodiments, the POS apparatus 104 may be provided as a Set-Top Box (STB) in conjunction with an interactive television (ITV) station (exemplified as ITV block108 in FIG. 1A) wherein, for example, a home shopping application can be engaged for ordering a product or service through the ITV server's network (not shown in FIG. 1A). In yet another exemplary embodiment, the POS apparatus 104 may comprise a WWW-based network appliance 110 (i.e., an Internet appliance or information appliance such as, e.g., a personal computer, hand-held computer, laptop or palmtop computer, Web-enabled personal digital assistant (PDA) or a phone, etc.) that can accept a transaction card or card information for effectuating a transaction.

Depending upon the type of POS apparatus and transaction card, an appropriate transaction record database 112 is provided in the arrangement 100A for record maintenance, billing, etc. with respect to the transactions associated with the card. A card/user authentication system 114 may also be preferably provided therewith. A data communication path 105 is conventionally disposed between the transaction record database 112 and the POS apparatus 104.

The transaction record database 112 and associated authentication

Petitioner Askeladden LLC
Exhibit 1002 - Page 265 of 350

system 114 may be located at the same facility where the POS apparatus 104 is located, or may be remotely disposed. Accordingly, it should be appreciated that the communication path 105 provided for transmitting a transaction-related indication (i.e., card number, amount of the transaction, time/date stamp of the transaction, etc.) from the POS apparatus 104 to the transaction record database 112 may involve a network (e.g., a card reader network or an ATM network, et cetera).

As those skilled in the art should readily recognize, the transaction record database 112 and associated authentication system 114 are conventionally disposed in the arrangement 100A with respect to the card company 116 which issues or causes to issue cards such as the transaction card obtained by the user 102. Although not explicitly depicted, a network may be conventionally involved for effectuating a communication path 111 disposed between the transaction record database 112 and the card company 116. Those skilled in the art should further recognize that the transaction record database 112, authentication system 114, and the card company site 116 may be co-located also.

A service node, e.g., a Service Control Point (SCP) 118, is provided in the exemplary arrangement 100A for implementing a subscriber-selectable notification service in accordance with the teachings of the present invention. Preferably, the SCP node 118 is in data communication with the transaction record database 112 via a network 120 (e.g., a telecommunications network, a packet-switched data network such as the Internet, or a hybrid network). A notification service profile 122 comprising various notification service options available to the subscriber 101 is provided with the SCP 118 such that appropriate service logic is executed for informing or notifying the subscriber of a card-based

Petitioner Askeladden LLC
Exhibit 1002 - Page 266 of 350

transaction. By way of example, the following options may be advantageously provided as part of the notification service profile 122:

- Notification mode 124: In real-time mode, a notification may be transmitted to the subscriber immediately in real-time, i.e, as soon as practicable once a card-based transaction is effectuated by a user. In delayed mode, notifications are delayed by a delay factor that is subscriber-selectable.
- Notification system/method 126: This option allows the subscriber to specify the manner of notification. Examples include pagers (with option to send confirmation using two-way paging); email; voice mail; phone (wireless or wireline); facsimile transmission; wireless PDAs, et cetera; or any combination thereof (i.e., multi-device dissemination)
- Frequency of transaction 128: A notification may be based on the number of transactions per a select period. For instance, the subscriber may be notified when the number of transactions per day reach a threshold. Similar thresholds may be established for number of transactions per week, per billing period, etc.
- Frequency of amount charged 130: A notification may be provided to the subscriber based on the total amount charged or transacted per a select period, e.g., per day or per week, etc.
- Combination method 132: Several subscriber-selectable (i.e., subscriber-configurable) notification schemes may be provided using one or several of the foregoing options. Default combinations may also be provided as packaged or pre-packaged notification service options.

Petitioner Askeladden LLC
Exhibit 1002 - Page 267 of 350

- Transaction area 133: Based on where the transaction takes place, the subscriber may define different notification options as well. For example, when a transaction occurs in a particular area, the subscriber wishes to receive a notification in real-time; on the other hand, when transactions take place in other areas, a delayed notification may be desirable. Accordingly, a plurality of transaction locations (e.g., Location-1 through Location-N) may be included in the subscriber's notification service profile 122. Clearly, other service options may be bundled with the transaction area 133 option in various permutations and combinations.

Based on the notification service profile 122, the SCP node 118 is provided with the capability to initiate a "call" to the notification device/apparatus 134 specified by the subscriber 101 at the time/interval indicated in the profile. Depending upon the notification device, accordingly, a communication path 117 between the SCP node 118 and the apparatus 134 may be effectuated via a suitable network, e.g., a telecommunications network, a packet-switched data network such as the Internet, or a hybrid network. In addition, notification may be forwarded to various subscriber-designated third parties such as, e.g., subscriber's secretary, power of attorney, etc., as may be indicated in the notification service profile 122.

Referring now to FIG. 1B, reference numeral 100B refers to another exemplary network arrangement wherein the notification system and method of the present invention may be advantageously practiced. It should be apparent that the network arrangement 100B is essentially similar to the network arrangement 100A depicted in FIG. 1A, except that the service

Petitioner Askeladden LLC
Exhibit 1002 - Page 268 of 350

logic and notification service profile 122 are directly available to the transaction record database 112 without the involvement of a dedicated service node (such as the SCP 118 provided in the arrangement 100A). Accordingly, in one implementation, the transaction record database 112 and subscriber notification service profile 122 may be integrated into a single node having processing capability for executing appropriate notification service logic that is loadable from a computer-accessible medium. Computing and networking capability of the integrated node allows it to inform or notify the subscriber of a transaction based on applicable service profile options via a suitable device (e.g., notification apparatus ensemble 134). As is the case with the SCP-generated notification process described hereinabove, the integrated transaction record database node uses an appropriate network (e.g., network 120) to connect to the notification apparatus 134 at the time/interval indicated in the service profile database 122.

FIG. 2 depicts a flowchart of the steps involved in an exemplary notification process of the present invention wherein a subscriber is informed of a card-based transaction on the basis of a suitable subscriber-selectable service option profile when a user engages in such a transaction via a POS apparatus. Upon receiving transaction information (i.e., amount of the transaction, time/date stamp of the transaction, etc.) by way of one or more appropriate indications from the POS apparatus (step 202), the transaction record database associated with the card being used transmits a notification to a service node for further analysis (step 204). The notification preferably includes at least a portion of the transaction information. Based on the transmitted transaction information and the service option profile information, a determination is then made whether a

Petitioner Askeladden LLC
Exhibit 1002 - Page 269 of 350

notification option is to be triggered (decision block 206). If not, the notification process terminates (step 214).

Upon determining that a notification option is to be triggered, an appropriate service logic portion is invoked so that a notification is transmitted by the service node to the subscriber's device based on the service profile (step 208). Such notification information may include the amount involved in the transaction; time/date stamp information; place/facility where the POS apparatus is located; type of goods/services or merchandise, if applicable; card number; etc.

The subscriber may be provided with the capability to interact with the service node after receiving the notification therefrom in order to indicate further actions such as, for example, reporting the transaction to the card issuing company or alerting a law enforcement agency, if fraudulent card use is suspected (decision block 210 and step 212). In some implementations, such interactive capability may be indicated as part of the subscriber's service profile also. If no further action is provided for, the notification process of the present invention terminates (step 214).

Based on the foregoing, those skilled in the art should appreciate that the present invention's system and method of notifying transaction information based on a subscriber's service profile offers several advantages. First, by practicing the present invention in accordance with the teachings contained herein, it is envisaged that there will be a substantial reduction in fraudulent card transactions because a law enforcement agency may be notified as soon as an unauthorized or unlawful transaction takes place. Clearly, this is beneficial to the consumers as well as the card companies. Further, increased accountability will result on the part of authorized users in situations where the subscriber (i.e., the primary

Petitioner Askeladden LLC
Exhibit 1002 - Page 270 of 350

cardholder) allows others to use the subscriber's card or additional cards for which the subscriber is the paying party because of immediate notification of the card transactions. In addition, since it is possible to track or account for each transaction immediately, no surprising entries or items will be expected in billing statements from the card company at the end of a billing cycle.

It is believed that the operation and construction of the present invention will be apparent from the foregoing Detailed Description. While the system and method shown and described have been characterized as being preferred, it should be readily understood that various changes, modifications and enhancements could be made therein without departing from the scope of the present invention as set forth in the following claims. For example, the teachings of the present invention may be practiced in some instances where the user and subscriber are the same. Thus, user 102 and subscriber 101 exemplified in FIGS. 1A and 1B may be the same in such circumstances and transaction notifications may be forwarded to, e.g., a subscribed-designated third party, for instance, subscriber's spouse.

Further, it is possible to suppress the card number when a transaction notification is sent to the subscriber. Instead of the card number, the service logic may supply a subscriber-selectable alias/identification such as, e.g., "account 1", "my _card 1", etc. Additionally, where a subscriber has multiple cards or multiple types of cards, different notification options may be provided as part of the subscriber service profile for each card. By way of example, a subscriber may choose to be notified every time a business transaction card is used, but only when a sum total of charges on a personal card exceeds a specified daily/weekly amount. Also, because of the integration of voice networks and Internet Protocol (IP)-based data

Petitioner Askeladden LLC
Exhibit 1002 - Page 271 of 350

networks, a plethora of diverse personal communication devices may be employed for purposes of the present invention. For example, such devices may comprise H.323-compatible terminals, Session Initiation Protocol (SIP)-based phones, and the like. Accordingly, those skilled in the art should readily appreciate that these and other variations, additions, modifications, enhancements, etc. are deemed to be within the ambit of the present invention whose scope is determined solely by the following claims.

Petitioner Askeladden LLC
Exhibit 1002 - Page 272 of 350

WHAT IS CLAIMED IS:

1. A method of notifying a subscriber of a transaction that is based on a card issued to said subscriber, comprising the steps of:

receiving, in a transaction record database associated with said card, an indication from a Point-Of-Sale (POS) apparatus with respect to said transaction, said indication including transaction information associated with said transaction;

determining, based on a service profile associated with said subscriber, if at least a portion of said transaction information triggers a notification service for which said subscriber has a subscription; and

if so, invoking said notification service to inform said subscriber, based on said service profile, of said transaction.

2. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said POS apparatus comprises a card reader terminal located at a merchant's facility for effectuating said transaction.

3. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said POS apparatus comprises an interactive television (ITV) set having means capable of accepting card information from a user for effectuating said transaction over a network.

4. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said POS apparatus comprises an interactive network appliance having means capable of accepting card information from a user for effectuating said transaction over the Internet.

Petitioner Askeladden LLC
Exhibit 1002 - Page 273 of 350

5. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said transaction information comprises a monetary value associated with said transaction.

6. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said transaction information comprises a time stamp of said transaction.

7. The method of notifying a subscriber of a transaction as set forth in claim 1, further comprising the step of alerting a law enforcement agency with respect to said transaction based on said service profile.

8. The method of notifying a subscriber of a transaction as set forth in claim 1, further comprising the step of alerting, based on said service profile, a card issuing company that issued said card.

9. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said notification service includes informing said subscriber via email.

10. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said notification service includes informing said subscriber via facsimile transmission.

Petitioner Askeladden LLC
Exhibit 1002 - Page 274 of 350

11. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said notification service includes informing said subscriber via a pager.

12. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said notification service includes informing said subscriber via a wireline telephone.

13. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said notification service includes informing said subscriber via a wireless telephone.

14. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said notification service includes informing said subscriber via an Internet appliance.

15. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said notification service includes informing said subscriber via a personal digital assistant.

16. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said notification service includes informing said subscriber via a hand-held computer.

17. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said notification service includes informing said subscriber in a substantially real-time mode.

Petitioner Askeladden LLC
Exhibit 1002 - Page 275 of 350

18. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said notification service includes informing said subscriber once per a select period.

19. The method of notifying a subscriber of a transaction as set forth in claim 18, wherein said select period comprises a day.

20. The method of notifying a subscriber of a transaction as set forth in claim 18, wherein said select period comprises a week.

21. The method of notifying a subscriber of a transaction as set forth in claim 18, wherein said select period comprises a billing cycle associated with said card.

22. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said notification service includes informing said subscriber based on a predetermined subscriber-selectable criterion.

23. The method of notifying a subscriber of a transaction as set forth in claim 1, wherein said determination step is effectuated at a Service Control Point (SCP) disposed in an Intelligent Network, said SCP being receiving a service request message from said transaction record database.

Petitioner Askeladden LLC
Exhibit 1002 - Page 276 of 350

24. A system for notifying a subscriber of a transaction in a subscriber-selectable manner, wherein said transaction is based on a card issued to said subscriber, comprising:

a Point-Of-Sale (POS) apparatus for generating an indication to a transaction record database, said indication including transaction information associated with said transaction;

means for determining, based on a service profile associated with said subscriber, if at least a portion of said transaction information triggers a notification service for which said subscriber has a subscription; and

means for invoking said notification service, responsive to said means for determining, to inform said subscriber of said transaction based on said service profile.

25. The system for notifying a subscriber of a transaction as set forth in claim 24, wherein said means for determining and said means for invoking are co-located at a Service Control Point (SCP) disposed in an Intelligent Network, said SCP including said service profile associated with said subscriber.

26. The system for notifying a subscriber of a transaction as set forth in claim 24, wherein said means for determining and said means for invoking are co-located at said transaction record database, said transaction record database including said service profile associated with said subscriber.

Petitioner Askeladden LLC
Exhibit 1002 - Page 277 of 350

27. The system for notifying a subscriber of a transaction as set forth in claim 24, wherein said POS apparatus comprises a card reader terminal located at a merchant's facility for effectuating said transaction.

28. The method for notifying a subscriber of a transaction as set forth in claim 24, wherein said POS apparatus comprises an interactive television (ITV) set having means capable of accepting card information from a user for effectuating said transaction over a network.

29. The method for notifying a subscriber of a transaction as set forth in claim 24, wherein said POS apparatus comprises an interactive network appliance having means capable of accepting card information from a user for effectuating said transaction over the Internet.

Petitioner Askeladden LLC
Exhibit 1002 - Page 278 of 350

30. A computer-accessible medium associated with a transaction record database, said transaction record database for recording transactions based on a card issued to a subscriber, wherein said computer-accessible medium carries a sequence of instructions provided for executing service logic which, when executed by a processor, causes said processor to perform the steps of:

upon receiving an indication in said transaction record database with respect to a Point-Of-Sale (POS) transaction that is based on said card, said indication including transaction information associated with said transaction, determining, based at least in part on a service profile associated with said subscriber, if at least a portion of said transaction information triggers a notification service for which said subscriber has a subscription; and

responsive to said determination step, invoking said notification service to inform said subscriber, based on said service profile, of said transaction.

31. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said POS transaction is effectuated by means of a card reader terminal located at a merchant's facility.

32. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said POS transaction is effectuated via an interactive television (ITV) set having means capable of accepting card information from a user for carrying out said transaction over a network.

Petitioner Askeladden LLC
Exhibit 1002 - Page 279 of 350

33. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said POS transaction is effectuated via an interactive network appliance having means capable of accepting card information from a user for carrying out said transaction over the Internet.

34. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said transaction information comprises a monetary value associated with said transaction.

35. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said transaction information comprises a time stamp associated with said transaction.

36. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said notification service includes informing said subscriber via email.

37. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said notification service includes informing said subscriber via facsimile transmission.

38. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said notification service includes informing said subscriber via a pager.

Petitioner Askeladden LLC
Exhibit 1002 - Page 280 of 350

39. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said notification service includes informing said subscriber via a wireline telephone.

40. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said notification service includes informing said subscriber via a wireless telephone.

41. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said notification service includes informing said subscriber via an Internet appliance.

42. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said notification service includes informing said subscriber via a personal digital assistant.

43. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said notification service includes informing said subscriber via a hand-held computer.

44. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said notification service includes informing said subscriber in a substantially real-time mode.

45. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said notification service includes informing said subscriber once per a select period.

Petitioner Askeladden LLC
Exhibit 1002 - Page 281 of 350

46. The computer-accessible medium associated with a transaction record database as set forth in claim 45, wherein said select period comprises a day.

47. The computer-accessible medium associated with a transaction record database as set forth in claim 45, wherein said select period comprises a week.

48. The computer-accessible medium associated with a transaction record database as set forth in claim 45, wherein said select period comprises a billing cycle associated with said card.

49. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said notification service includes informing said subscriber based on a predetermined combination of subscriber-selectable criteria.

50. The computer-accessible medium associated with a transaction record database as set forth in claim 30, wherein said notification service includes informing said subscriber in a delayed mode.

Petitioner Askeladden LLC
Exhibit 1002 - Page 282 of 350

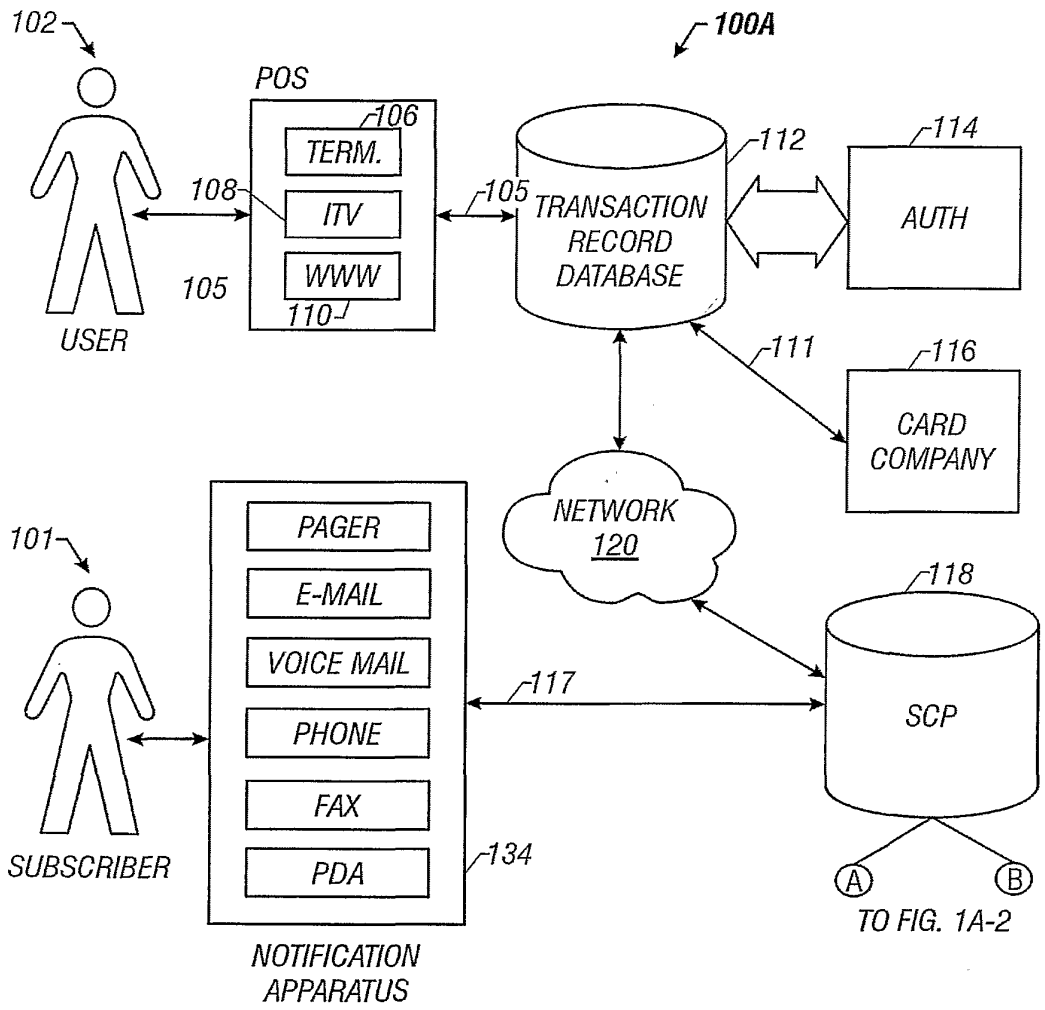

102
100A
POS
106
TERM.
ITV
WWW
110
108
105
105
USER
TRANSACTION RECORD DATABASE
112
114
AUTH
111
116
CARD COMPANY
NETWORK 120
101
PAGER
E-MAIL
VOICE MAIL
PHONE
FAX
PDA
134
117
118
SCP
A
B
TO FIG. 1A-2
SUBSCRIBER
NOTIFICATION APPARATUS

FIG. 1A-1

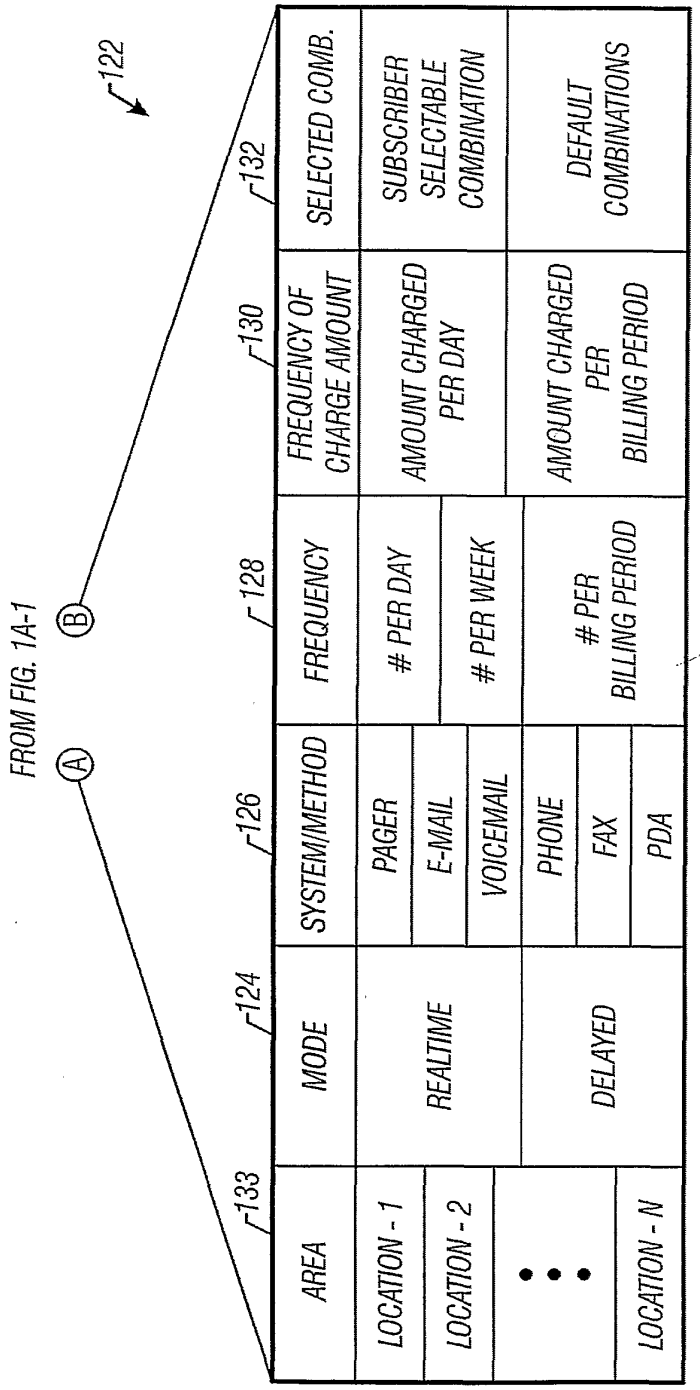

122
FROM FIG. 1A-1
A
B
133
124
126
128
130
132
AREA
MODE
SYSTEM/METHOD
FREQUENCY
FREQUENCY OF CHARGE AMOUNT
SELECTED COMB.
LOCATION - 1
LOCATION - 2
LOCATION - N
REALTIME
DELAYED
PAGER
E-MAIL
VOICEMAIL
PHONE
FAX
PDA
PER DAY
PER WEEK
PER BILLING PERIOD
AMOUNT CHARGED PER DAY
AMOUNT CHARGED PER BILLING PERIOD
SUBSCRIBER SELECTABLE COMBINATION
DEFAULT COMBINATIONS

FIG. 1A-2

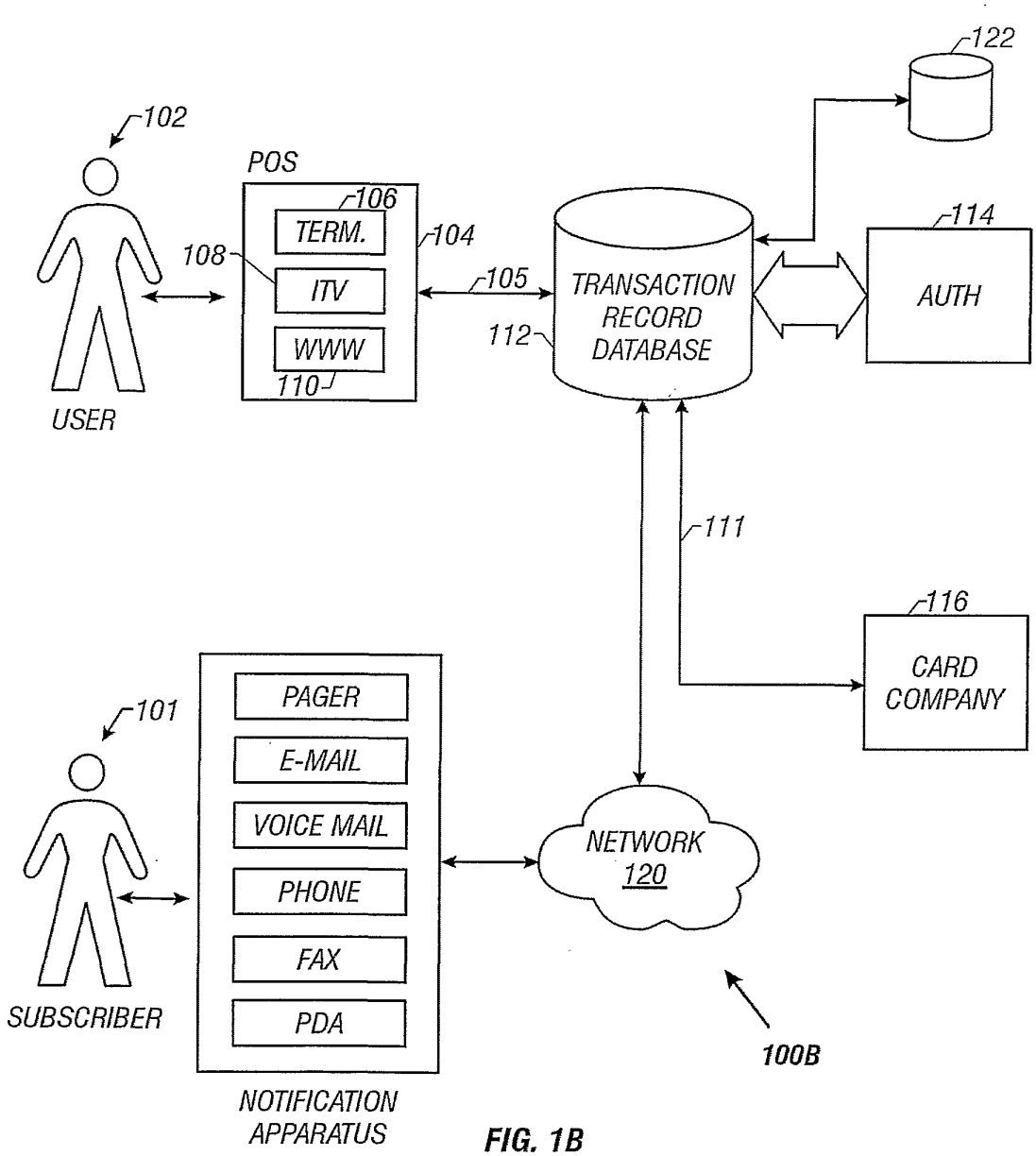

122
102
POS
106
TERM.
104
108
ITV
105
TRANSACTION RECORD DATABASE
114
AUTH
WWW
112
110
USER
111
116
CARD COMPANY
101
PAGER
E-MAIL
VOICE MAIL
PHONE
FAX
PDA
NETWORK 120
SUBSCRIBER
100B
NOTIFICATION APPARATUS

FIG. 1B

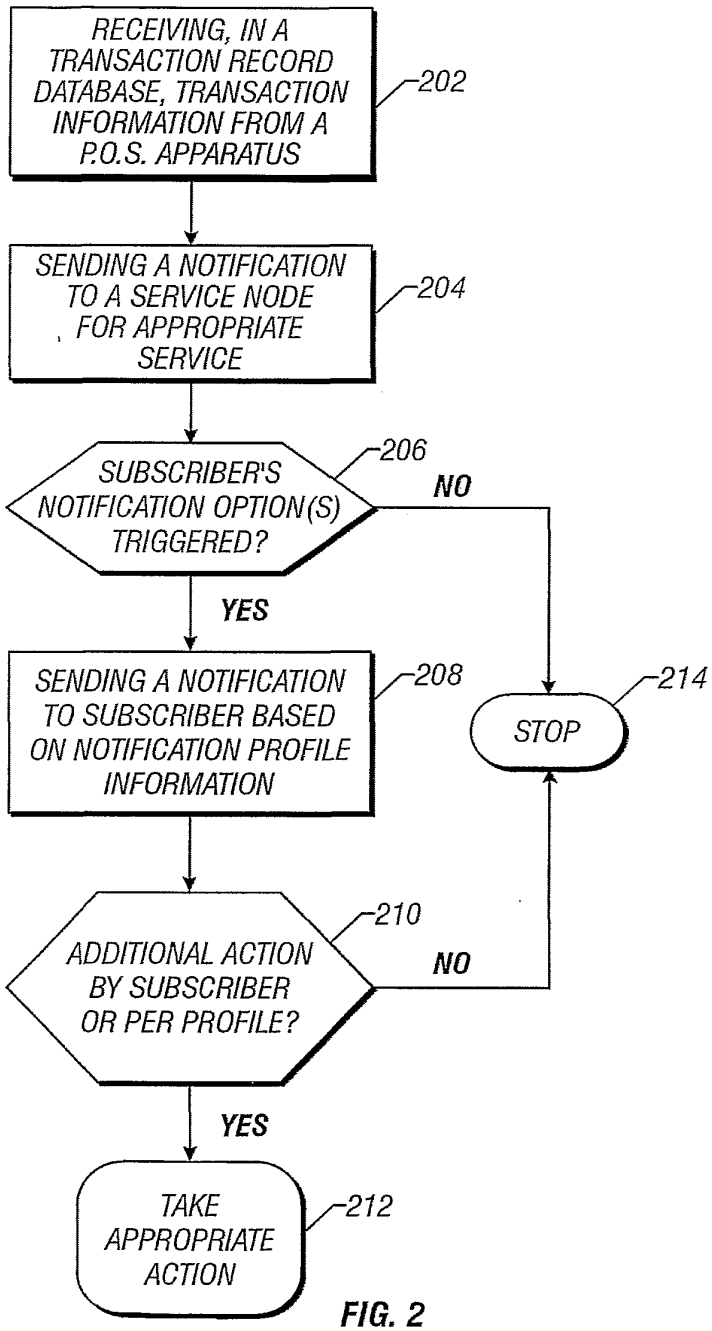

RECEIVING, IN A TRANSACTION RECORD DATABASE, TRANSACTION INFORMATION FROM A P.O.S. APPARATUS
202
SENDING A NOTIFICATION TO A SERVICE NODE FOR APPROPRIATE SERVICE
204
SUBSCRIBER'S NOTIFICATION OPTION(S) TRIGGERED?
206
NO
YES
SENDING A NOTIFICATION TO SUBSCRIBER BASED ON NOTIFICATION PROFILE INFORMATION
208
STOP
214
ADDITIONAL ACTION BY SUBSCRIBER OR PER PROFILE?
210
NO
YES
TAKE APPROPRIATE ACTION
212

FIG. 2

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 October 2002 (17.10.2002)

PCT

(10) International Publication Number
WO 02/082392 A2

(51) International Patent Classification[7]: G07F 19/00

(21) International Application Number: PCT/GB02/01029

(22) International Filing Date: 7 March 2002 (07.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/827,075 5 April 2001 (05.04.2001) US

(71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(71) Applicant *(for MG only)*: **IBM UNITED KINGDOM LIMITED** [GB/GB]; P O Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

(72) Inventor: **PETERS, Mark, Emmette**; 2109 Fountain Ridge Road, Chapel Hill, NC 27514 (US).

(74) Agent: **FOURNIER, Kevin, John**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

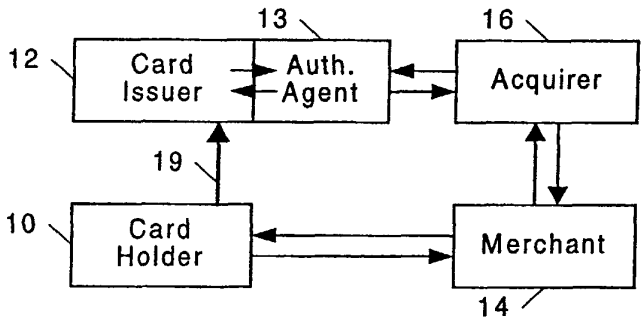
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT,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

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, 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, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

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: ACCOUNT-BASED TRANSACTIONS USING PERSONAL AUTHORIZATION CRITERIA



(57) Abstract: Account holders, such as credit or debit card holders, are sometimes concerned that information supplied to a merchant during transactions will be misappropriated and misused for fraudulent purposes. To improve the confidence of account holders that such misuse will not occur, an account holder may add merchant-specific personal authorization criteria to the account record. Criteria may also be established for controlling dealings with merchants for whom no explicit criteria exist.

WO 02/082392 A2

Petitioner Askeladden LLC
Exhibit 1002 - Page 287 of 350

ACCOUNT-BASED TRANSACTIONS USING PERSONAL AUTHORIZATION CRITERIA

The present intention relates to methods and systems for enhancing the security of account-based transactions through the use of personal authorization criteria.

The explosive growth of the Internet, and particularly the user-friendly World Wide Web, have created unprecedented opportunities for computer users to explore their world, retrieve information once relegated to the dusty shelves of distant reference libraries and to do more mundane things, like buy things. The World Wide Web has become a virtual Worldwide bazaar, offering products from the remote corners of the planet to shoppers who have to travel no further than the closest computer system with Internet access in order to learn about and buy such products. On perhaps a less exotic level, even staid, tradition-rich retailers have almost universally embraced the Internet and have begun to encourage their customers to use the World Wide Web to buy many products formerly available only at retail stores. Retailers with a Web presence stress the convenience of on-line shopping and are acutely aware that a well-designed Web site can effectively promote brand recognition and customer loyalty.

Because an on-line shopper and an on-line merchant do not engage in a face-to-face transaction, normal payment mechanisms such as personal checks or cash are seldom used for on-line transactions. By far, the bulk of on-line transactions are conducted using credit cards or debit cards as the payment mechanism. An on-line buyer sitting at a personal computer keyboard keys in critical account information, usually including the card identification, the name on the card, the card number and an expiration date. An on-line buyer using the telephone to contact a retailer provides the same information to the merchant's representative at the other end of the telephone connection.

A significant number of people refuse to shop on-line because they are concerned that the card information they must supply through a data network or over a telephone connection will find its way into the hands of criminals, who will use that information to make fraudulent purchases that will be billed to the card owner's account. While laws exist in some countries, including the United States, which limit the financial liability of a card owner for purchases made without the owner's consent, some people

Petitioner Askeladden LLC
Exhibit 1002 - Page 288 of 350

nevertheless are still reluctant to use credit or debit cards for on-line transactions. These people fear that, notwithstanding the laws, it will prove difficult and time-consuming to get fraudulent charges removed from their account records and that their credit rating and reputation will suffer damage even if they can ultimately show that they were not responsible for the charges.

Concerns such as those discussed above have led to the development of what are referred to as alternative payment options to enable shoppers to engage in on-line shopping without revealing credit card information. Alternative payment options, sometimes referred to as e-cash, generally conform to one of two major models. The more common of the two models is a stored-value model. According to this model, the user uses off-line transactions to create and maintain an on-line account with a particular merchant. The off-line transactions may consist of mailing a check to the merchant or presenting a credit card directly at a local establishment operated by the merchant or the merchant's agent in order to transfer funds into the on-line account. Once the on-line account is funded, the user can shop on-line with the merchant. The shopper provides a personal identification number known only to the shopper and the merchant to authorize the merchant to draw on the account.

The second e-cash model requires that a shopper establish an account with a third party willing to guarantee payment to a participating merchant. When a participating merchant fulfils an on-line order from the shopper, the merchant bills the third party, rather than the shopper. The third party then notifies the shopper of the account balance. To maintain the account, the shopper must pay off the balance on a regular basis. This e-cash model is very much like a normal credit card model but on a much smaller scale. The buyer's account information is more secure simply because there are fewer places at which a criminal can use that information to make fraudulent purchases.

A basic problem with e-cash models such as these is that participating merchants must do extra work to set up and use e-cash accounts. Relatively few merchants have been convinced they receive any substantial benefit from participating in e-cash programs, which means that there are relatively few places that shoppers with e- cash accounts can make use of them. This results in a chicken and egg situation with merchants being reluctant to

Petitioner Askeladden LLC
Exhibit 1002 - Page 289 of 350

participate in e-cash programs until more shoppers make use of them and shoppers being reluctant to join such programs until there are more merchants who are willing to participate in them. Another problem with e-cash models is that cardholders may not be able to repudiate a transaction if fraud occurs or if merchandise is misrepresented.

Still other payment mechanisms have been proposed which are intended to improve security for card holders while allowing merchants to use conventional card-based transaction authorization processes. According to one such mechanism, a buyer who wants to place an on-line order first provides notice of the proposed transaction to the card issuer or another agent to whom the responsibility for authorizing (or not authorizing) transactions has been delegated. For simplicity, institutions or agencies responsible for approving/disapproving on-line transactions in response to merchant requests are referred to as authorization agents. When notified of a proposed transaction by a card holder, the authorization agent responds by issuing a use-once-only surrogate number to the card holder. In the course of the following on-line transaction, the card holder uses the surrogate number in place of his regular account number. The merchant processes the surrogate card number in the conventional way, presenting the surrogate number to the authorization agent as part of its request for authorization. Because the surrogate number remains valid only for duration of the single transaction for which it was issued, it has no value to anyone who fraudulently acquires it for future use.

Under still another scheme, a card holder can turn his card "on" and "off". The card holder is supposed to keep his card "off" or deactivated until he wants to use it in support of an on-line transaction. At that point, the card holder sends instructions to the authorization agent to turn the card "on". Once the on-line transaction or transactions have been concluded, the card holder may expressly instruct the authorization agent to turn the card "off" or may simply wait for a time-out period to expire. The card will automatically be turned "off" on expiration of the time-out period. One potential problem specific to this scheme is that a diligent card holder may have completed a previous legitimate transaction before beginning the current transaction. If the card turns "off" as a result of the previous transaction before the merchant completes the authorization process for the current transaction, the possibility exists that authorization for the current transaction will be incorrectly withheld.

Petitioner Askeladden LLC
Exhibit 1002 - Page 290 of 350

A more general problem with schemes such as the ones just discussed is the card holder must make an extra effort to provide advance notice to an authorization agent for each and every proposed on-line transaction. While some card holders may be willing to accept this burden, others will probably will find it to be annoying and frustrating, particularly if a communications problem keeps them from reaching the authorization agent when the shopper is ready to begin the on-line transaction.

The present invention provides a method as claimed in claim 1, a system as claimed in claim 7, and computer program product as claimed in claim 8 for enhancing the security of an account by enhancing the control an account holder has over where and how the account can be used. An account is initially created in any of several conventional ways; for example, by an account candidate responding to direct mail or telephone solicitations by an account issuer. Once the account is established, however, the card holder creates his or her own credit authorization policy by providing personal authorization criteria to the authorization agent, who stores the criteria as part of the account record. Preferably in subsequent transactions, stored personal authorization criteria override any default authorization criteria normally followed by the authorization agent when receiving a request for authorization.

While the specification concludes with claims particularly pointing out and distinctly claiming that which is regarded as the present invention, details of preferred embodiments of the invention may be more readily ascertained from the following technical description when read in conjunction with the accompanying drawings wherein:

Figure 1 is a block diagram of a conventional transaction system suitable for establishing the necessary relationships among participants in account-based transactions;

Figure 2 is a block diagram of a transaction system showing the ordinary flow of information during account-based, such as those involving the use of credit or debit cards;

Figure 3 is a block diagram of a transaction system showing both the ordinary flow of information and the added security-enhancing flow of

Petitioner Askeladden LLC
Exhibit 1002 - Page 291 of 350

information in accordance with a preferred embodiment of the present invention;

Figure 4 is a functional representation of a network system suitable for processing requests for conducting transactions in accordance with a preferred embodiment of the present invention;

Figure 5 is a block diagram of a computer system capable of implementing a preferred embodiment of the present invention;

Figure 6 represents the data structure of an account record suitable for use in an implementation of the preferred embodiment of the present invention;

Figure 7 is a simplified flowchart of the basic method steps that are performed in implementing a preferred embodiment of the present invention in a card-based transaction system; and

Figure 8, consisting of figures 8A and 8B taken together, is a more detailed flowchart of steps performed in the course of a request for authorization in a system implementing the preferred embodiment of the present invention.

Figure 1 is a block diagram showing the participants involved in almost any transaction involving an account established by a user. For the sake of simplicity, the participants are described in the context of a card-based system in which the user (or card holder) makes use of an account by means of a credit card or a debit card. These terms should not be construed as limiting the scope of the invention, which can be employed in any transaction system in which a user authorizes payments to be made from an existing account. The payments may be authorized by the presentation of credit/debit cards or written instruments such as checks, or by furnishing necessary account information orally or electronically. Before any transaction can be conducted a user 10 must establish an account with a card issuer 12 through an exchange 11 of information. The card issuer 12, typically a bank, is interested in receiving information bearing on the card holder's ability and willingness to make account payments. Assuming the card issuer 12 is willing to issue a card, it configures the account by establishing the account number, any Personal Identification Number (PIN), the applicable interest

Petitioner Askeladden LLC
Exhibit 1002 - Page 292 of 350

rate, the account limits, etc. and conveys this information back to the user 10, usually along with the card itself.

For an issued card to have value to the user (now card holder) 10, it must be accepted as a form of payment by a merchant 14 who has independently established a relationship (through an information exchange 15) with an acquirer 16 whose primary responsibility is to see that the merchant receives payments for authorized card transactions. The acquirer 16 is usually the banking institution with whom the merchant does his banking business. The acquirer 16, in turn, must have established a relationship with the card issuer 12, perhaps through an authorization agent 13. The authorization agent 13 may be an integral part of the card issuer's organization or may be a third party with whom the card issuer has contracted to perform the actual transaction authorization function. The information exchange required for establishing the relationship of the relationship between the acquirer 16 and card issuer 12 will probably bypass the authorization agent. When actual transaction information is processed, the acquirer 16 will almost always work directly with the authorization agent 13.

Referring to Figure 2, once the account has been established, about the only further dialog between the card holder 10 and the card issuer 12 is the monthly presentation of an account statement by the card issuer 12 to the card holder 10 and the return of a payment on the account by the card holder 10. The card holder 10 deals directly with the merchant 14 by presenting either the card itself or account information to the merchant as a proposed form of payment for goods or services. The merchant passes the account information on to the acquirer for authorization of the transaction. Unless the acquirer happens to also be the card issuer, the acquirer in turn seeks approval of the transaction from the authorization agent 13, which is either part of or a representative of the card issuer 12. The authorization agent applies a standard set of criteria in deciding whether to authorize the transaction.

When the authorization agent 13 receives the transaction information from acquirer 16, the agent 13 performs certain standard processing operations which potentially will result in denial of authorization without going any further. For example, if the account information received from the merchant identifies a non-existent or closed account, authorization will immediately be denied. Assuming the standard processing operations are

Petitioner Askeladden LLC
Exhibit 1002 - Page 293 of 350

completed successfully, the agent 13 then accesses the account record associated with the received card number. Conventionally, the account record includes a credit limit and the amount of any unpaid charges already levied against the limit.

The authorization agent conventionally approves or disapproves the request for authorization depending on whether the proposed transaction satisfies default criteria, such as whether the proposed transaction will exceed the stated credit limit or will exceed an allowable transaction velocity; that is, a maximum number of transactions over a given period of time. . The default criteria are established solely by the authorization agent and do not take any wishes or desires of a particular account holder into account.

The tenet which underlies the present invention is that no one knows better how a card holder uses or wants to use a credit or debit card than the card holder himself. This tenet is implemented using a system similar to that already described above. Referring to Figure 3, the significant difference is that the card holder's interaction with the card issuer does not essentially end once the account is established. Instead, the card holder is empowered to impose personal authorization criteria (represented by arrow 19) on the card issuer, spelling out the conditions under which the card (or other account) can be used. These personal authorization criteria, which will be discussed in greater detail below, can be changed by the card holder from time to time and are binding on the authorization agent once they are accepted by the card issuer.

Figure 4 illustrates the hardware and network components of a system in which a preferred embodiment of the invention may be implemented. A card holder, using a personal computer 10a or perhaps a telephone 10b, initially establishes an account by communicating with a card issuer, represented as a computer system 12, through an intervening network 20, such as Public Switched Telephone Network (PSTN) or a data network. Once an account has been established, the user may use the same personal computer system 10a or telephone 10b to interact with a merchant through a merchant system 14a or merchant telephone system 14b. The network 21 connecting the user and the merchant may be a PSTN or a public data network such as the Internet. The merchant, in turn, interacts with the acquirer system through another network 23. Assuming the acquirer is a different entity than the card issuer, the

Petitioner Askeladden LLC
Exhibit 1002 - Page 294 of 350

acquirer interacts with the authorization agent 13 through still another set 22 of network connections. A system implementing the invention differs from a conventional system in that the invention allows personal authorization criteria to be provided by the card holder to the authorization agent through the card issuer. Those criteria are then used by the authorization agent in deciding whether to approve or reject a received request for authorization.

The invention is not limited to systems of the type shown in Figure 4. Instead of a conventional telephone or a conventional personal computer system, a user may interact with card issuers and merchants through Internet appliances, Internet-enabled wireless telephones, certain types of Personal Digital Assistants (PDA's) or any other kind of device capable of transmitting and receiving data.

Figure 5 is a block diagram of a system suitable for the authorization agent system. A processor 24 communicates with remaining components of the system through an bus 25. The other components include one or more communications adapters 26 for allowing the authorization agent system to communicate with merchants and card issuers, random access memory 28 and a high capacity memory 32 for providing non-volatile store of data and programs. A number of technologies, including magnetic and optical technologies, may be employed for the high capacity memory. For purposes of the present invention, it is not important which of these technologies is used. For purposes of explaining the invention, the authorization agent system is also shown having an operating system memory 30 for storing the operating system which controls system operation and an application memory 34 for storing application programs to be executed under the control of the operating system. In practice, both the operating system and application programs being executed would likely be stored in random access memory and/or high capacity memory even during execution rather than in separate dedicated memories.

The application of interest stored in application memory 34 is a transaction authorization application 36 which processes proposed transactions received from acquirers through the communications adapters 26. The authorization application 36 would operate in accordance with a basic set of parameters 38 which, as noted earlier, will cause, among other things, a proposed transaction to be rejected if a nonexistent or invalid account is

Petitioner Askeladden LLC
Exhibit 1002 - Page 295 of 350

identified in the transaction information. The authorization application would also make use of a set 40 of default authorization criteria and a set of account records 42 which may contain personal authorization criteria provided by the account holder.

As noted earlier, a card account is normally established in a direct transaction between the card holder and the card issuer. Once the account is established, the card holder rarely deals directly with the card issuer or authorization agent, other than to make payments on the established account. However, according to the preferred embodiment of the present invention, the card holder is empowered to continue to deal directly with the card issuer (or authorization agent) through a direct link. The card holder can use the direct link to provide instructions to the authorization agent as to the conditions under transactions are to be approved. These conditions or personal authorization criteria are stored by the authorization agent as part of the account record.

While a wide variety of personal authorization criteria are possible, a logical dichotomy would be to have one or more sets of criteria for dealings with merchants with whom the card holder is already done business and a different set of criteria for dealings with all other merchants.

For merchants with whom the card holder has already done business, on a card-present and/or a card-not-present basis, the card holder knows whether there is a consistent pattern to the transactions that have already occurred with a particular merchant. If the card holder has a history of making frequent but small purchases from a particular merchant, the card holder may choose to establish personal authorization criteria for that merchant that would enable the authorization agent to approve only relatively small transactions but without regard for how frequently those purchases are made. If the card holder has a history of making relatively few, but high-value purchases from a different merchant, the card holder may choose to establish personal authorization criteria for that merchant which allows a limited number of high-value transactions to be approved over a given period of time. Potentially, a card holder could establish a unique set of authorization criteria for every merchant with whom he or she has done business in the past by identifying each merchant using some sort of merchant number or perhaps even the merchant's phone number and entering the merchant-specific authorization criteria.

Petitioner Askeladden LLC
Exhibit 1002 - Page 296 of 350

The card holder has similar options available in establishing personal authorization criteria for classes of merchants for whom he or she does not wish to enter explicit criteria. For such merchants, the card holder decide to eliminate any risks by instructing the card issuer to never authorize an on-line transaction with any merchant for whom explicit personal authorization criteria have not already been established. Alternatively, the card holder may choose to allow the authorization agent to approve only relatively low-value transactions, possibly with a relatively low limit on the number of any such transactions that will be approved over a given period of time.

Card holders may also choose to establish personal authorization criteria which prevent online or card-not-present transactions from being authorized for merchants outside the card holder's home country. Similarly, the card holder may set up personal criteria which prevent the account from being used to pay for "adult" merchandise or for telephone calls of the type where the called party dispenses psychic advice or "adult" conversation while charging the card account significant amounts per minute of off-hook time.

If a card holder has already personal authorization criteria in mind when the account is initially established, the criteria may be entered and recorded as part of the account setup operation. As the card holder develops or changes his personal authorization criteria for particular merchants, he can contact the card issuer or authorization agent whenever necessary to add new criteria or revise existing criteria. Giving the card holder the power to alter existing criteria makes it possible for the card holder to preauthorize a particular purchase that falls outside the scope of preexisting personal authorization criteria. If the card holder knows that only one such purchase will occur, a parameter may be entered which will cause the preexisting criteria to be restored once the purchase is complete.

Regardless of the details of the authorization criteria provided by the card holder, those criteria will become part of an account record having the general structure shown in Figure 6. The account record will include a set 44 of standard account information including the account number, the identity of the account holder, a personal identification number, and challenge information which the card holder may use to obtain either the same or a new personal identification number if the card holder loses or forgets the old

Petitioner Askeladden LLC
Exhibit 1002 - Page 297 of 350

one. The standard account information will typically also include the credit limit, the amount of credit currently available, and other account information or history which the authorization agent considered worth maintaining.

In systems implementing the present invention, the account record will also include a set 46 of personal authorization criteria established under the control of the card holder. The personal authorization criteria may include global criteria applicable to all merchants, sets of criteria applicable to explicitly identified merchants (that is, merchants of record), and sets of criteria applicable to merchants for whom no explicit criteria has been entered (that is, new merchants). It should be noted that the term "new merchants" as used here can include not only merchants with whom the card hold has never done business as well as merchants with whom the card holder has done business in the past but for whom no merchant-explicit personal authorization criteria have been entered.

The set 46 of information may also include instructions as to what should happen if the authorization agent disapproves a proposed transaction. Such instructions are identified in the drawings as a Consequences of Denial protocol and will spell out the steps the card holder wants the card issuer to take following a denial. A conservative card holder may want the card issuer to "freeze" the account following any denial for any reason. A less conservative card holder may conclude there is no reason to freeze the account if the denial was for some relatively innocuous reason, such as the transaction would have caused the credit limit to be exceeded.

The Consequences of Denial Protocol may also spell out the conditions for notifying the card holder of a denial. The card holder may agree that notification of the denial and reasons for it can be provided through the merchant or directly via telephone contact, e-mail, separate letter or (for trivial denials) only as part of the next statement received from the card issuer. One advantage of allowing the merchant to provide immediate feedback of a notice of denial is that the card holder would have the immediate opportunity to revise the personal authorization criteria in a way that would allow the transaction to continue. For obvious security reasons, the card holder would be likely to perform the revision in a separate session with the card issuer or authorization agent.

Petitioner Askeladden LLC
Exhibit 1002 - Page 298 of 350

Figure 7 is a flowchart of basic method steps that are performed in carrying out the present invention. Some of these steps have already been described but will repeated here for the sake of completeness. In an initial step 48, the card holder and the card issuer perform the steps needed to initially establish the card account, including any credit limit and any system-level criteria which the authorization agent will employ without regard to whether personal authorization criteria have been established. Personal authorization criteria will be provided by the card holder to the card issuer or authorization agent in one or more iterations of a step 50. As noted earlier, personal authorization criteria may be entered when the account is established or later at the discretion of the card holder.

When the card (or account information) is used during a later transaction, the merchant to whom it is presented requests authorization (operation 52) for the transaction in the conventional way. The merchant will neither know nor care whether the card holder has provided personal authorization criteria specific to the requesting merchant. When the request for authorization is received, the authorization agent performs system-level operations 54 (e.g., is there a valid account) before attempting to recover account-specific information, Assuming the request for authorization survives the system-level checks, the authorization agent then retrieves the account record for the relevant account, determines whether the account contains personal authorization criteria, and processes the transaction accordingly in operation 56. If the card holder has entered personal authorization criteria, the transaction is processed using the recorded criteria. If no personal authorization criteria is found, the card issuer applies standard or default criteria in deciding whether to approve the transaction.

Figure 8 is a more detailed flowchart of steps that may be performed by an authorization agent in executing a preferred implementation of the present invention. The method is initiated in step 58 when a request for an authorization is received. System-level tests 60 are performed. If the request fails those tests, the request is denied in a step 62 and any existing system-level Consequences-of-Denial protocol is implemented in a step 64. Assuming the request survives the system-level tests, the appropriate account record is identified in step 66 using information received in the request for authorization. Once the account is identified and the account record is retrieved, the card issuer tests the proposed transaction against a set of globally applicable criteria. The global

Petitioner Askeladden LLC
Exhibit 1002 - Page 299 of 350

criteria will generally always include a test 68 whether the proposed transaction will cause the credit limit of the identified account to be exceeded, may include a test 70 whether the proposed transaction will a monetary velocity limit (maximum amount chargeable over a given period of time) to be exceeded and/or a test 72 whether the proposed transaction will cause a numeric velocity limit (maximum number of transactions allowed over a given period of time) to be exceeded. If any of these checks yields a positive result, the request for authorization of the proposed transaction is denied in operation 62 and any existing account-level consequence-of-denial protocol is implemented.

Assuming that all the global tests are satisfied, the next step in the method is a check 74 whether the account contains any personal authorization criteria. If no such criteria is found, the proposed transaction is authorized in step 76. However, if the account does contain personal authorization criteria, the proposed transaction is tested against such criteria beginning with a check 78 of whether the merchant requesting authorization has actually seen the credit card; that is, whether the card holder and the merchant are engaged in a face-to-face transaction or a remote transaction.

A card holder may decide that he or she the card to be used only for face-to-face transactions, making that one of the personal authorization criteria provided to the card issuer. If the card holder has done that and if the merchant has not seen the card, a test 80 will yield a negative result which will result in denial of authorization in step 82. Any consequence-of-denial protocol specified by the card holder will be implemented in step 84.

If the merchant has seen the card or card holder has authorized at least some card-not-present transactions, the next step 86 is a determination whether any personal authorization criteria specific to the calling merchant are of record in the account information. For simplicity, personal authorization criteria specific to a particular merchant is identified as MAC or Merchant Authorization Criteria. If MAC exist for the calling merchant, they are retrieved in step 88. The proposed transaction is tested against the retrieved MAC in step 90. If the transaction conforms, it is authorized in step 92. If the transaction does not conform to the retrieved MAC, the

request for authorization is denied in step 96 and any specified consequence of denial protocol is implemented in step 98.

If the test performed at step 86 does not find any MAC for the calling merchant, a check 94 is made as to whether the account record includes instructions or criteria for dealing with other merchants. If no such instructions are found, authorization is denied in step 96 and any specified personalized consequence-of-denial protocol is implemented in step 98.

If the card holder has provided instructions for dealing with merchants for whom no MAC records exist, those instructions are retrieved in step 100 and used to test the proposed transaction in step 102. If the proposed transaction fails any of the tests, the request for authorization is denied. If the proposed transaction satisfies all criteria provided by the card holder, the transaction is authorized in step 104.

The preferred embodiment of the present invention imposes no constraints on how the card holder elects to do business with merchants, on how merchants do business with acquirers or on how acquirers do business with authorization agents. Similarly, it does not require that a card holder be limited to using a personal computer system to enter personal authorization criteria. The card holder may use an Internet enabled telephone or even a conventional telephone to provide the criteria to the card issuer through a public telephone network connection.

In fact, as noted earlier, there is no requirement that the invention be limited to remote transactions. The value of the system even for face-to-face transactions is apparent in the description of Figure 8 above. Finally, while most of the discussion has been in terms of use of credit or debit cards, the invention has value for different kinds of accounts, including conventional checking accounts and so-called positive-pay accounts.

CLAIMS

1. A method for enhancing the security of account-based transactions comprising the steps of:

receiving a request for authorization from a merchant, the request for authorization including at least an account number and the amount of the transaction;

identifying an account record associated with the received account number;

determining from the account record personal authorization criteria provided previously by the owner of the identified account; and

using the personal authorization criteria to process the request for authorization.

2. A method as set forth in claim 1 wherein the using step further includes the steps of:

processing the request for authorization in accordance with any available personal authorization criteria relating to merchant-independent properties of the transaction;

where the request cannot be processed using only personal authorization criteria relating to merchant-independent properties of the transaction, processing the transaction in accordance with any available merchant-specific criteria, otherwise determining whether the account record contains personal authorization criteria for dealing with authorizations requested by previously-unidentified merchants; and

where criteria are found dealing with previously-unidentified merchants, processing the request for authorization in accordance with said criteria.

3. A method as set forth in either claim 1 or claim 2 further including the steps of:

denying the request for authorization where the transaction fails to comply with applicable criteria;

implementing a consequence-of-denial protocol upon denial of the request, said protocol specifying the actions to be taken upon denial.

4. A method as set forth in claim 3 further including the step of notifying the account owner of the denial of authorization in accordance with notification requirements set forth in the consequence-of-denial protocol.

Petitioner Askeladden LLC
Exhibit 1002 - Page 302 of 350

5. A method as set forth in claim 4 wherein the personal authorization criteria relating to properties of the transaction includes criteria relating to the location of merchants for whom transactions may be authorized.

6. A method as set forth in claim 4 wherein the personal authorization criteria relating to properties of the transaction includes criteria relating to classes of goods or services for which transactions may be authorized.

7. A system for enhancing the security of account-based transactions comprising:

means for receiving a request for authorization from a merchant, the request for authorization including at least an account number and the amount of the transaction;

means for identifying an account record associated with the received account number;

means for determining from the account record personal authorization criteria provided previously by the owner of the identified account; and

means for using the personal authorization criteria to process the request for authorization.

8. A computer program product stored on a computer readable storage medium for, when run on a computer system, carrying out the method of any preceding method claim.

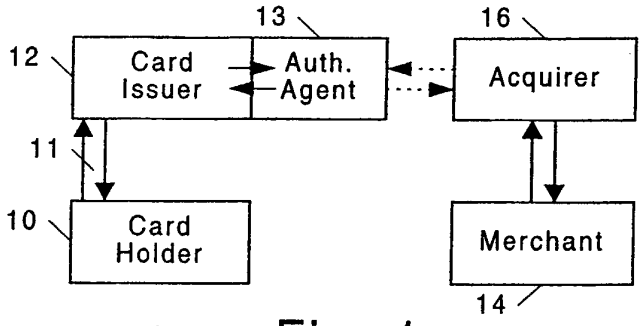


Fig. 1

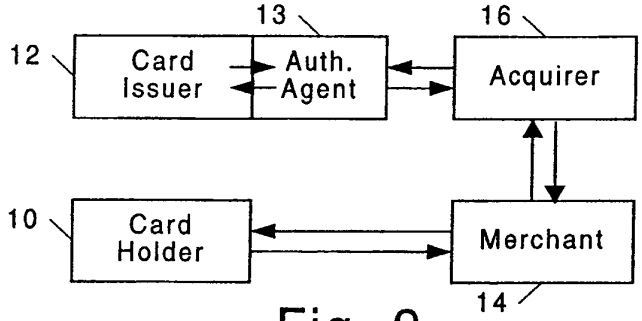


Fig. 2

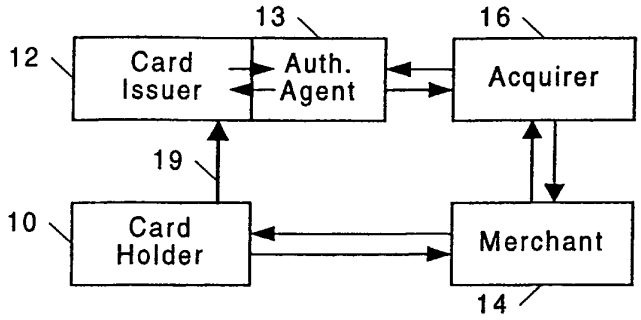


Fig. 3

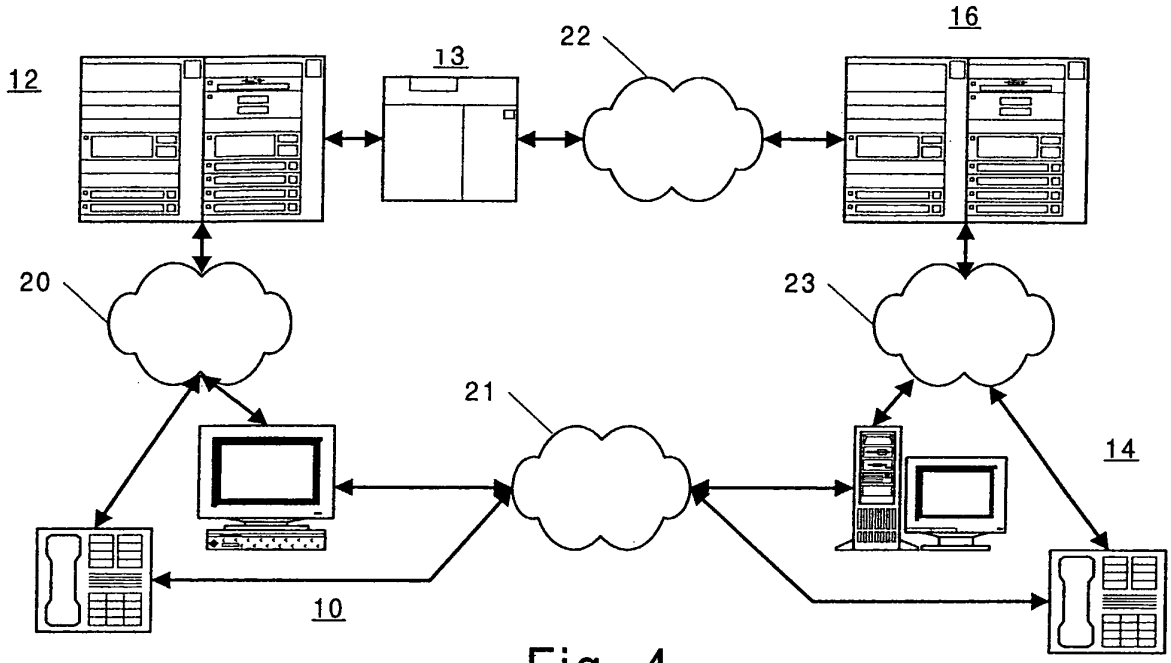

12
13
22
16
20
23
21
14
10

Fig. 4

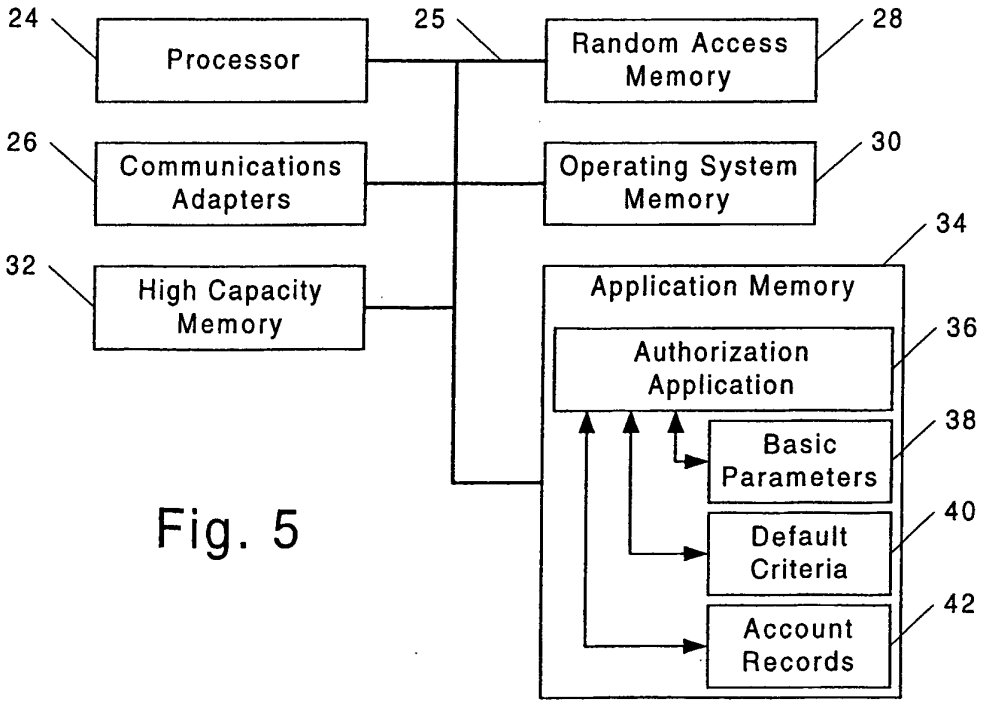

24
Processor
25
Random Access Memory
28
26
Communications Adapters
Operating System Memory
30
32
High Capacity Memory
34
Application Memory
Authorization Application
36
Basic Parameters
38
Default Criteria
40
Account Records
42

Fig. 5

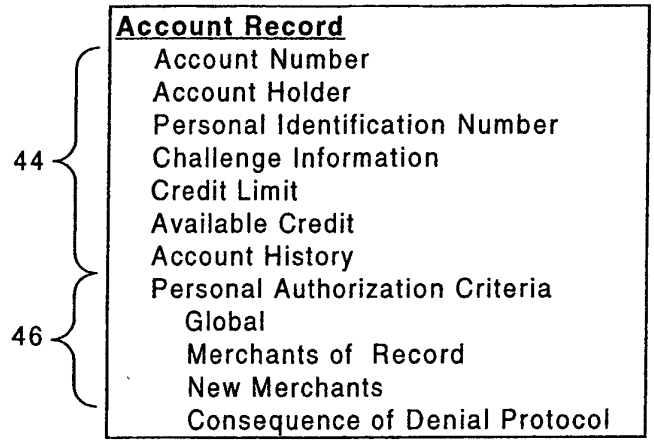

Account Record
Account Number
Account Holder
Personal Identification Number
Challenge Information
Credit Limit
Available Credit
Account History
Personal Authorization Criteria
Global
Merchants of Record
New Merchants
Consequence of Denial Protocol
44
46

Fig. 6

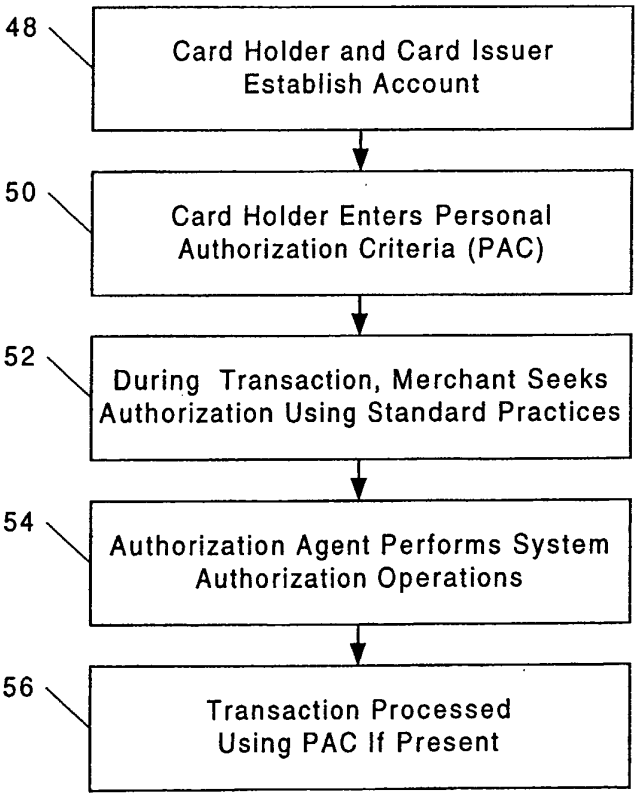

48
Card Holder and Card Issuer Establish Account
50
Card Holder Enters Personal Authorization Criteria (PAC)
52
During Transaction, Merchant Seeks Authorization Using Standard Practices
54
Authorization Agent Performs System Authorization Operations
56
Transaction Processed Using PAC If Present

Fig. 7

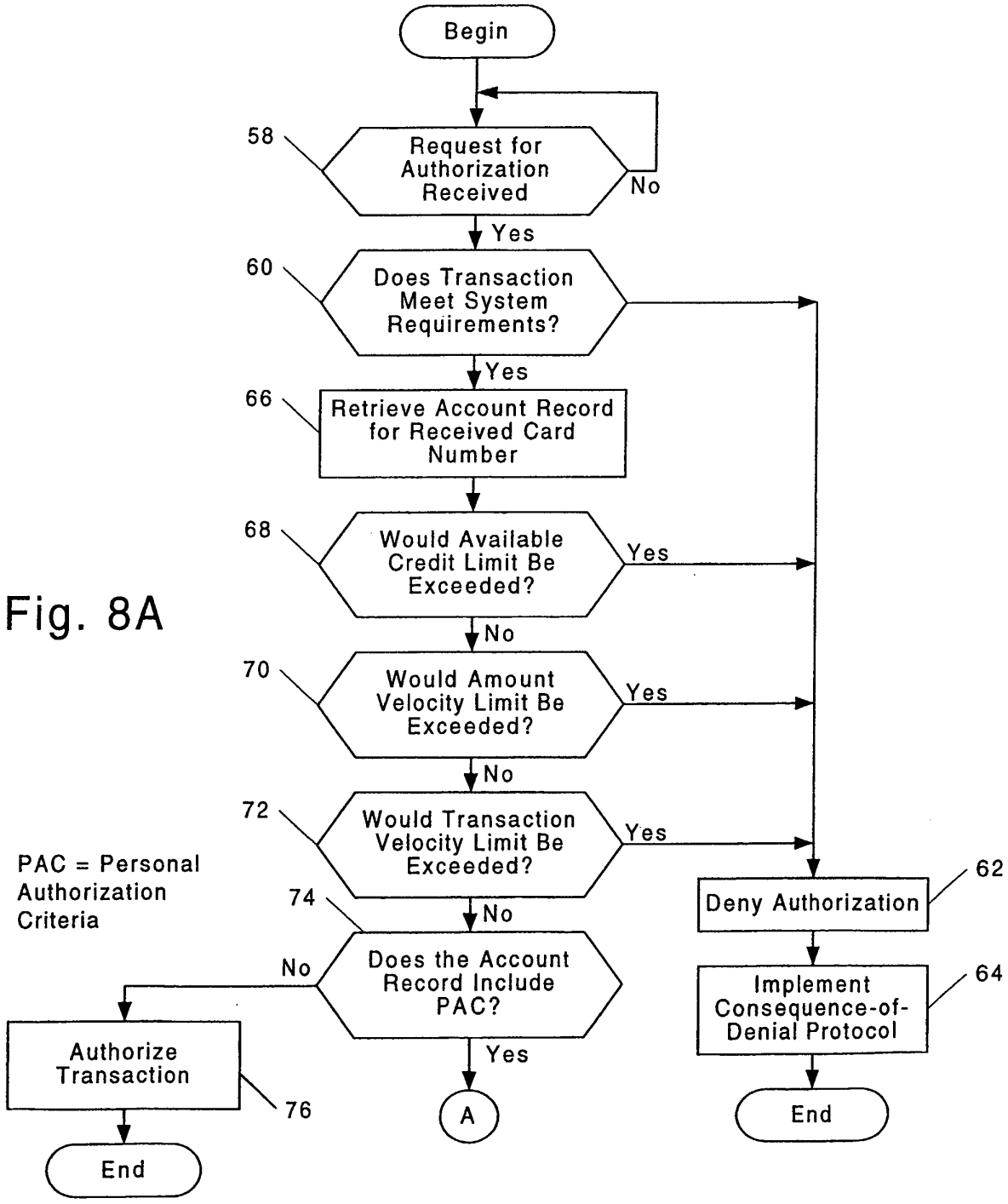

Begin
58
Request for Authorization Received
No
Yes
60
Does Transaction Meet System Requirements?
Yes
66
Retrieve Account Record for Received Card Number
68
Would Available Credit Limit Be Exceeded?
Yes
No
70
Would Amount Velocity Limit Be Exceeded?
Yes
No
72
Would Transaction Velocity Limit Be Exceeded?
Yes
No
74
Does the Account Record Include PAC?
No
Yes
Authorize Transaction
76
End
A
Deny Authorization
62
Implement Consequence-of-Denial Protocol
64
End
PAC = Personal Authorization Criteria

Fig. 8A

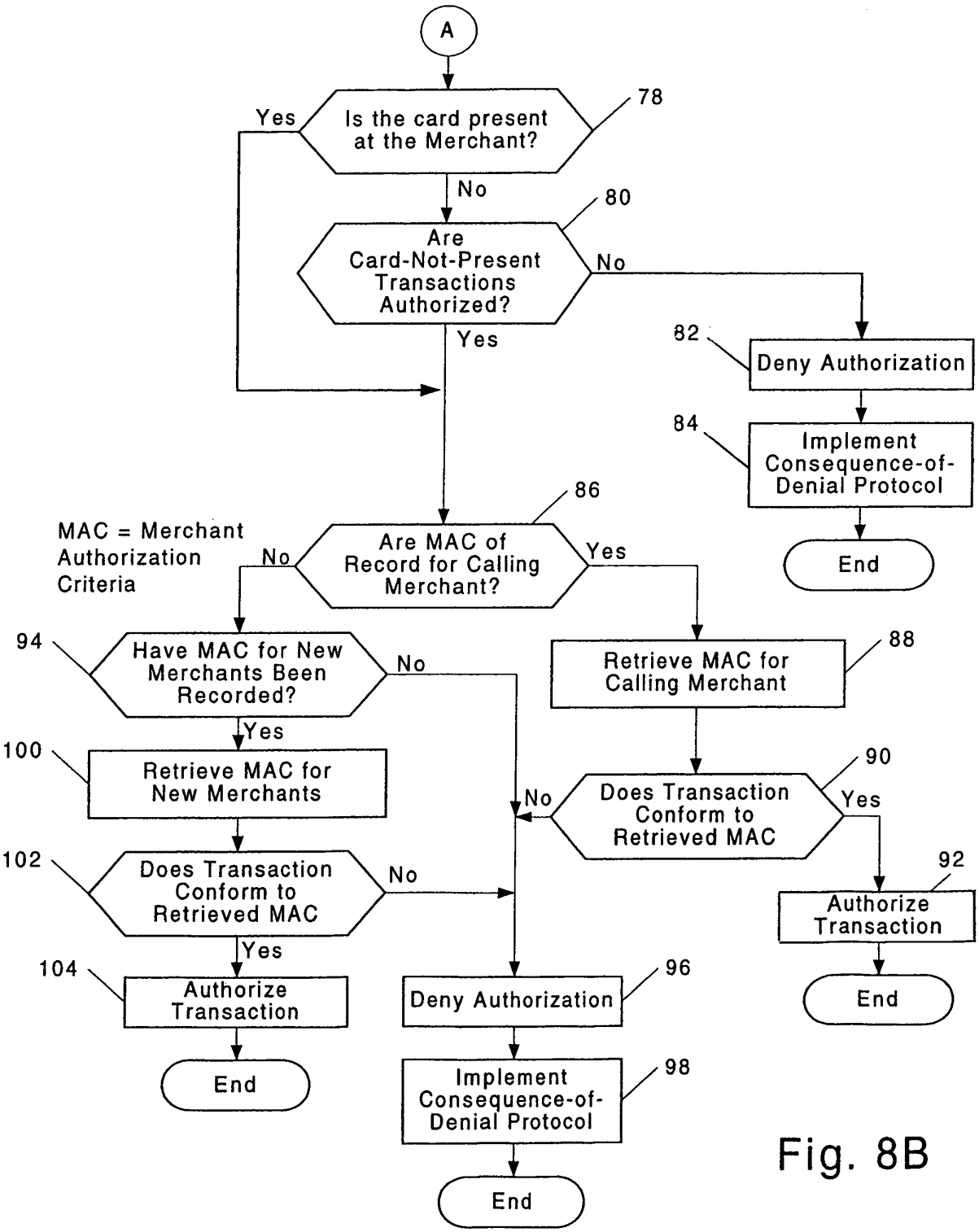

A
Is the card present at the Merchant?
78
Yes
No
Are Card-Not-Present Transactions Authorized?
80
No
Yes
82
Deny Authorization
84
Implement Consequence-of-Denial Protocol
End
MAC = Merchant Authorization Criteria
Are MAC of Record for Calling Merchant?
86
No
Yes
94
Have MAC for New Merchants Been Recorded?
No
Yes
100
Retrieve MAC for New Merchants
102
Does Transaction Conform to Retrieved MAC
No
Yes
104
Authorize Transaction
End
Retrieve MAC for Calling Merchant
88
Does Transaction Conform to Retrieved MAC
90
No
Yes
92
Authorize Transaction
End
Deny Authorization
96
Implement Consequence-of-Denial Protocol
98
End

Fig. 8B

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/974,462	Filing Date 08/23/2013	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 01/14/2014

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 19	Minus	** 23	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/PAULA MCCRAY STANLEY/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24131 7590 03/28/2014
LERNER GREENBERG STEMER LLP
P O BOX 2480
HOLLYWOOD, FL 33022-2480

EXAMINER
KIM, AHSHIK

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 03/28/2014

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/974,462	08/23/2013	GERRY CALABRESE	W-9001D3	4957

TITLE OF INVENTION: TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	06/30/2014

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

Petitioner Askeladden LLC
Exhibit 1002 - Page 310 of 350

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

24131 7590 03/28/2014
LERNER GREENBERG STEMER LLP
P O BOX 2480
HOLLYWOOD, FL 33022-2480

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/974,462	08/23/2013	GERRY CALABRESE	W-9001D3	4957

TITLE OF INVENTION: TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	06/30/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
KIM, AHSHIK	2876	235-380000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Petitioner Askeladden LLC
Exhibit 1002 - Page 311 of 350

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/974,462	08/23/2013	GERRY CALABRESE	W-9001D3	4957

24131 7590 03/28/2014

LERNER GREENBERG STEMER LLP
P O BOX 2480
HOLLYWOOD, FL 33022-2480

EXAMINER	
KIM, AHSHIK	

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 03/28/2014

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 02/11)

Petitioner Askeladden LLC
Exhibit 1002 - Page 312 of 350

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/974,462	Applicant(s) CALABRESE ET AL.	
	Examiner AHSHIK KIM	Art Unit 2876	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment filed on 1/14/14*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-9 and 14-23*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 1/14/14
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/AHSHIK KIM/
Primary Examiner, Art Unit 2876

Petitioner Askeladden LLC
Exhibit 1002 - Page 314 of 350

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13974462
	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	2876
	Examiner Name	Ahshik Kim
	Attorney Docket Number	W-9001D3

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8296228	B1	2012-10-23	Kloor	
	2	7427021	B2	2008-09-23	Kemper et al.	Corresponds to EP 2287793 A1

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010051920	A1	2001-12-13	Joao et al.	
	2	20060085337	A1	2006-04-20	Conforti et al.	Corresponds to WO 2005031541 A2
	3	20030105707	A1	2003-06-05	Audebert et al.	Corresponds to WO 03046778 A2
	4	20020161724	A1	2002-10-31	Peters	Corresponds to WO 02082392 A2

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.K./

Receipt date: 01/14/2014	Application Number	13974462 13974462 - GAU: 2876
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	2876
(Not for submission under 37 CFR 1.99)	Examiner Name	Ahshik Kim
	Attorney Docket Number	W-9001D3

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	9914711	WO	A2	1999-03-25	Andrasev	Published in the English language	☐
	2	2823882	FR	A1	2002-10-25	Inventor not named	English abstract	☒
	3	2005031541	WO	A2	2005-04-07	Conforti et al.	Published in the English language and corresponds to US 20060085337 A1	☐
	4	1067492	EP	A3	2001-01-17	Palmquist	Published in the English language	☐
	5	2287793	EP	A1	2011-02-23	Kemper et al.	Published in the English language and corresponds to US 7427021 B2	☐
	6	03046778	WO	A2	2003-06-05	Audebert et al.	Published in the English language and corresponds to US20030105707 A1	☐
	7	0193213	WO	A2	2001-12-06	Mani et al.	Published in the English language	☐
	8	02082392	WO	A2	2002-10-17	Peters	Published in the English language and corresponds to US 20020161724 A1	☐

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.K./

Receipt date: 01/14/2014	Application Number	13974462 13974462 - GAU: 2876
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	2876
	Examiner Name	Ahshik Kim
	Attorney Docket Number	W-9001D3

	1	SAXENA ET AL., "MMPS: A Versatile Mobile-to-Mobile Payment System", Proceedings of the International Conference on Mobile Business (ICMB'05), 2005, IEEE, pages 1-6	☐
	~~2~~	~~2.1 Electronic Payment System, 23 pages~~	☐
	3	WOLFGANG WOPPERER, "Fraud Risks in E-commerce Transactions", The Geneva Papers on Risk and Insurance, Vol. 27 No. 3 (July 2002), pages 383-394	☐
	~~4~~	~~WRONA ET AL., "Mobile Payments - State-of-the-Art and Open Problems",~~ Ericsson Research, Germany, 13 pages	☐
	5	AMIR HERZBERG, "Payments and Banking with Mobile Personal Devices", Communications of the ACM, May 2003, Vol. 46, No. 5, pages 53-58	☐
	6	~~GORDON-AGNEW, Chapter 10 Secure Electronic Transactions: Overview,~~ Capabilities, and Current Status, pages 211-226	☐
	7	WANG ET AL., "Secure Wireless Payment Protocol", Proceedings of International Conference on Wireless Networks (ICWN), Las Vegas, Nevada, 2003 pages 1-7	☐
	8	CAROL L. CLARK, "Shopping without cash: The emergence of the e-purse", 4Q/2005, Economic Perspectives, pages 34-51	☐
	9	HALL ET AL., "WPP: A Secure Payment Protocol for Supporting Credit- And Debit-Card Transactions Over Wireless Networks, IEEE International Conference on Telecomuniations (ICT), Bucharest, June 2001, pages 1-6	☐
	10	MARK E. PETERS, "Emerging eCommerce Credit and Debit Card Protocols", Proceedings of the 3rd International Symposium on Electronic Commerce (ISEC'02), 2002, IEEE Computer Society, 8 pages	☐
	11	KARNOUSKOS ET AL., "Mobile Payment: A Journey Through Existing Procedures and Standardization Initiatives" IEEE Communications Surveys, Fouth Quarter 2004, Volume 6, No. 4, pages 44-66	☐

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.K./

Receipt date: 01/14/2014	Application Number	13974462 13974462 - GAU: 2876
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	2876
	Examiner Name	Ahshik Kim
	Attorney Docket Number	W-9001D3

	12	VORAPRANEE KHU-SMITH, "Enhancing the security of electronic commerce transactions", Technical Report RHUL-MA-2003-7, June 2003, Royal Holloway Univesity of London, Department of Mathematics, England, 183 pages	☐
	13	CAI ET AL., "Authorization Mechanisms for Mobile Commerce Implementations in Enhanced Prepaid Solutions", Bell Labs Technical Journal 8(4), 2004, pages 121-131	☐
	14	XINGJIANG SONG, "Mobile Payment and Security", Article in T-110.501 Seminar on Network Security 2001 ISBN 951-22-5807-2, Publications in Telecommunications Software and Multimedia TML-C7 ISSN 1455-9749, Helsinky University of Technology, Telecommunications Software and Multimedia Laboratory, 15 pages	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Ahshik Kim/	Date Considered	03/22/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Applicant is required to show date for the crossed items in the IDS.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.K./

Petitioner Askeladden LLC
Exhibit 1002 - Page 318 of 350

Receipt date: 01/14/2014	Application Number	13974462	13974462 - GAU: 2876
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2013-08-23	
	First Named Inventor	Gerry Calabrese et al.	
	Art Unit	2876	
	Examiner Name	Ahshik Kim	
	Attorney Docket Number	W-9001D3	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Werner H. Stemer/	Date (YYYY-MM-DD)	2014-01-14
Name/Print	Werner H. Stemer	Registration Number	34956

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.K./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.K./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13974462	CALABRESE ET AL.
	Examiner	**Art Unit**
	AHSHIK KIM	2876

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/01/2013	03/22/2014							
	1	=	=							
	2	=	=							
	3	=	=							
	4	=	=							
	5	=	=							
	6	=	=							
	7	=	=							
	8	=	=							
	9	=	=							
	10	✓	-							
	11	✓	-							
	12	✓	-							
	13	✓	-							
	14	=	=							
	15	=	=							
	16	=	=							
	17	=	=							
	18	=	=							
	19	=	=							
	20	=	=							
	21	=	=							
	22	=	=							
	23	=	=							

Petitioner Askeladden LLC
Exhibit 1002 - Page 321 of 350

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13974462	CALABRESE ET AL.
	Examiner	Art Unit
	AHSHIK KIM	2876

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
235	380	12/1/2013	ak
	382	12/1/2013	ak
	379	12/1/2013	ak
705	77		ak

SEARCH NOTES		
Search Notes	Date	Examiner
See attached EAST search history	12/1/2013	ak
Reviewed parent cases	12/1/2013	ak
Updated Search	3/22/2014	ak

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
Same as above (see Searched)		3/22/2014	ak

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13974462	CALABRESE ET AL.
	Examiner	**Art Unit**
	AHSHIK KIM	2876

CPC		
Symbol	**Type**	**Version**

CPC Combination Sets				
Symbol	**Type**	**Set**	**Ranking**	**Version**

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	19	
/AHSHIK KIM/ Primary Examiner.Art Unit 2876	03/22/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Petitioner Askeladden LLC
Exhibit 1002 - Page 323 of 350

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13974462	CALABRESE ET AL.
	Examiner	**Art Unit**
	AHSHIK KIM	2876

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
235	380	G	0	6	K	5 / 00 (2006.01.01)						
CROSS REFERENCE(S)												
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)											
235	382											

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 19	
/AHSHIK KIM/ Primary Examiner.Art Unit 2876 (Primary Examiner)	03/22/2014 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13974462	CALABRESE ET AL.
	Examiner	**Art Unit**
	AHSHIK KIM	2876

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	13	17												
2	2	14	18												
3	3	15	19												
4	4	16	20												
5	5	17	21												
6	6	18	22												
7	7	19	23												
8	8														
9	9														
	10														
	11														
	12														
	13														
10	14														
11	15														
12	16														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 19	
/AHSHIK KIM/ Primary Examiner.Art Unit 2876 (Primary Examiner)	03/22/2014 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Petitioner Askeladden LLC
Exhibit 1002 - Page 325 of 350

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13974462
	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	2876
	Examiner Name	Ahshik Kim
	Attorney Docket Number	W-9001D3

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8229854	B2	2012-07-24	Stephen, et al. (Kavanagh)	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								Add

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13974462
	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	2876
	Examiner Name	Ahshik Kim
	Attorney Docket Number	W-9001D3

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13974462
	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	2876
	Examiner Name	Ahshik Kim
	Attorney Docket Number	W-9001D3

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Werner H. Stemer/	Date (YYYY-MM-DD)	2014-04-10
Name/Print	Werner H. Stemer	Registration Number	34956

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Petitioner Askeladden LLC
Exhibit 1002 - Page 329 of 350

Electronic Patent Application Fee Transmittal

Application Number:	13974462
Filing Date:	23-Aug-2013
Title of Invention:	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD
First Named Inventor/Applicant Name:	GERRY CALABRESE
Filer:	Werner H. Stemer/Birgit Bartell
Attorney Docket Number:	W-9001D3

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	18729568
Application Number:	13974462
International Application Number:	
Confirmation Number:	4957
Title of Invention:	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD
First Named Inventor/Applicant Name:	GERRY CALABRESE
Customer Number:	24131
Filer:	Werner H. Stemer/Michelle Janca
Filer Authorized By:	Werner H. Stemer
Attorney Docket Number:	W-9001D3
Receipt Date:	10-APR-2014
Filing Date:	23-AUG-2013
Time Stamp:	16:26:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$90
RAM confirmation Number	3111
Deposit Account	121099
Authorized User	GREENBERG, LAURENCE A

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	W-9001D3-IDS.pdf	612301 6325663ef86838266b824b6f4202bdb3dc908124	no	4
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30356 34ac569bf067f432d3606b33080253dbf4e0e334	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	642657		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/974,462	08/23/2013	GERRY CALABRESE	W-9001D3	4957

24131 7590 06/02/2014

LERNER GREENBERG STEMER LLP
P O BOX 2480
HOLLYWOOD, FL 33022-2480

EXAMINER	
KIM, AHSHIK	

ART UNIT	PAPER NUMBER
2876	

NOTIFICATION DATE	DELIVERY MODE
06/02/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

boxoa@patentusa.com
docket@patentusa.com

Petitioner Askeladden LLC
Exhibit 1002 - Page 334 of 350

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
13/974,462	23 August, 2013	CALABRESE ET AL.	W-9001D3

LERNER GREENBERG STEMER LLP
P O BOX 2480
HOLLYWOOD, FL 33022-2480

EXAMINER	
AHSHIK KIM	
ART UNIT	PAPER
2876	20140527

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

IDS filed on 4/10/14 is considered. Signed PTO-1449 is enclosed.

/AHSHIK KIM/
Primary Examiner, Art Unit 2876

PTO-90C (Rev.04-03)

Receipt date: 04/10/2014
Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13974462
	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
	Art Unit	2876
	Examiner Name	Ahshik Kim
	Attorney Docket Number	W-9001D3

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8229854	B2	2012-07-24	Stephen, et al. (Kavanagh)	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.K./

Receipt date: 04/10/2014	Application Number	13974462
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
(Not for submission under 37 CFR 1.99)	Art Unit	2876
	Examiner Name	Ahshik Kim
	Attorney Docket Number	W-9001D3

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Ahshik Kim/	Date Considered	05/27/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.K./

Receipt date: 04/10/2014	Application Number	13974462
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2013-08-23
	First Named Inventor	Gerry Calabrese et al.
(Not for submission under 37 CFR 1.99)	Art Unit	2876
	Examiner Name	Ahshik Kim
	Attorney Docket Number	W-9001D3

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Werner H. Stemer/	Date (YYYY-MM-DD)	2014-04-10
Name/Print	Werner H. Stemer	Registration Number	34956

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.K./

Receipt date: 04/10/2014

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.K./

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

24131 7590 03/28/2014
LERNER GREENBERG STEMER LLP
P O BOX 2480
HOLLYWOOD, FL 33022-2480

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/974,462	08/23/2013	GERRY CALABRESE	W-9001D3	4957

TITLE OF INVENTION: TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	06/30/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
KIM, AHSHIK	2876	235-380000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Werner H. Stemer
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Calabrese Stemer LLC

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Hollywood, FL

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
- ☒ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ☐ A check is enclosed.
- ☒ Payment by credit card. Form PTO-2038 is attached.
- ☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 12-1099 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ☐ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ☐ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature [signature] Date June 12, 2014

Typed or printed name WERNER H. STEMER Registration No. 34,956

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Petitioner Askeladden LLC
Exhibit 1002 - Page 340 of 350

Electronic Patent Application Fee Transmittal

Application Number:	13974462
Filing Date:	23-Aug-2013
Title of Invention:	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD
First Named Inventor/Applicant Name:	GERRY CALABRESE
Filer:	Werner H. Stemer/Michelle Janca
Attorney Docket Number:	W-9001D3

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	480	480
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**480**

Electronic Acknowledgement Receipt

EFS ID:	19281655
Application Number:	13974462
International Application Number:	
Confirmation Number:	4957
Title of Invention:	TRANSACTION NOTIFICATION AND AUTHORIZATION METHOD
First Named Inventor/Applicant Name:	GERRY CALABRESE
Customer Number:	24131
Filer:	Werner H. Stemer/Michelle Janca
Filer Authorized By:	Werner H. Stemer
Attorney Docket Number:	W-9001D3
Receipt Date:	12-JUN-2014
Filing Date:	23-AUG-2013
Time Stamp:	09:30:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$480
RAM confirmation Number	9866
Deposit Account	121099
Authorized User	GREENBERG, LAURENCE A

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	W9001D3.pdf	157492 4a3f99584bfdcc4555e11cc3363889aae2193542	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30496 1e8db4da94350bca0a78ea7553818e241c45f1d0	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	187988		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/974,462	07/22/2014	8783564	W-9001D3	4957

24131 7590 07/02/2014

LERNER GREENBERG STEMER LLP
P O BOX 2480
HOLLYWOOD, FL 33022-2480

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

GERRY CALABRESE, SOUTHWEST RANCHES, FL;
WERNER STEMER, FORT LAUDERDALE, FL;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY.DOCKET NO./TITLE	REQUEST ID
13/974,462	08/23/2013	GERRY CALABRESE	W-9001D3	85807

Acknowledgement of Loss of Entitlement to Entity Status Discount

The entity status change request below filed through Private PAIR on 04/16/2019 has been accepted.

CERTIFICATIONS:

Change of Entity Status:

X Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be notification of loss of entitlement to small or micro entity status, as applicable.

This portion must be completed by the signatory or signatories making the entity status change in accordance with 37 CFR 1.4(d)(4).

Signature:	/LAURENCE A GREENBERG/
Name:	LAURENCE A GREENBERG
Registration Number:	29308

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-CV-00386	10/4/2022	Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
CALABRESE STEMER LLC	COMERICA BANK

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,783,564 B2	7/22/2014	CALABRESE STEMER LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court WESTERN DISTRICT OF TEXAS on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
1:23-CV-00231	3/1/2023	WESTERN DISTRICT OF TEXAS

PLAINTIFF	DEFENDANT
CALABRESE STEMER LLC	WISE US INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,783,564 B2	7/22/2014	CALABRESE STEMER LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
PHILIP J. DEVLIN		03/06/2023

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court WESTERN DISTRICT OF TEXAS on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
1:23-CV-00231	3/1/2023	WESTERN DISTRICT OF TEXAS

PLAINTIFF	DEFENDANT
CALABRESE STEMER LLC	WISE US INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,783,564 B2	7/22/2014	CALABRESE STEMER LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT
See attached Order re Voluntary Dismissal

CLERK	(BY) DEPUTY CLERK	DATE
PHILIP J. DEVLIN	Jay Vicha	06/08/2023

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

CALABRESE STEMER LLC,	§	
	§	
Plaintiff,	§	
	§	
v.	§	1:23-CV-231-DII
	§	
WISE US INC.,	§	
	§	
Defendant.	§	

ORDER

On June 7, 2023, Plaintiff dismissed all claims in this case without prejudice. (Dkt. 24). Rule 41(a)(1)(A)(i) allows a plaintiff to voluntarily dismiss an action without a court order by filing a notice of dismissal before the opposing party serves an answer or a motion for summary judgment. Fed. R. Civ. P. 41(a)(1)(A)(i). Defendant has not served an answer or motion for summary judgment. Plaintiff's notice is therefore "self-effectuating and terminates the case in and of itself; no order or other action of the district court is required." *In re Amerijet Int'l, Inc.*, 785 F.3d 967, 973 (5th Cir. 2015), *as revised* (May 15, 2015).

As nothing remains to resolve, **IT IS ORDERED** that the case is **CLOSED**.

SIGNED on June 8, 2023.

ROBERT PITMAN
UNITED STATES DISTRICT JUDGE