US 20040158532A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2004/0158532 A1

Breck et al. (43) Pub. Date: Aug. 12, 2004

(54) SYSTEM FOR FACILITATING A TRANSACTION

(76) Inventors: **Lydia Breck**, New York, NY (US); **Jessica Zoob**, New York, NY (US); **Glen Salow**, Holmdel, NJ (US); **Fred Bishop**, Phoenix, AZ (US); **William Schwarz**, Scottsdale, AZ (US); **Elliot Glazer**, Chesterfield, VA (US); **David Johnstone**, Cave Creek, AZ (US); **Katie Cunningham**, New York, NY (US); **Anant Nambiar**, New Rochelle, NY (US); **Jan Nunney Belt**, Scottsdale, AZ (US); **Martin Wittwer**, New York, NY (US); **David Armes**, Phoenix, AZ (US); **Christina Chow**, Phoenix, AZ (US)

Correspondence Address:
SNELL & WILMER
ONE ARIZONA CENTER
400 EAST VAN BUREN
PHOENIX, AZ 850040001

(21) Appl. No.: **10/787,716**

(22) Filed: **Feb. 26, 2004**

Related U.S. Application Data

(63) Continuation of application No. 09/800,461, filed on Mar. 7, 2001.

(60) Provisional application No. 60/187,620, filed on Mar. 7, 2000. Provisional application No. 60/200,625, filed on Apr. 28, 2000. Provisional application No. 60/213,323, filed on Jun. 22, 2000.

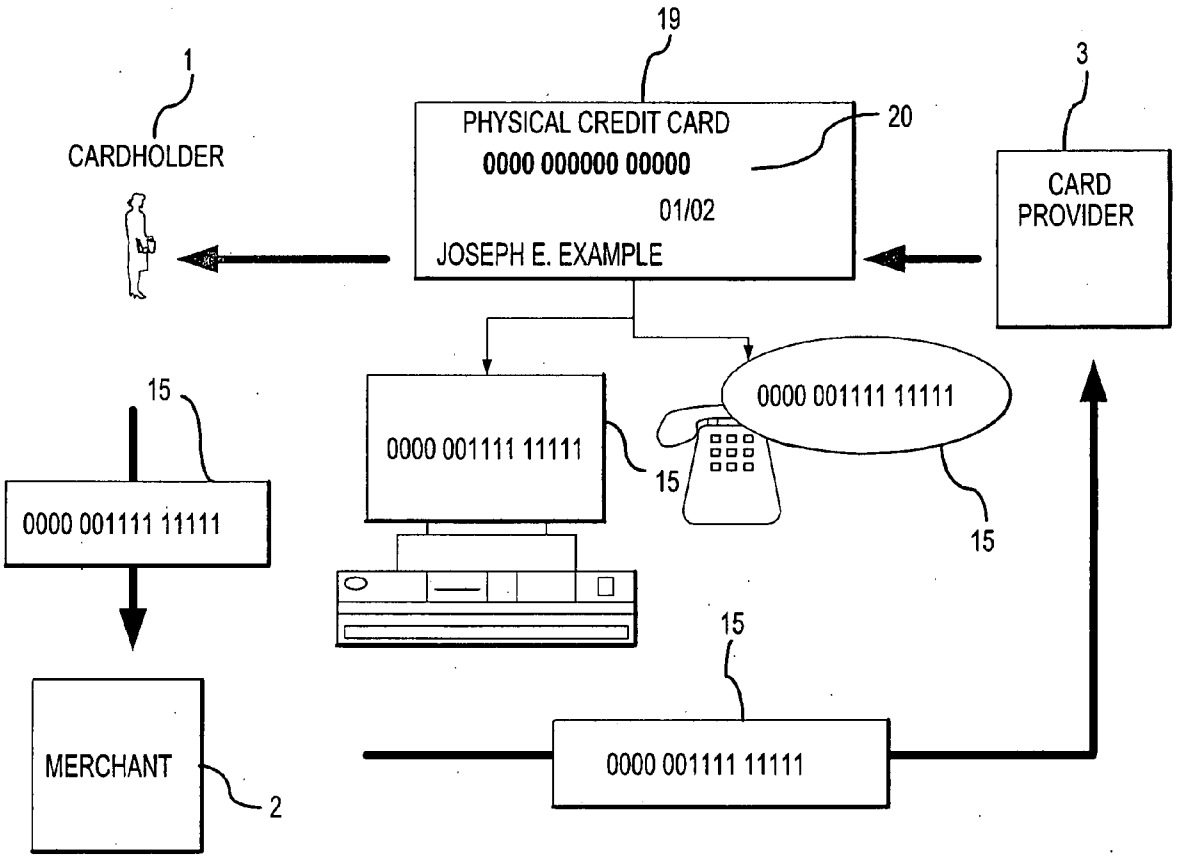
Publication Classification

(51) **Int. Cl.**[7] **G06F 17/60**

(52) **U.S. Cl.** **705/74**

(57) **ABSTRACT**

The present invention provides a system and method for facilitating a transaction using a secondary transaction number that is associated with a cardholder's primary account. The cardholder provides the secondary transaction number, often with limited-use conditions associated therewith, to a merchant to facilitate a more secure and confident transaction.



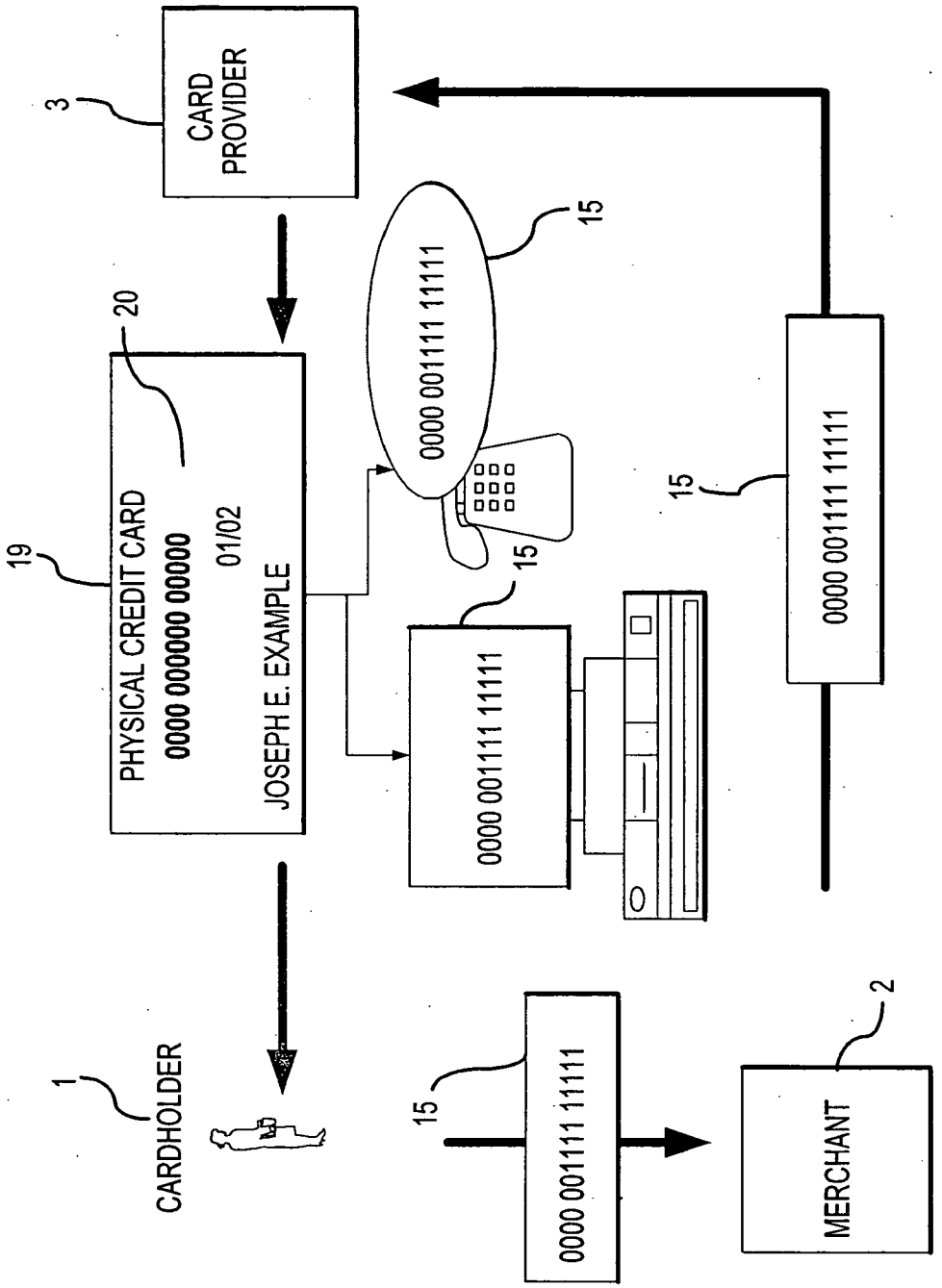

3
CARD PROVIDER
20
PHYSICAL CREDIT CARD
0000 000000 00000
01/02
JOSEPH E. EXAMPLE
19
15
0000 001111 11111
15
0000 001111 11111
15
0000 001111 11111
15
0000 001111 11111
1
CARDHOLDER
2
MERCHANT

FIG. 1

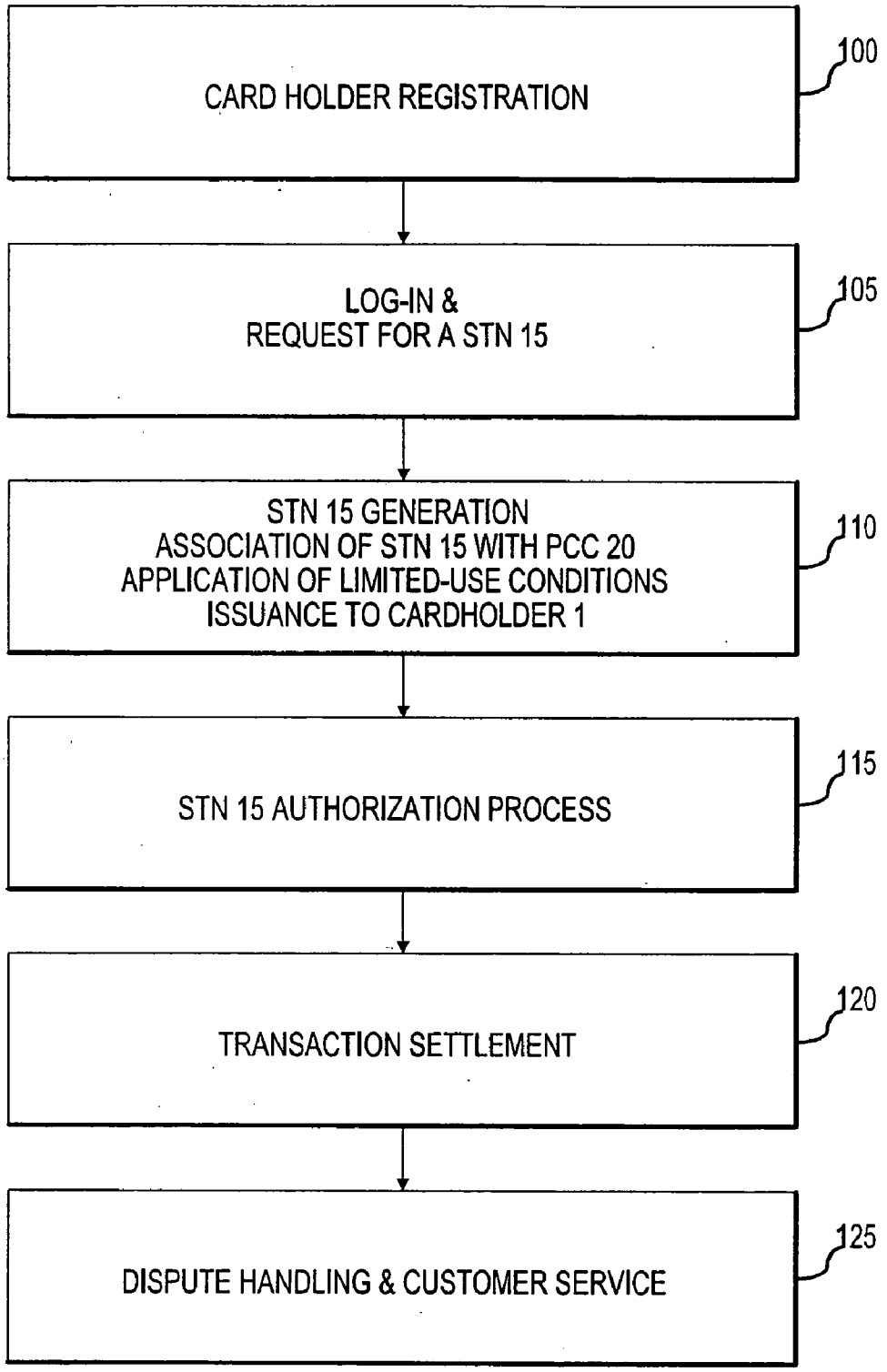

CARD HOLDER REGISTRATION
100
LOG-IN &
REQUEST FOR A STN 15
105
STN 15 GENERATION
ASSOCIATION OF STN 15 WITH PCC 20
APPLICATION OF LIMITED-USE CONDITIONS
ISSUANCE TO CARDHOLDER 1
110
STN 15 AUTHORIZATION PROCESS
115
TRANSACTION SETTLEMENT
120
DISPUTE HANDLING & CUSTOMER SERVICE
125

FIG. 2

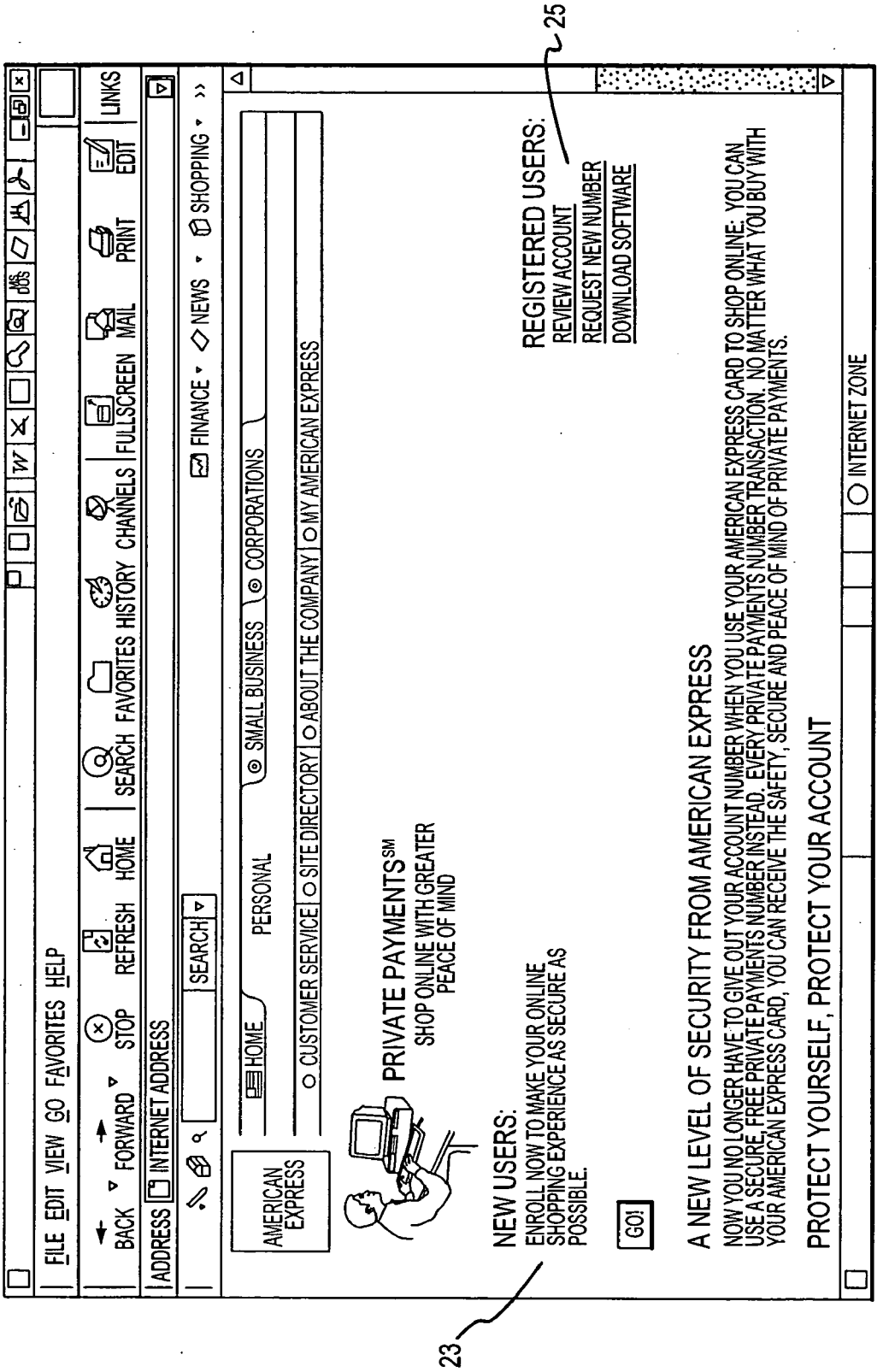

FILE EDIT VIEW GO FAVORITES HELP
BACK FORWARD STOP REFRESH HOME SEARCH FAVORITES HISTORY CHANNELS FULLSCREEN MAIL PRINT EDIT LINKS
ADDRESS INTERNET ADDRESS
SEARCH
FINANCE NEWS SHOPPING
AMERICAN EXPRESS
HOME
PERSONAL
SMALL BUSINESS
CORPORATIONS
CUSTOMER SERVICE
SITE DIRECTORY
ABOUT THE COMPANY
MY AMERICAN EXPRESS
PRIVATE PAYMENTS℠
SHOP ONLINE WITH GREATER PEACE OF MIND
NEW USERS:
ENROLL NOW TO MAKE YOUR ONLINE SHOPPING EXPERIENCE AS SECURE AS POSSIBLE.
GO!
REGISTERED USERS:
REVIEW ACCOUNT
REQUEST NEW NUMBER
DOWNLOAD SOFTWARE
A NEW LEVEL OF SECURITY FROM AMERICAN EXPRESS
NOW YOU NO LONGER HAVE TO GIVE OUT YOUR ACCOUNT NUMBER WHEN YOU USE YOUR AMERICAN EXPRESS CARD TO SHOP ONLINE. YOU CAN USE A SECURE, FREE PRIVATE PAYMENTS NUMBER INSTEAD. EVERY PRIVATE PAYMENTS NUMBER TRANSACTION. NO MATTER WHAT YOU BUY WITH YOUR AMERICAN EXPRESS CARD, YOU CAN RECEIVE THE SAFETY, SECURE AND PEACE OF MIND OF PRIVATE PAYMENTS.
PROTECT YOURSELF, PROTECT YOUR ACCOUNT
INTERNET ZONE
23
25

FIG.3

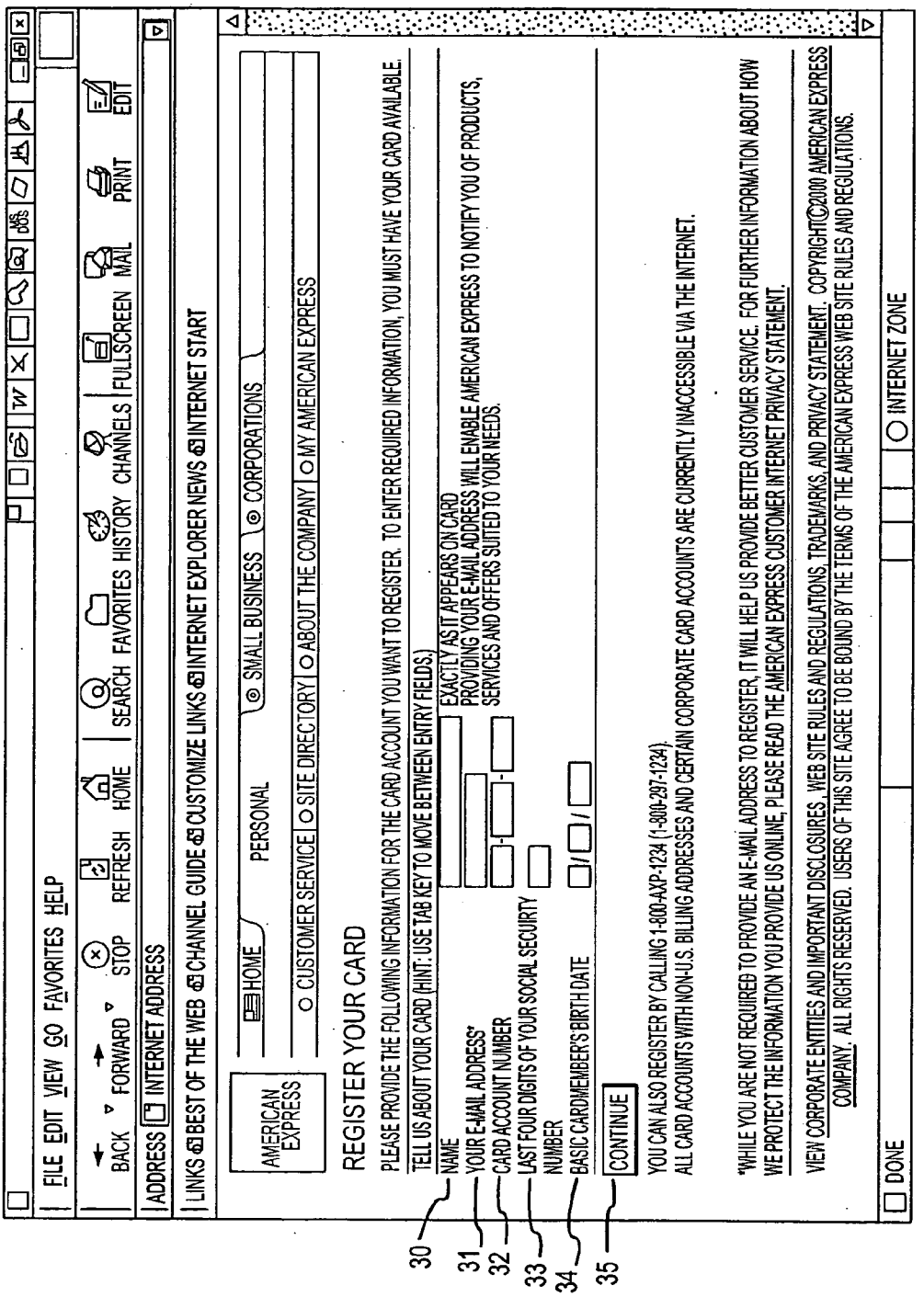

FILE EDIT VIEW GO FAVORITES HELP
BACK FORWARD STOP REFRESH HOME SEARCH FAVORITES HISTORY CHANNELS FULLSCREEN MAIL PRINT EDIT
ADDRESS INTERNET ADDRESS
LINKS BEST OF THE WEB CHANNEL GUIDE CUSTOMIZE LINKS INTERNET EXPLORER NEWS INTERNET START
AMERICAN EXPRESS
HOME
PERSONAL
SMALL BUSINESS
CORPORATIONS
CUSTOMER SERVICE
SITE DIRECTORY
ABOUT THE COMPANY
MY AMERICAN EXPRESS
REGISTER YOUR CARD
PLEASE PROVIDE THE FOLLOWING INFORMATION FOR THE CARD ACCOUNT YOU WANT TO REGISTER. TO ENTER REQUIRED INFORMATION, YOU MUST HAVE YOUR CARD AVAILABLE.
TELL US ABOUT YOUR CARD (HINT: USE TAB KEY TO MOVE BETWEEN ENTRY FIELDS.)
NAME
EXACTLY AS IT APPEARS ON CARD
YOUR E-MAIL ADDRESS*
PROVIDING YOUR E-MAIL ADDRESS WILL ENABLE AMERICAN EXPRESS TO NOTIFY YOU OF PRODUCTS, SERVICES AND OFFERS SUITED TO YOUR NEEDS.
CARD ACCOUNT NUMBER
LAST FOUR DIGITS OF YOUR SOCIAL SECURITY NUMBER
BASIC CARDMEMBER'S BIRTH DATE
CONTINUE
YOU CAN ALSO REGISTER BY CALLING 1-800-AXP-1234 (1-800-297-1234).
ALL CARD ACCOUNTS WITH NON-U.S. BILLING ADDRESSES AND CERTAIN CORPORATE CARD ACCOUNTS ARE CURRENTLY INACCESSIBLE VIA THE INTERNET.
*WHILE YOU ARE NOT REQUIRED TO PROVIDE AN E-MAIL ADDRESS TO REGISTER, IT WILL HELP US PROVIDE BETTER CUSTOMER SERVICE. FOR FURTHER INFORMATION ABOUT HOW WE PROTECT THE INFORMATION YOU PROVIDE US ONLINE, PLEASE READ THE AMERICAN EXPRESS CUSTOMER INTERNET PRIVACY STATEMENT.
VIEW CORPORATE ENTITIES AND IMPORTANT DISCLOSURES. WEB SITE RULES AND REGULATIONS, TRADEMARKS, AND PRIVACY STATEMENT. COPYRIGHT©2000 AMERICAN EXPRESS COMPANY. ALL RIGHTS RESERVED. USERS OF THIS SITE AGREE TO BE BOUND BY THE TERMS OF THE AMERICAN EXPRESS WEB SITE RULES AND REGULATIONS.
DONE
INTERNET ZONE
30
31
32
33
34
35

FIG.4

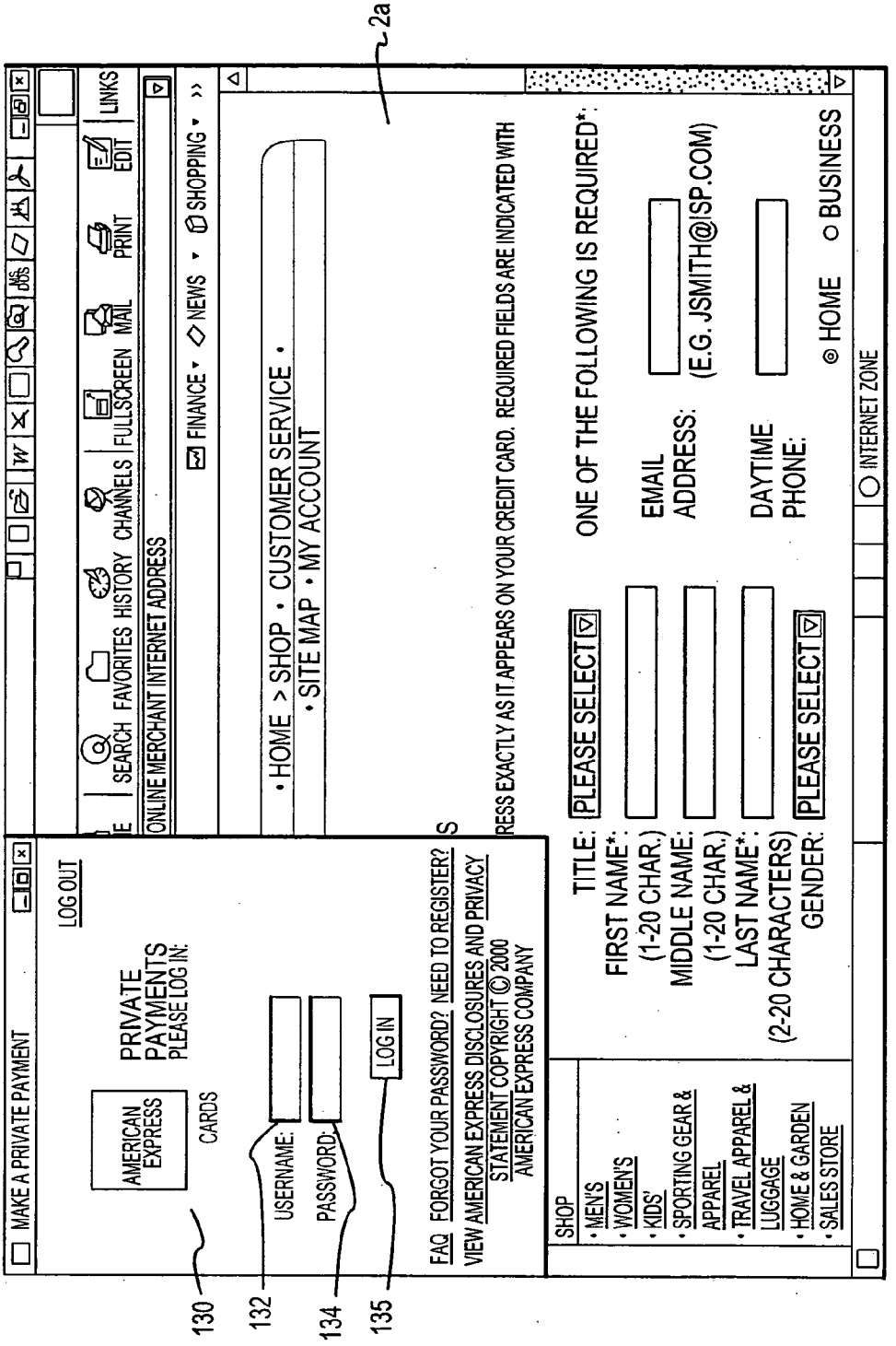

2a
MAKE A PRIVATE PAYMENT
LOG OUT
PRIVATE PAYMENTS
PLEASE LOG IN:
AMERICAN EXPRESS CARDS
USERNAME:
PASSWORD:
LOG IN
FAQ FORGOT YOUR PASSWORD? NEED TO REGISTER?
VIEW AMERICAN EXPRESS DISCLOSURES AND PRIVACY STATEMENT COPYRIGHT © 2000 AMERICAN EXPRESS COMPANY
SHOP
• MEN'S
• WOMEN'S
• KIDS'
• SPORTING GEAR & APPAREL
• TRAVEL APPAREL & LUGGAGE
• HOME & GARDEN
• SALES STORE
ONLINE MERCHANT INTERNET ADDRESS
SEARCH FAVORITES HISTORY CHANNELS FULLSCREEN MAIL PRINT EDIT LINKS
FINANCE NEWS SHOPPING
• HOME > SHOP • CUSTOMER SERVICE •
• SITE MAP • MY ACCOUNT
RESS EXACTLY AS IT APPEARS ON YOUR CREDIT CARD. REQUIRED FIELDS ARE INDICATED WITH
ONE OF THE FOLLOWING IS REQUIRED*:
TITLE: PLEASE SELECT
FIRST NAME*: (1-20 CHAR.)
MIDDLE NAME: (1-20 CHAR.)
LAST NAME*: (2-20 CHARACTERS)
GENDER: PLEASE SELECT
EMAIL ADDRESS: (E.G. JSMITH@ISP.COM)
DAYTIME PHONE:
HOME BUSINESS
INTERNET ZONE
130
132
134
135

FIG.5

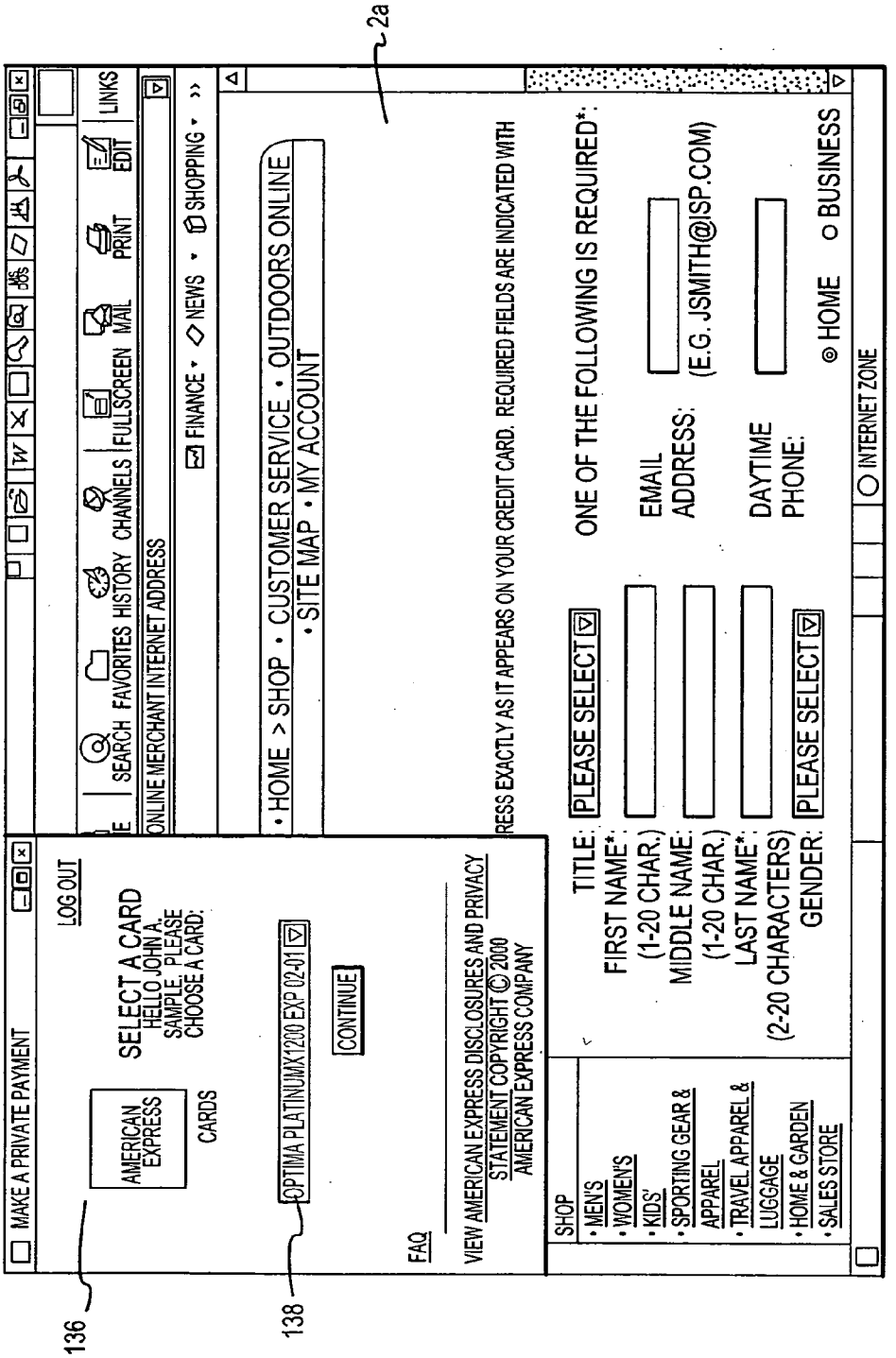

2a
136
138
MAKE A PRIVATE PAYMENT
LOG OUT
AMERICAN EXPRESS
CARDS
SELECT A CARD
HELLO JOHN A. SAMPLE. PLEASE CHOOSE A CARD:
OPTIMA PLATINUMX1200 EXP 02-01
CONTINUE
FAQ
VIEW AMERICAN EXPRESS DISCLOSURES AND PRIVACY STATEMENT COPYRIGHT © 2000 AMERICAN EXPRESS COMPANY
SEARCH FAVORITES HISTORY CHANNELS FULLSCREEN MAIL PRINT EDIT LINKS
ONLINE MERCHANT INTERNET ADDRESS
FINANCE NEWS SHOPPING
HOME > SHOP • CUSTOMER SERVICE • OUTDOORS ONLINE • SITE MAP • MY ACCOUNT
RESS EXACTLY AS IT APPEARS ON YOUR CREDIT CARD. REQUIRED FIELDS ARE INDICATED WITH
ONE OF THE FOLLOWING IS REQUIRED*:
TITLE: PLEASE SELECT
FIRST NAME*: (1-20 CHAR.)
MIDDLE NAME: (1-20 CHAR.)
LAST NAME*: (2-20 CHARACTERS)
GENDER: PLEASE SELECT
EMAIL ADDRESS: (E.G. JSMITH@ISP.COM)
DAYTIME PHONE:
HOME BUSINESS
SHOP
MEN'S
WOMEN'S
KIDS'
SPORTING GEAR & APPAREL
TRAVEL APPAREL & LUGGAGE
HOME & GARDEN
SALES STORE
INTERNET ZONE

FIG.6

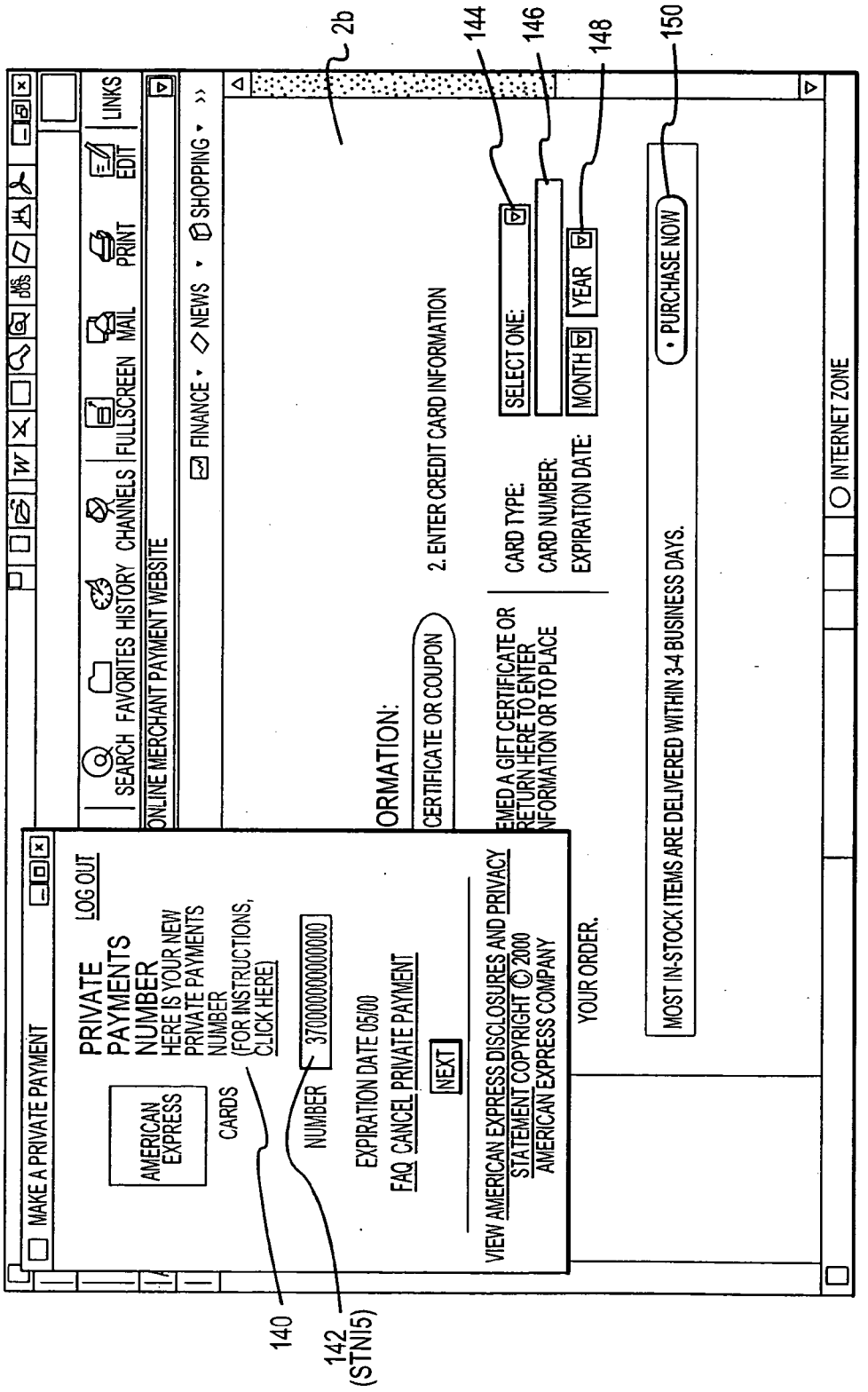

MAKE A PRIVATE PAYMENT
LOG OUT
PRIVATE PAYMENTS NUMBER
HERE IS YOUR NEW PRIVATE PAYMENTS NUMBER
(FOR INSTRUCTIONS, CLICK HERE)
AMERICAN EXPRESS CARDS
NUMBER 370000000000000
EXPIRATION DATE 05/00
FAQ CANCEL PRIVATE PAYMENT
NEXT
VIEW AMERICAN EXPRESS DISCLOSURES AND PRIVACY STATEMENT COPYRIGHT © 2000 AMERICAN EXPRESS COMPANY
ONLINE MERCHANT PAYMENT WEBSITE
SEARCH FAVORITES HISTORY CHANNELS FULLSCREEN MAIL PRINT EDIT LINKS
FINANCE NEWS SHOPPING
ORMATION:
CERTIFICATE OR COUPON
EMED A GIFT CERTIFICATE OR RETURN HERE TO ENTER NFORMATION OR TO PLACE
YOUR ORDER.
2. ENTER CREDIT CARD INFORMATION
CARD TYPE:
CARD NUMBER:
EXPIRATION DATE:
SELECT ONE:
MONTH
YEAR
PURCHASE NOW
MOST IN-STOCK ITEMS ARE DELIVERED WITHIN 3-4 BUSINESS DAYS.
INTERNET ZONE
140
142 (STNI5)
2b
144
146
148
150

FIG.7

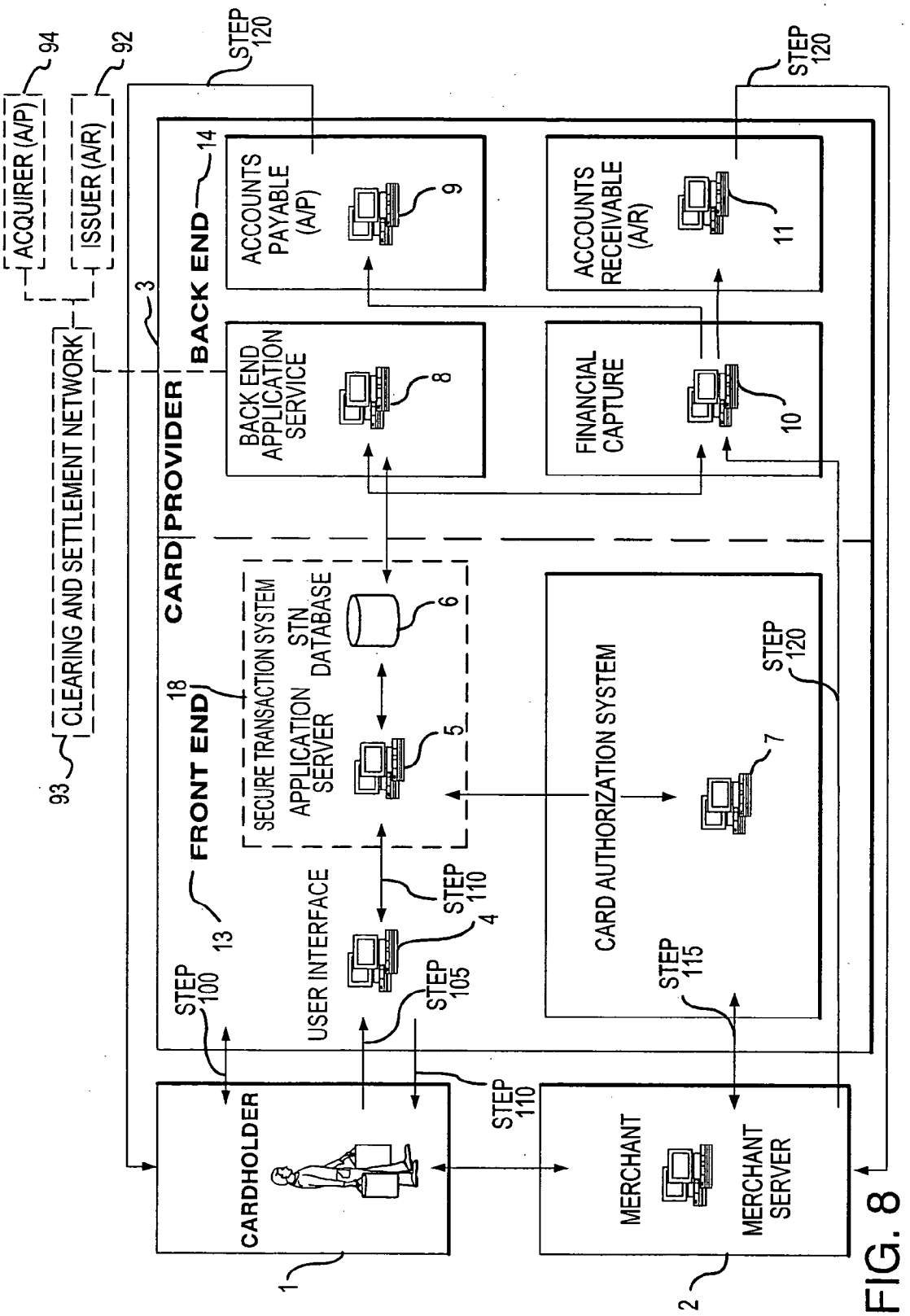

ACQUIRER (A/P)
94
ISSUER (A/R)
92
STEP 120
STEP 120
CLEARING AND SETTLEMENT NETWORK
93
3
CARD PROVIDER
BACK END
14
ACCOUNTS PAYABLE (A/P)
9
ACCOUNTS RECEIVABLE (A/R)
11
BACK END APPLICATION SERVICE
8
FINANCIAL CAPTURE
10
FRONT END
13
18
SECURE TRANSACTION SYSTEM
APPLICATION SERVER
STN DATABASE
6
5
CARD AUTHORIZATION SYSTEM
7
STEP 120
USER INTERFACE
STEP 110
4
STEP 100
STEP 105
STEP 115
STEP 110
CARDHOLDER
1
MERCHANT
MERCHANT SERVER
2

FIG. 8

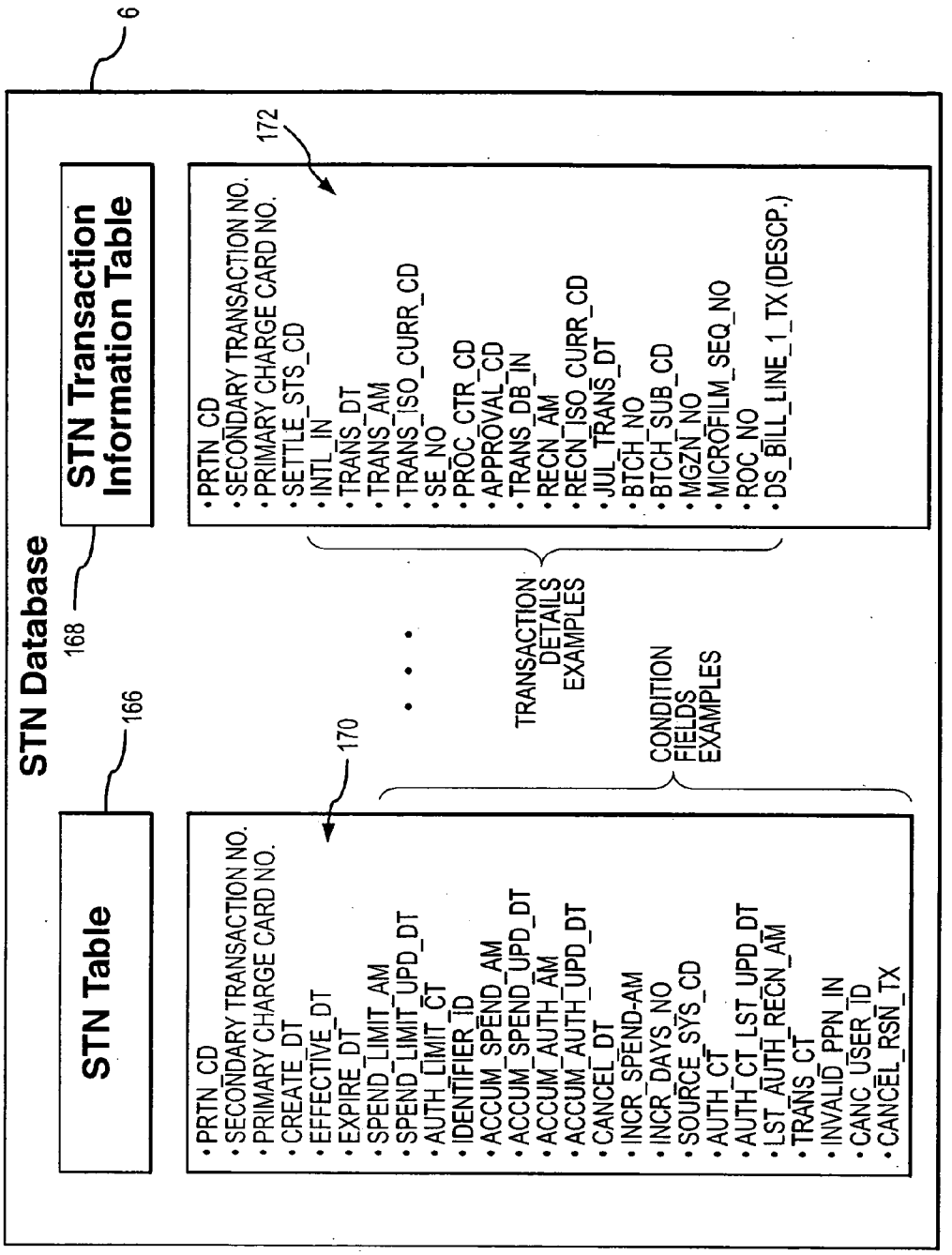

6
STN Database
STN Transaction Information Table
168
172
• PRTN_CD
• SECONDARY TRANSACTION NO.
• PRIMARY CHARGE CARD NO.
• SETTLE_STS_CD
• INTL_IN
• TRANS_DT
• TRANS_AM
• TRANS_ISO_CURR_CD
• SE_NO
• PROC_CTR_CD
• APPROVAL_CD
• TRANS_DB_IN
• RECN_AM
• RECN_ISO_CURR_CD
• JUL_TRANS_DT
• BTCH_NO
• BTCH_SUB_CD
• MGZN_NO
• MICROFILM_SEQ_NO
• ROC_NO
• DS_BILL_LINE_1_TX (DESCP.)
TRANSACTION DETAILS EXAMPLES
CONDITION FIELDS EXAMPLES
STN Table
166
170
• PRTN_CD
• SECONDARY TRANSACTION NO.
• PRIMARY CHARGE CARD NO.
• CREATE_DT
• EFFECTIVE_DT
• EXPIRE_DT
• SPEND_LIMIT_AM
• SPEND_LIMIT_UPD_DT
• AUTH_LIMIT_CT
• IDENTIFIER_ID
• ACCUM_SPEND_AM
• ACCUM_SPEND_UPD_DT
• ACCUM_AUTH_AM
• ACCUM_AUTH_UPD_DT
• CANCEL_DT
• INCR_SPEND-AM
• INCR_DAYS_NO
• SOURCE_SYS_CD
• AUTH_CT
• AUTH_CT_LST_UPD_DT
• LST_AUTH_RECN_AM
• TRANS_CT
• INVALID_PPN_IN
• CANC_USER_ID
• CANCEL_RSN_TX

FIG. 9

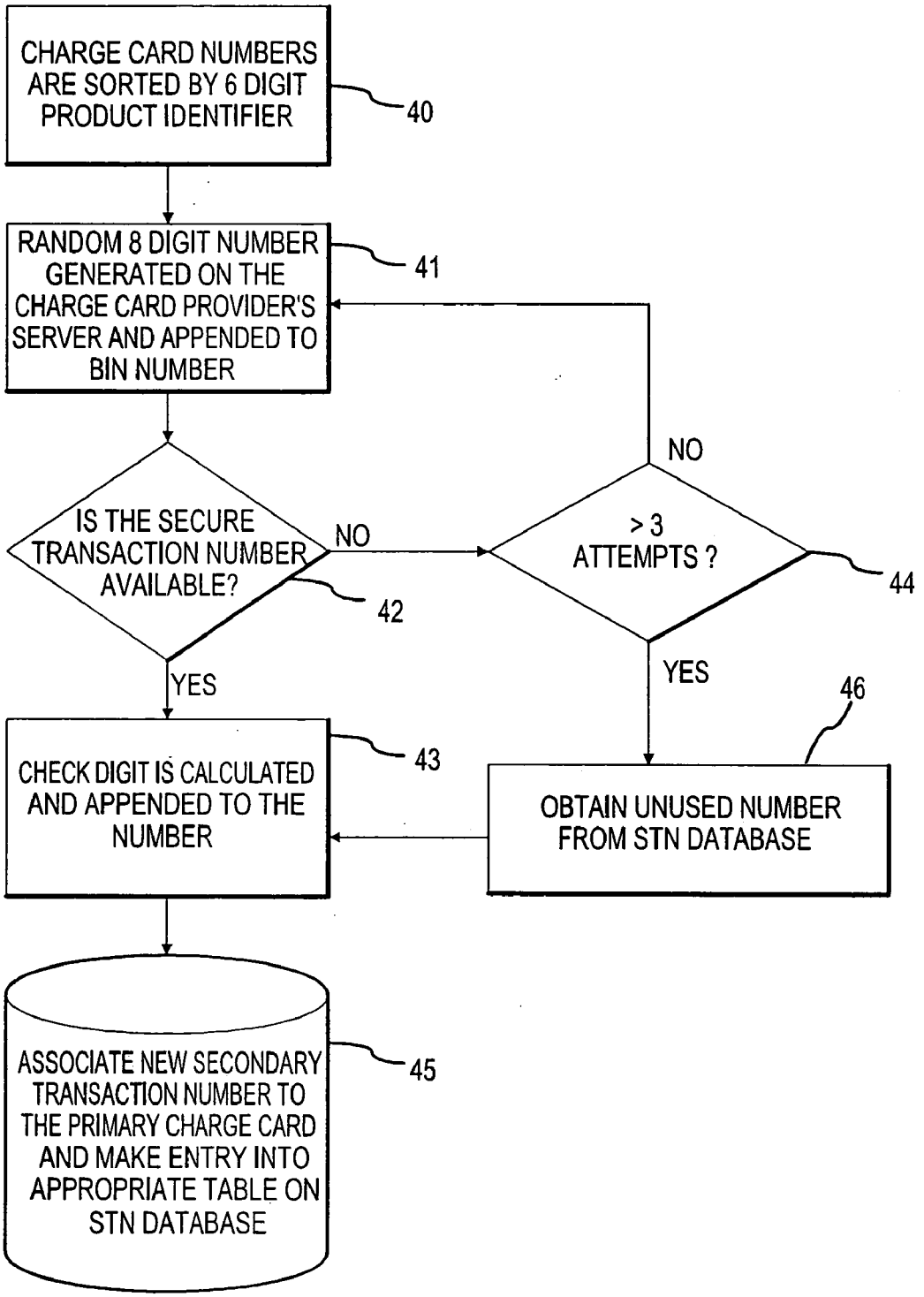

CHARGE CARD NUMBERS ARE SORTED BY 6 DIGIT PRODUCT IDENTIFIER
40
RANDOM 8 DIGIT NUMBER GENERATED ON THE CHARGE CARD PROVIDER'S SERVER AND APPENDED TO BIN NUMBER
41
IS THE SECURE TRANSACTION NUMBER AVAILABLE?
NO
42
> 3 ATTEMPTS ?
NO
44
YES
YES
46
CHECK DIGIT IS CALCULATED AND APPENDED TO THE NUMBER
43
OBTAIN UNUSED NUMBER FROM STN DATABASE
ASSOCIATE NEW SECONDARY TRANSACTION NUMBER TO THE PRIMARY CHARGE CARD AND MAKE ENTRY INTO APPROPRIATE TABLE ON STN DATABASE
45

FIG. 10

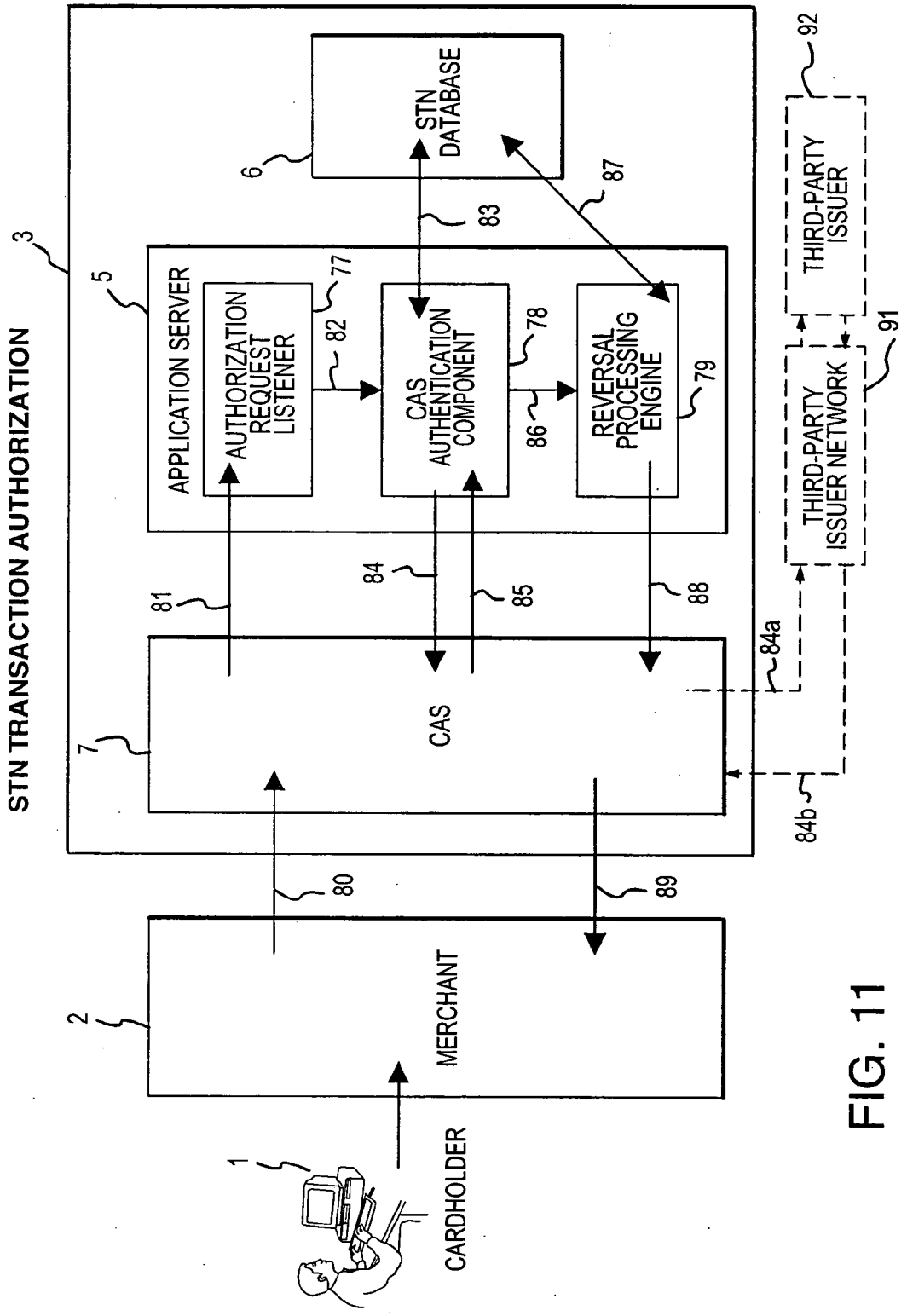

STN TRANSACTION AUTHORIZATION
3
APPLICATION SERVER
5
AUTHORIZATION REQUEST LISTENER
77
82
CAS AUTHENTICATION COMPONENT
78
86
REVERSAL PROCESSING ENGINE
79
STN DATABASE
6
83
87
81
84
85
88
CAS
7
84a
84b
80
89
MERCHANT
2
CARDHOLDER
1
THIRD-PARTY ISSUER
92
THIRD-PARTY ISSUER NETWORK
91

FIG. 11

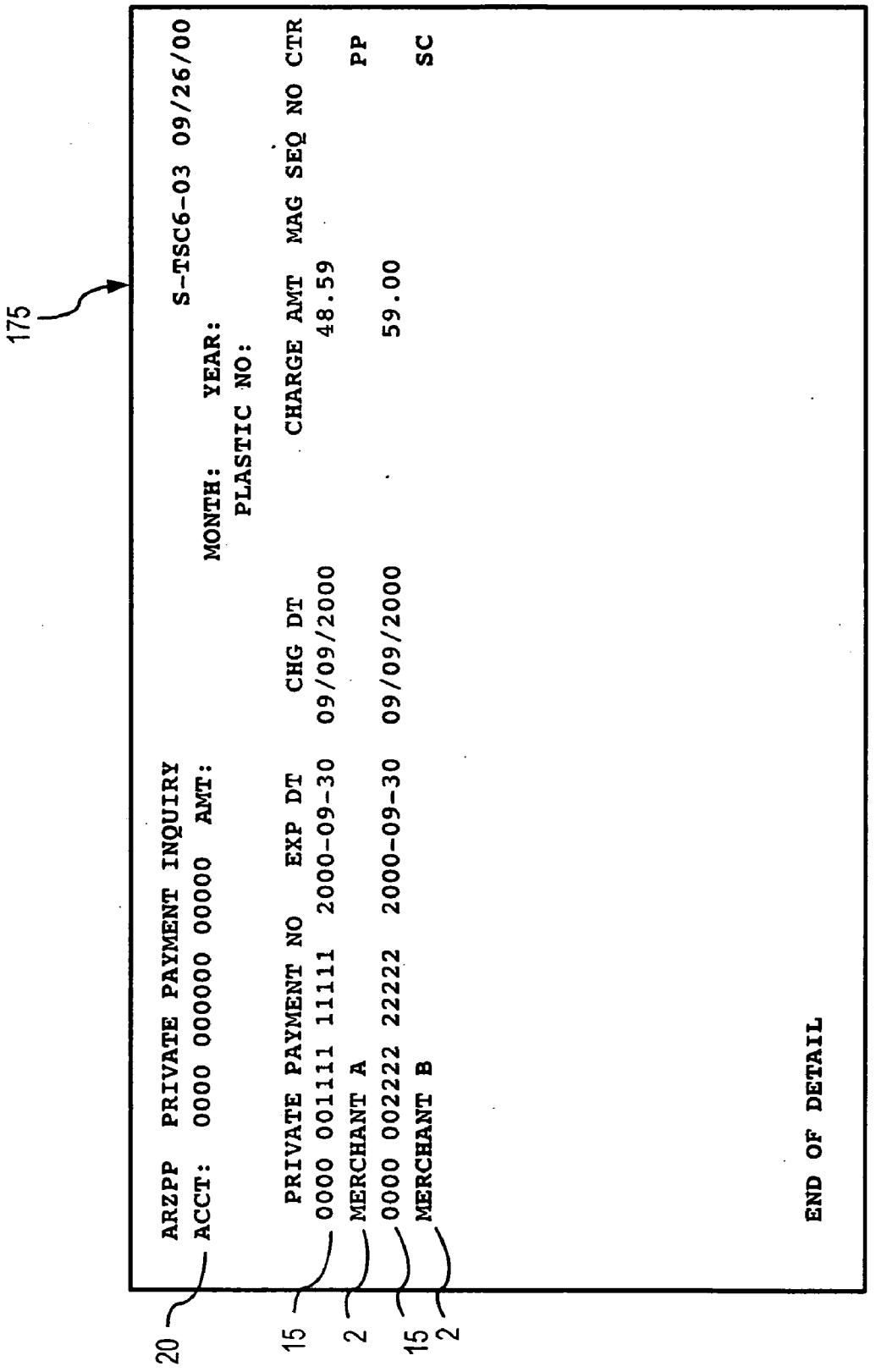

175
ARZPP PRIVATE PAYMENT INQUIRY
S-TSC6-03 09/26/00
ACCT: 0000 000000 00000 AMT:
MONTH: YEAR:
PLASTIC NO:
PRIVATE PAYMENT NO EXP DT CHG DT CHARGE AMT MAG SEQ NO CTR
0000 001111 11111 2000-09-30 09/09/2000 48.59 PP
MERCHANT A
0000 002222 22222 2000-09-30 09/09/2000 59.00 SC
MERCHANT B
END OF DETAIL
20
15
2
15
2

FIG. 12

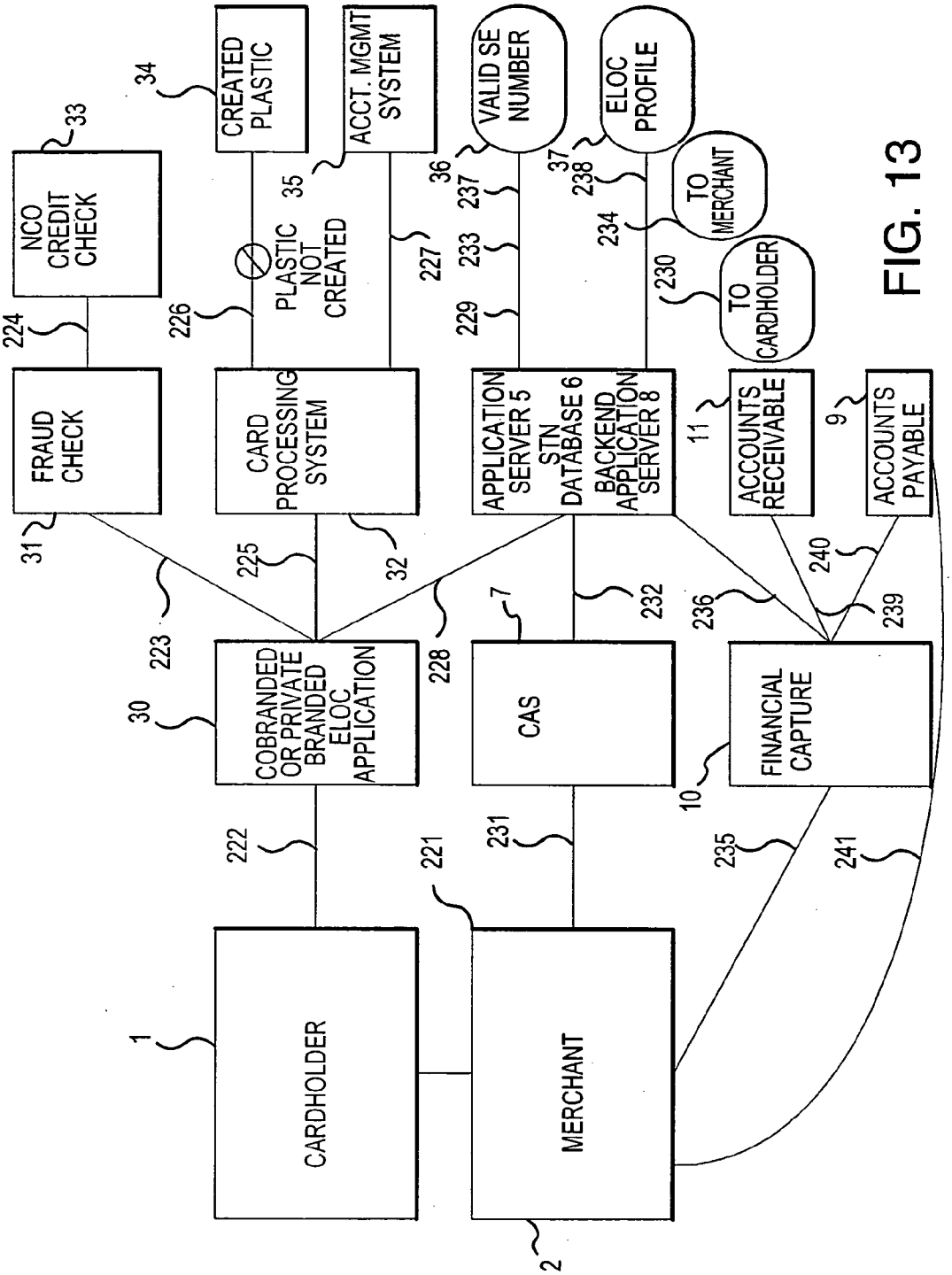

CARDHOLDER
1
MERCHANT
2
COBRANDED OR PRIVATE BRANDED ELOC APPLICATION
30
CAS
7
FINANCIAL CAPTURE
10
FRAUD CHECK
31
CARD PROCESSING SYSTEM
32
APPLICATION SERVER 5 STN DATABASE 6 BACKEND APPLICATION SERVER 8
ACCOUNTS RECEIVABLE
11
ACCOUNTS PAYABLE
9
NCO CREDIT CHECK
33
CREATED PLASTIC
34
ACCT. MGMT SYSTEM
35
VALID SE NUMBER
36
ELOC PROFILE
37
PLASTIC NOT CREATED
TO MERCHANT
TO CARDHOLDER
222
221
231
235
241
223
225
228
232
236
239
240
224
226
227
229
233
237
238
234
230

FIG. 13

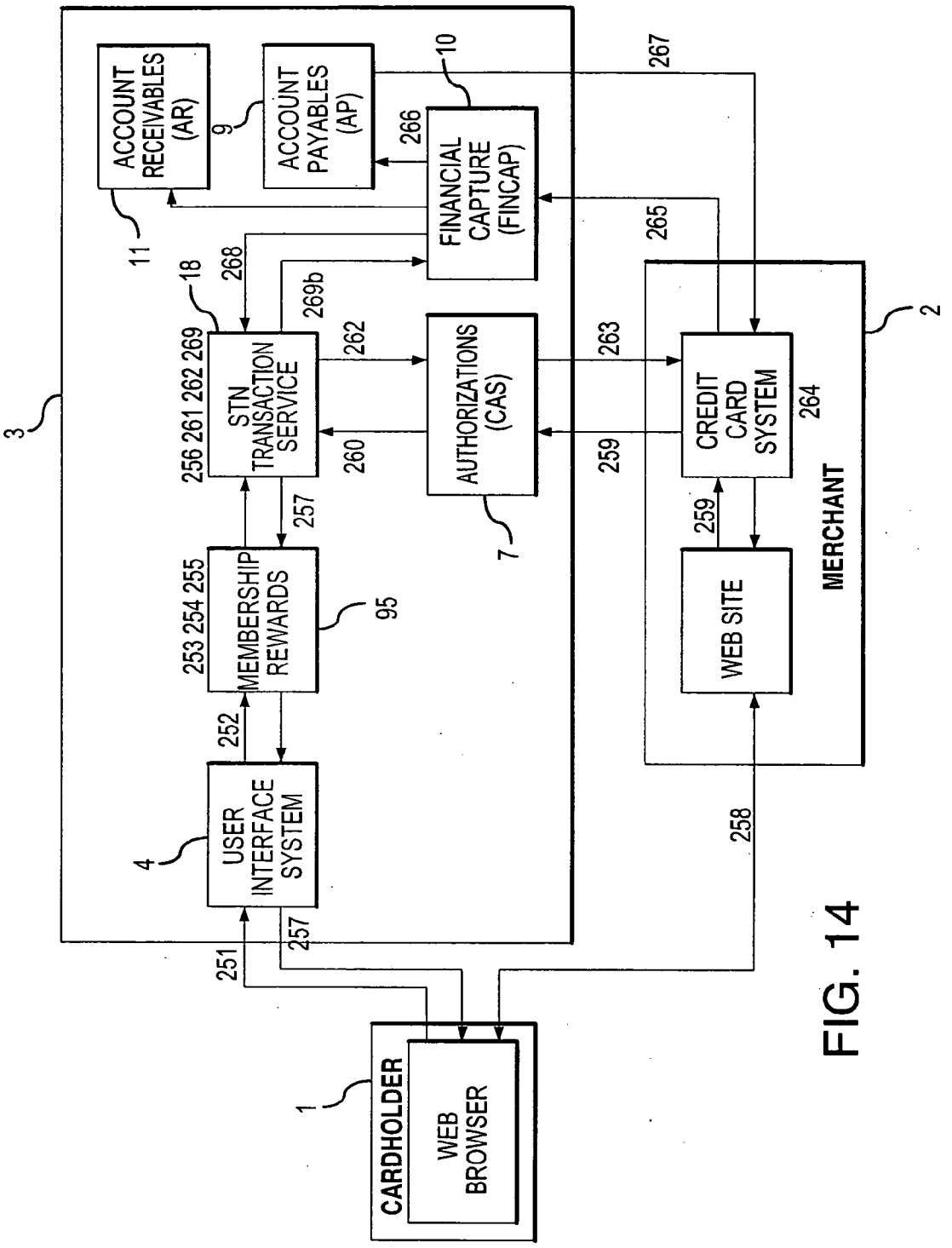

ACCOUNT RECEIVABLES (AR)
9
ACCOUNT PAYABLES (AP)
10
267
266
FINANCIAL CAPTURE (FINCAP)
11
265
18
268
269b
STN TRANSACTION SERVICE
256 261 262 269
262
AUTHORIZATIONS (CAS)
263
CREDIT CARD SYSTEM
264
2
3
260
259
257
7
MEMBERSHIP REWARDS
253 254 255
95
259
WEB SITE
MERCHANT
252
USER INTERFACE SYSTEM
4
258
257
251
CARDHOLDER
1
WEB BROWSER

FIG. 14

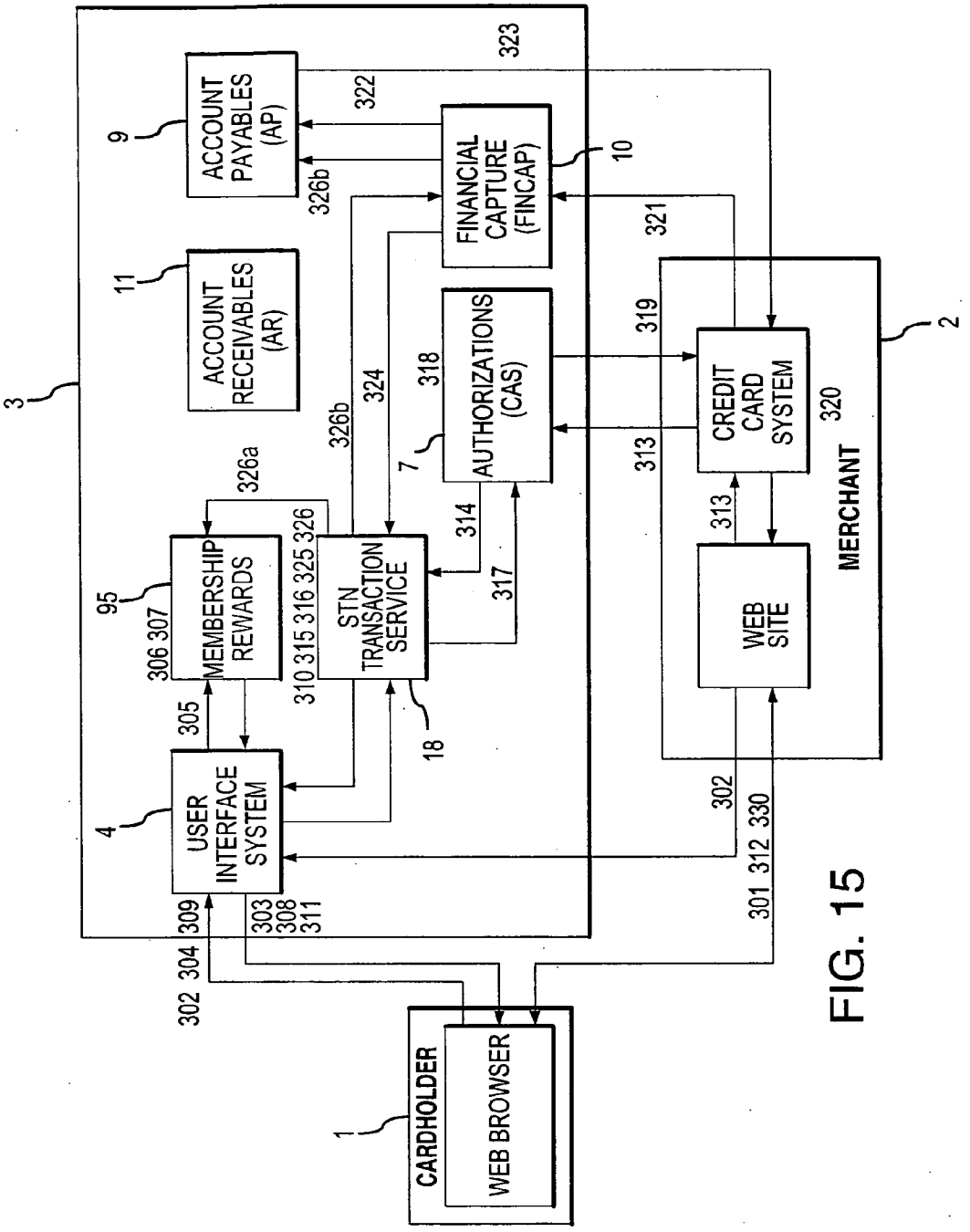

ACCOUNT PAYABLES (AP)
9
322
323
FINANCIAL CAPTURE (FINCAP)
10
326b
321
ACCOUNT RECEIVABLES (AR)
11
AUTHORIZATIONS (CAS)
318
319
CREDIT CARD SYSTEM
320
MERCHANT
2
3
324
326b
7
313
326a
MEMBERSHIP REWARDS
95
306 307
STN TRANSACTION SERVICE
310 315 316 325 326
314
317
313
WEB SITE
305
18
USER INTERFACE SYSTEM
4
302
330
309
303
308
311
301 312
304
302
CARDHOLDER
WEB BROWSER
1

FIG. 15

SYSTEM FOR FACILITATING A TRANSACTION

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to, and the benefit of, U.S. provisional applications: (1) Ser. No. 60/187,620, filed Mar. 7, 2000, (2) Ser. No. 60/200,625, filed Apr. 28, 2000, and (3) Ser. No. 60/213,323, filed Jun. 22, 2000, all of which are hereby incorporated by reference.

FIELD OF THE INVENTION

[0002] The present invention generally relates to a system for facilitating transactions utilizing a secondary transaction number that is associated with a primary transaction card. More particularly, the system allows a cardholder to pay a merchant with a private, limited-use, transaction number without the need to disclose to the merchant or others the cardholder's primary charge card number. Moreover, the present invention provides registration, number generation and association, authorization, settlement and customer service processes that achieve an improved secure and private transaction system.

BACKGROUND OF THE INVENTION

[0003] The proliferation of the Internet has resulted in a thriving electronic commerce industry, where more and more products and services are available to consumers in a variety of non-traditional ways, e.g., internet, telephone sales, wireless, interactive TV, etc. For example, in traditional online consumer-merchant transactions, consumers typically provide merchants with transaction numbers (e.g, charge card numbers) from their existing debit, phone, credit or other transaction/service cards (e.g., American Express®, VISA®, MasterCard® and Discover Card®, AT&T®, MCI®, etc.). Transmission of transaction numbers via these traditional means has created increased opportunities for fraud. Namely, it is possible for these numbers to be intercepted during transmission, after transmission, while being stored electronically or at the merchant's online or offline location. In light of the increase in charge card fraud involving situations where the physical charge card is not actually presented to the merchant, consumers are becoming increasingly cautious and leery of giving out their actual charge card number to merchants (or other unknown third parties asserting to be merchants).

[0004] In traditional online purchases, a consumer often browses the Internet for items to purchase. When the consumer finds an item that he or she is interested in purchasing, the consumer typically selects an item to add to a virtual shopping cart. When the consumer has finished shopping, and desires to purchase an item, the consumer usually proceeds to a virtual checkout, where the consumer is prompted for payment and delivery information. The consumer then typically is required to enter the appropriate delivery and credit card information, where the the consumer reads the credit card number directly from the consumer's physical credit card. This information is then transmitted electronically to the merchant via a public internet network. Although the transmission is often encrypted, there exists the possibility that the number will be intercepted en route to the merchant. More likely, however, is that the number will be fraudulently used by an unscrupulous third party, such as a dishonest employee of the merchant.

[0005] In addition to the previous example, various other means of credit card skimming are common in the industry. In an attempt to minimize these and similar problems relating to credit card fraud, banks and other credit card institutions have begun to explore various ways to provide customers with temporary transaction numbers to facilitate online transactions, where the actual credit card is not disclosed to the merchant or any other third party.

[0006] For example, U.S. Pat. No. 5,883,810 issued to Franklin, et al., which is hereby incorporated by reference, discloses a system to facilitate online commerce where a customer is able to register and sign-up for an "online commerce card." This online commerce card does not exist in physical form, but instead exists in a digital form that can be electronically configured for online commerce. The issuing bank issues the digital card to the customer in the form of a signed digital certificate binding the customer to the bank and provides the customer a software module that can be invoked when using the commerce card to conduct an online transaction. This online commerce card is assigned a permanent customer account number that resides with the issuing bank and is not given to the customer. In Franklin, when a customer desires to make an online purchase, the customer requests from the bank a transaction number that is good for a single transaction and with a limited life. This single transaction number is provided to a merchant to complete a purchase and is then processed by the merchant for authorization and settlement, with the issuing bank substituting and re-substituting the single transaction number and the customer account number as necessary in order to insure that the actual account number is not released to any third party.

[0007] Although the single use transaction number disclosed by Franklin provided some improvement over the traditional online transaction methods, several problems remained. For example, Franklin's system, which requires the generation of a digitally keyed online commerce card that does not exist in the physical form, requires customers to register and use an assigned digital certificate. Furthermore, this system requires the customer to download modules to facilitate the registration and transaction processes. Although Franklin notes that the commerce card is configured to be used by the customer in one or more areas of commerce in which the customer typically employs a charge card, Franklin fails to disclose how a consumer's existing plastic credit card number could be used to facilitate transactions. Specifically, Franklin requires instead, for the cardholder to sign-up and register in advance for an online commerce card that is not the cardholder's existing physical credit card, but is a non-physical digital card. Furthermore, the Franklin single transaction number will not work for multiple payment arrangements, i.e., where there is one purchase but multiple payment components.

[0008] Additional publications also disclose efforts to make transactions more secure, such as, for example, PCT Application, WO 99\49424, published on Sep. 30, 1999, and PCT Application WO 99\49586, published on Aug. 24, 2000 (collectively "Orbis"), hereby incorporated by reference, which attempt to expand and improve on the use of temporary transaction numbers. Specifically, Orbis discloses the use of a limited use credit card number that is associated with a master credit card (e.g., a physical credit card).

[0009] Orbis discloses using this limited use credit card number for transactions with merchants so that the physical credit card is not disclosed to the merchant or other third parties. In Orbis, for example, the bank or credit card provider issues the cardholder a non-activated limited use credit card number that is associated with the cardholder's master credit card. In an online transaction, the cardholder activates the limited use credit card and provides that number to the merchant to complete a transaction. On presentment to the card provider for authorization, the card provider verifies, inter alia, that the conditions of use have been met. If the conditions have been met, the card provider provides the merchant with an approval code that will accompany the payment request during settlement. If, however, during the authorization process, it is determined that certain conditions of use have not been met, the card provider de-activates the limited-use card. With the limited-use credit card de-activated, the merchant will not be paid and the transaction is not able to proceed through settlement. Conversely, if the limited use number is not submitted at all for authorization, and the merchant chooses to process this transaction for settlement, settlement may later occur and the merchant may be paid, with the incumbent risk to the merchant, however, that charge-back is likely if the charge is later disputed by the cardholder.

[0010] In prior art systems, if a transaction involving a temporary number is not authorized for failing to meet certain limited-use conditions, the number is deactivated and will not be processed through settlement. In real world environments, this creates certain problems. For instance, many online or telephonic purchases are multiple payment purchases, where one product may be purchased but multiple periodic payments are used to complete the transaction. Although the consumer is usually provided with the product up front, there may be occasions where the product is not delivered until all payments have been completed. The prior art systems occasionally create situations where the temporary transaction number is deactivated at some point in the multiple payment process where the merchant is not fully paid, possibly resulting in the product not being delivered to the consumer.

[0011] As previously noted, prior art systems typically use the authorization process to determine whether limited-use conditions are satisfied. The resultant comparison utilized in the authorization process is then used to update a conditions database. However, the consumer rarely knows exactly how many authorization requests will be submitted by the merchant. For example, a consumer may purchase an item online for $1000, agreeing to apply ten monthly $100 payments to complete the purchase. Initially, one employing a prior art system may think to apply a number of different limited use conditions to facilitate this transaction, e.g., one transaction for $1000, ten transactions for $100, or any combination. Additionally, different merchants may handle authorization requests in a number of different ways. A merchant may send to the card provider (i) only one authorization request for $1000; (ii) one authorization request for $1000, followed by subsequent authorization requests for each $100 payment; (iii) one authorization request for each $100 payment, or (iv) only a few periodic authorization requests. It is also common in the industry for merchants to submit pre-authorization requests followed by a subsequent request for authorization. In sum, it can be difficult for the consumer to guess exactly what method will be employed by the merchant to facilitate the authorization process.

[0012] As such, the prior art systems create situations where a temporary transaction number may be inadvertently deactivated prior to completion of the periodic payments. If, for example, the consumer only authorized one transaction, the card would be deactivated where the merchant submits one pre-authorization request, followed by a second authorization request prior to the first payment.

SUMMARY OF THE INVENTION

[0013] The present invention facilitates transactions between a first party (referred to herein as "cardholder") and a second party (referred to herein as "merchant") by providing the cardholder with a secondary transaction number that is associated with a cardholder's primary account, (e.g., charge card), wherein the cardholder presents or transmits the transaction number—not the primary charge card number—to the merchant to initiate a transaction.

[0014] More particularly, the system involves the process of registering a cardholder (if not already pre-registered) to participate in a transaction system; generating a secondary transaction number and issuing this number to the cardholder, where the cardholder presents this number to a merchant to complete a sales transaction; the merchant processing this secondary transaction number, similar to any other credit card number, where the number is typically presented to the credit card provider for authorization. Throughout this process, the cardholder's primary charge card number is never passed to the merchant or any other third party. Additionally, the secondary transaction number may also carry with it certain limitations-on-use conditions, where the transaction is not authorized unless these conditions are met.

[0015] In generating a secondary transaction number, upon a cardholder's request, the card provider generates a random number and associates this number with the cardholder's primary charge card account. This instantaneous and immediate generation of a random number allows for the number to be used by the cardholder immediately upon receipt. This process obviates the need for separate activation of the secondary transaction number, and minimizes the possibility that a secondary transaction number, once issued, will not be utilized because the cardholder or card provider failed to "activate" it.

[0016] During the authorization phase of the transaction process, the card provider receives the merchant's authorization request and verifies that certain limitations-on-use conditions, if any, have been satisfied. If the conditions have been satisfied, the request is approved and the card provider sends the merchant an approval code. If conditions have not been met, the request is declined. Although the request is declined, in an exemplary embodiment, the secondary transaction number is not "deactivated," and, as a result, may still continue through the payment process.

[0017] An exemplary settlement process of the present invention involves receiving a request from a merchant to be paid for a particular transaction and paying the merchant. As noted above, even a secondary transaction number that has not been authorized or that has been denied authorization by the card provider, may proceed through settlement, with the

incumbent risk to the merchant that the transaction (if not accompanied by a valid approval code) may later be charged back to the merchant if the transaction is ever disputed. During the settlement process, the accounts payable system pays the merchant, referencing only the secondary transaction number. However, prior to the accounts receivable processing, the secondary transaction number is replaced with the primary account for cardholder billing. The cardholder's statement may reflect, as desired, the secondary transaction number(s), the primary account number(s), all numbers or any combination of these numbers

[0018] The dispute handling and customer service processes of an exemplary embodiment of this invention enable customer service representatives to retrieve information and initiate customer or merchant inquiries based on the primary account number, the secondary transaction number or other transaction specific information provided by either the cardholder or the merchant. Therefore, the cardholder may provide either the primary account number or the secondary transaction number to the customer service representative to initiate a dispute. With either number, the representative is able to look-up the associated account number and account information. The system provides seamless integration of the secondary transaction number and the primary account (i.e., charge card) number to ensure that the merchant only sees statements, reports, letters, or financial adjustments bearing the secondary transaction number—not the charge card number, while the cardholder need only reference the primary charge card account. Additionally, it is through the dispute handling process that the cardholder may dispute a transaction involving, inter alia, an unauthorized use of the secondary transaction number and it is during this process that the transaction amount is charged back to the merchant. Other situations involving a merchant charge-back may include duplicate billing; service or item not received; item returned; or wrong amount billed.

[0019] Various embodiments of the present transaction system incorporate, and improve upon, existing or developing technologies, such as, for example, non-currency based programs and loyalty systems, electronic lines of credit, online banking, etc.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] Additional aspects of the present invention will become evident upon reviewing the non-limiting embodiments described in the specification and the claims taken in conjunction with the accompanying figures, wherein like reference numerals denote like elements.

[0021] **FIG. 1** is an overview of an exemplary system for facilitating a transaction.

[0022] **FIG. 2** is a flow diagram of exemplary processes of the present invention;

[0023] **FIG. 3** is a web page screen shot of a card provider's exemplary splash page for a transaction system;

[0024] **FIG. 4** is a web page screen shot of a card provider's exemplary online registration page for a transaction system;

[0025] **FIG. 5** is a web page screen shot of a card provider's exemplary online log-in page for a transaction system;

[0026] **FIG. 6** is a web page screen shot of a card provider's exemplary online drop-down menu used to select a primary charge card in the foreground and an online merchant's payment web page in the background;

[0027] **FIG. 7** is a web page screen shot, displaying in the foreground, an exemplary secondary transaction number (e.g., Private Payments™ number) returned to the user; and in the background, a merchant's payment web page;

[0028] **FIG. 8** is a block diagram of exemplary components of the present invention;

[0029] **FIG. 9** is a block diagram of an example of some of the exemplary data structure of the STN database of the present invention;

[0030] **FIG. 10** is a flow chart of an exemplary secondary transaction number generation process of the present invention;

[0031] **FIG. 11** is a flow diagram of an exemplary transaction authorization phase of the present invention;

[0032] **FIG. 12** is an screen shot of an exemplary transaction history report of the present invention;

[0033] **FIG. 13** is a flow diagram depicting an exemplary embodiment of the present invention involving an electronic line of credit system;

[0034] **FIG. 14** is a flow diagram depicting one embodiment of an exemplary transaction system of the present invention used to facilitate a non-currency based membership rewards program;

[0035] **FIG. 15** is a flow diagram depicting a second embodiment of an exemplary transaction system of the present invention used to facilitate a membership rewards program.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

[0036] As background, the various prior art methods for implementing transactional systems utilizing temporary numbers have failed to satisfy certain consumer demands for more secure and confident transactions. Specifically, the prior art systems have typically required, inter alia, (i) additional software to provide registration and transaction processes, (ii) the generation of a separate digital certificate embodying a non-physical online commerce card, (iii) separate activation of the temporary transaction number; or (vi) a deactivation of the temporary number if predefined conditions are not met. In short, previous transaction systems have not sufficiently adapted to real world demands for a more secure and confident transaction system that is readily compatible with existing banking and electronic commerce systems.

[0037] The present invention includes a unique system for facilitating transactions that is easily and readily adaptable to existing commercial transaction processing systems. While the system may contemplate upgrades or reconfigurations of existing processing systems, changes to cardholder or merchant systems are not necessarily required by the present invention. For example, the present system may contemplate, but does not require: downloading of software modules; a digitally-based, non-physical commerce card; activation or deactivation of the secondary transaction num-

ber; and certain embodiments do not require the existing online customer to separately register for the service. Moreover, the transaction system herein described can be seamlessly integrated into current electronic commerce processes with minimal to no changes to existing systems used by cardholders or merchants.

[0038] The transaction system of the present invention may be described herein in terms of functional block components, flow charts, screen shots, optional selections and various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware and/or software components configured to perform the specified functions. For example, the present invention may employ various integrated circuit components, e.g., memory elements, processing elements, logic elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, the software elements of the present invention may be implemented with any programming or scripting language such as C, C++, Java, COBOL, assembler, PERL, or the like, with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. For a basic introduction of cryptography, please review a text written by Bruce Schneider which is entitled "Applied Cryptography: Protocols, Algorithms, And Source Code In C," published by John Wiley & Sons (second edition, 1996), which is hereby incorporated by reference.

[0039] It should be appreciated that the particular implementations shown and described herein are illustrative of the invention and its best mode and are not intended to otherwise limit the scope of the present invention in any way. Indeed, for the sake of brevity, conventional data networking, application development and other functional aspects of the systems (and components of the individual operating components of the systems) may not be described in detail herein. Furthermore, the connecting lines shown in the various figures contained herein are intended to represent exemplary functional relationships and/or physical couplings between the various elements. It should be noted that many alternative or additional functional relationships or physical connections may be present in a practical electronic transaction system.

[0040] It will be appreciated, that many applications of the present invention could be formulated. One skilled in the art will appreciate that a network may include any system for exchanging data or transacting business, such as the Internet, an intranet, an extranet, WAN, LAN, satellite or wireless communications, and/or the like. The cardholder may interact with the card provider's transaction system or a merchant via any input device such as a telephone, keyboard, mouse, kiosk, personal digital assistant, touch screen, voice recognition device, transponder, biometrics device, handheld computer (e.g., Palm Pilot®), cellular phone, web TV, web phone, blue tooth/beaming device and/or the like. Similarly, the invention could be used in conjunction with any type of personal computer, network computer, workstation, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, or the like. Moreover, although the invention uses protocols such as TCP/IP to facilitate network communications, it will be readily understood that the invention could also be implemented using IPX, Appletalk, IP-6, NetBIOS, OSI or any number of existing or future protocols. Moreover, the system contemplates the use, sale, exchange, transfer, or any other distribution of any goods, services or information over any network having similar functionality described herein.

[0041] As will be appreciated by one of ordinary skill in the art, the present invention may be embodied as a-method, a data processing system, a device for data processing, and/or a computer program product. Accordingly, the present invention may take the form of an entirely software embodiment, an entirely hardware embodiment, or an embodiment combining aspects of both software and hardware. Furthermore, the present invention may take the form of a computer program product on a computer-readable storage medium having computer-readable program code means embodied in the storage medium. Any suitable computer-readable storage medium may be utilized, including hard disks, CD-ROM, optical storage-devices, magnetic storage devices, flash card memory and/or the like.

[0042] Communication between the parties (e.g., cardholder, card provider, and/or merchant) to the transaction and the system of the present invention may be accomplished through any suitable communication means, such as, for example, a telephone network, Intranet, Internet, point of interaction device (point of sale device, personal digital assistant, cellular phone, kiosk, etc.), online communications, off-line communications, wireless communications, and/or the like. One skilled in the art will also appreciate that, for security reasons, any databases, systems, or components of the present invention may consist of any combination of databases or components at a single location or at multiple locations, wherein each database or system includes any of various suitable security features, such as firewalls, access codes, encryption, de-encryption, compression, decompression, and/or the like.

[0043] The present invention is described below with reference to block diagrams and flowchart illustrations of methods, apparatus (e.g., systems), and computer program products according to various aspects of the invention. It will be understood that each functional block of the block diagrams and the flowchart illustrations, and combinations of functional blocks in the block diagrams and flowchart illustrations, respectively, can be implemented by computer program instructions. These computer program instructions may be loaded onto a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions which execute on the computer or other programmable data processing apparatus create means for implementing the functions specified in the flowchart block or blocks.

[0044] These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means which implement the function specified in the flowchart block or blocks.

The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions which execute on the computer or other programmable apparatus provide steps for implementing the functions specified in the flowchart block or blocks.

[0045] Accordingly, functional blocks of the block diagrams and flowchart illustrations support combinations of means for performing the specified functions, combinations of steps for performing the specified functions, and program instruction means for performing the specified functions. It will also be understood that each functional block of the block diagrams and flowchart illustrations, and combinations of functional blocks in the block diagrams and flowchart illustrations, can be implemented by either special purpose hardware-based computer systems which perform the specified functions or steps, or suitable combinations of special purpose hardware and computer instructions.

[0046] Referencing the computer networked aspect of a preferred embodiment of this invention, each participant is equipped with a computing system to facilitate online commerce transactions. The computing units may be connected with each other via a data communication network. The network is a public network and assumed to be insecure and open to eavesdroppers. In the illustrated implementation, the network is embodied as the internet. In this context, the computers may or may not be connected to the internet at all times. For instance, the cardholder computer may employ a modem to occasionally connect to the internet, whereas the card provider computing center might maintain a permanent connection to the internet. It is noted that the network may be implemented as other types of networks, such as an interactive television (ITV) network.

[0047] The merchant computer and the card provider computer may be interconnected via a second network, referred to as a payment network. The payment network represents existing proprietary networks that presently accommodate transactions for credit cards, debit cards, and other types of financial/banking cards. The payment network is a closed network that is assumed to be secure from eavesdroppers. Examples of the payment network include the American Express®, VisaNet® and the Veriphone® network.

[0048] As depicted in **FIG. 1**, the present invention generally relates to a transaction system where a first party to a transaction ("cardholder **1**") provides to a second party to a transaction ("merchant **2**") a secondary transaction number (STN) **15** that was generated by an issuer ("card provider **3**"). In a preferred embodiment, although not required, the STN **15** is immediately usable by the cardholder **1** without need for activation and may have associated therewith cardholder **1**, card provider **3**, or merchant **2** defined conditions or parameters of use restrictions which limit use of the STN **15**. A "transaction," as defined herein, includes, inter alia, any exchange or delivery of value, exchange or delivery of data, gifting of value or data, etc. The term "transaction" not only contemplates an exchange of goods or services for value from one party to another, but also the gifting of something from one party to another. Additionally, transaction or charge card numbers are account numbers that are used to facilitate any type of transaction.

[0049] While an exemplary embodiment of the invention is described in association with a transaction system, the invention contemplates any type of networks or transaction systems, including, for example, unsecure networks, public networks, wireless networks, closed networks, open networks, intranets, extranets, and/or the like.

[0050] The first party to the transaction (referred to herein as a "cardholder **1**") is any individual, business or other entity who uses a STN **15** to facilitate any transaction. In a preferred embodiment, the cardholder **1** establishes a new or has an existing relationship or association with a card provider **3**. For example, in one embodiment, a cardholder **1** may be an American Express® card member. In another embodiment, a cardholder **1** may be a participant in a frequent flyer rewards program. In a further embodiment, the cardholder **1** is a member of any suitable organization that provides transaction products or services. Another embodiment contemplates the cardholder gifting a secondary transaction number to a second party. The term cardholder **1** may also be referred to herein as "consumer,""card member,""user,""customer" or the like.

[0051] The second party to the transaction (referred to herein as a "merchant **2**") is any individual, business, or other entity who receives a secondary transaction number, whether or not in exchange for goods or services. For example, in one embodiment, a merchant **2** may be an online bookstore such as Amazon.com®. In another embodiment, a merchant **2** may be a local plumber. In yet another embodiment, a merchant **2** may be a local hardware store. In some instances, the cardholder **1** and the merchant **2** may be the same. In other situations, the merchant **2** and the card provider **3** are the same. Although referred to herein as a "merchant," this term contemplates situations where any second party receives a secondary transaction number from the first party: such as, for example, where a cardholder **1** gifts a secondary transaction number to another individual (i.e., second party merchant).

[0052] The issuer ("card provider **3**") includes any provider of products and/or services that facilitates any type of transaction. As contemplated by an exemplary embodiment of the present invention, the card provider **3** establishes and maintains account and/or transaction information for the cardholder **1**. The card provider **3** may issue products to the cardholder **1** and may also provide both the cardholder **1** and the merchant **2** with the processes to facilitate the transaction system of the present invention. The card provider **3** includes banks; credit unions; credit, debit or other transaction-related companies, telephone companies; or any other type of card or account issuing institutions, such as card-sponsoring companies, incentive rewards companies, or third party providers under contract with financial institutions. Unless otherwise specifically set forth herein, although referred to as "card provider," this term should be understood to mean any entity issuing any type of account to facilitate any transaction, exchange or service; and should not be limited to companies possessing or issuing physical cards. In an exemplary system, the card provider **3** may be any transaction facilitating company such as a charge card provider like American Express®, VISA®, Mastercard®, Discover®, etc. In another embodiment, the card provider **3** could be any membership organization or union. In some instances, the card provider **3** and the merchant **2** may be the same, for example, where the STN **15** is issued by the same

entity that provides the product or service. A STN **15** phone card issued by a telephone company, where the STN **15** phone card is tied to a primary telephone account is one such occasion.

[**0053**] An exemplary STN **15** is any transaction number, code, symbol, indicia, etc. that is associated with another number or account that has been designated by the cardholder **1** or the card provider **3** as a primary charge card (PCC **20**), i.e., primary account number. In an exemplary embodiment, the STN **15** is a purchasing number that acts as a charge card number and is associated with a PCC **20** account (e.g., a main charge card, credit, debit card or other account number, such as a bank or brokerage account, reward program account, etc.). In an exemplary embodiment, a PCC **20** account is not identified by a STN **15**. In certain embodiments, the PCC **20** account may have some identifying elements related to the STN **15**. The PCC **20** is defined herein to include any type of transaction card that references any account, membership, affiliation or association. When more than one cardholder **1** account exists, the PCC **20** is the account that has been designated by the cardholder **1** or the card provider **3** as the primary account. Alternatively, there may be a hierarchy of accounts where the STN **15** is associated with one or more PCCs **20** in a designated order. Additionally, as depicted in at least one embodiment described herein, a STN **15** may be associated with two or more accounts. For example, a STN **15** could be associated with a non-currency based account and also a PCC **20** account.

[**0054**] As shown in **FIG. 1**, in a preferred embodiment, the STN **15** and the PCC **20** have the same format, although additional embodiments may provide for account numbers with varying formats. In an exemplary embodiment involving credit, debit or other banking cards, the STN **15** has the same industry standard format that is used for the regular banking cards (e.g., 15 or 16 digit numbers). Preferably, the numbers are formatted such that one is unable to tell the difference between a STN **15** and a regular physical charge card. Alternatively, however, the card provider/product identifier (e.g., BIN range, first 6 digits, etc.) numbers may be different so as to differentiate the STNs from regular charge card numbers. In referencing the STN **15** and the PCC **20** number, it should be appreciated that the number may be, for example, a sixteen-digit credit card number, although each card provider has its own numbering system, such as the fifteen-digit numbering system used by American Express. Each company's card numbers comply with that company's standardized format such that a company using a sixteen-digit format will generally use four spaced sets of numbers, as represented by the number "0000 0000 0000 0000." The first five to seven digits are reserved for processing purposes and identify the issuing bank, card type etc. In this example, the last sixteenth digit is used as a sum check for the sixteen-digit number. The intermediary eight-to-ten digits are used to uniquely identify the cardholder **1**. The invention contemplates the use of other numbers, indicia, codes or other security steps in addition to the use of the STN **15**, but in an exemplary embodiment, only the STN **15** is provided to the merchant **2**.

[**0055**] In a preferred embodiment, the STN **15** is randomly and instantaneously generated by the card provider **3**, usually upon a cardholder's request, and can be distributed to the cardholder **1** by a variety of methods (online, telephone, wireless, email, regular mail, etc.) all of which should be secure and dependent upon verification of the cardholder's identity. Unlike the temporary transaction numbers disclosed in the prior art previously discussed, in a preferred embodiment, although not required, the STN **15** is immediately active (and usable) once it is associated with the cardholder's designated PCC **20** and provided to the cardholder **1**. This feature minimizes the possibility that a merchant **2** will obtain a transaction number that will be worthless because it was not properly activated by the cardholder **1**. While the present invention may contemplate a previously allocated pool of numbers that needs to be activated, an exemplary embodiment of the present invention includes STNs **15** that are instantaneously and randomly generated, and are usable upon receipt by the cardholder **1** without the need for separate activation.

[**0056**] In another preferred embodiment, the STN **15** may have limited-use (or conditions-of-use) parameters placed upon it by either the cardholder **1**, merchant **2**, or the card provider **3** in order for the numbers to be restricted for particular uses. Alternatively, the cardholder **1** is able to choose system default parameters of use. Parameters may include, for example: (i) use of the STN **15** is good for a predetermined number of transactions; (ii) cardholder-determined expiration dates (i.e., STN **15** will be generated with expiration dates that are associated but unrelated to the expiration date of the cardholder's PCC **20** number, other than that it cannot exceed the expiration date of the PCC **20** account); (iii) limiting use of the STN **15** to a specified dollar amount, dollar amount per transaction, total dollar amount for predesignated number of transactions, maximum dollar amount per month, etc.; (iv) use of the STN **15** for a specified merchant only; (v) restricting use to a specified user, other than primary cardholder (e.g., child, spouse, gift recipient, etc.); or (vi) any combination of these or similar features, for example, a number can be used at a specified merchant only for a pre-designated number of transactions and for a maximum dollar amount. In an exemplary online embodiment, a cardholder **1** may desire to require all online transactions (e.g., purchases) be performed using only STNs, or alternatively, be performed only with specific merchants as defined. If the cardholder (or another individual) uses a physical charge card number for an online payment in violation of this condition, the card provider **3** would decline the authorization.

[**0057**] These parameters not only provide increased security, allowing a cardholder **1** to tailor the STN **15** to a particular use, but an ancillary benefit is the ability of a cardholder to select preferences to control spending for themselves or others who have registered eligibility to use the card (e.g., spouse, children, etc.). These preferences may include: Restrictions (cardholder **1** may choose to restrict use on certain sites or can pre-approve spending at particular sites); date range (cardholder **1** can select a period of time when transactions may occur); maximum budget amount (cardholder **1** can pre-set spending limits within certain periods of time or in certain categories (e.g. groceries, books, clothing)); credit and balance availability (cardholder **1** can check credit or demand deposit balance availability prior to transacting); non-currency based accounts, such as Reward Points as Currency (cardholder **1** can use reward points (e.g. Membership Rewards™, Blue Loot™) as cur-

rency to pay for purchases); and Gift Products (cardholder **1** can use a STN **15** to fund gift products to others for designated amounts).

[**0058**] As shown in **FIG. 2**, an exemplary embodiment of the present invention includes steps for: (i) registering a cardholder **1** to use the card provider's **3** transaction services (step **100**); (ii) receiving from a cardholder **1** a request for a STN **15** (step **105**); (iii) generating a STN **15**, associating the STN **15** with a PCC **20**, applying limited-use conditions, if desired, and issuing the STN **15** to the cardholder **1** (step **110**); (iv) processing a merchant's **2** authorization request involving the STN **15** to determine if use of the STN is authorized (step **115**); (v) processing a settlement request, paying the merchant, and billing the cardholder **1** (step **120**); and (vi) handling disputes and other customer service issues from the merchant or cardholder relating to use of the STN **15** (step **125**).

[**0059**] **FIG. 8** depicts an overview of the components of an exemplary transaction system. In general, the card provider's computer system utilizes front end **13** and backend **14** processing systems. The front end **13** system comprises, inter alia, a user interface system **4** (e.g., web server, IVR, etc), an application server **5**, a STN database **6**, and a card authorization system (CAS) **7**. The application server **5** and STN database **6** may, at times, be referred to collectively as the STN transaction system (or service) **18**. Referencing **FIGS. 2 and 8**, these front end **13** components facilitate (i) cardholder registration (step **100**), (ii) request for a STN **15** (step **105**), (ii) generation and issuance of the STN **15** (step **110**), and (iv) the STN authorization process (step **115**). The backend **14** system comprises, inter alia, a financial capture system **10**, a back-end application service **8**, an accounts payable system **9** and an accounts receivable system **11**. Again referencing **FIGS. 2 and 8**, the backend **14** components facilitate transaction settlement (step **120**). In an exemplary system, the dispute handling and customer service processes (step **125**) include, inter alia, in addition to the above mentioned systems, a system for identifying a PCC **20** from a STN **15**, a letter generating system for sending dispute inquiries to cardholders **1** and merchants **2**, and a system that accepts incoming communication from merchants **2** and converts the STN **15** received to the PCC **20** for the purpose of facilitating the dispute handling process. More specifically, as shown in **FIG. 8**, the card provider **3** user interface system **4** provides the cardholder **1** with access to the card provider's transaction services. It is through this interface that the cardholder **1** may register with the card provider **3**, may request a STN **15**, and, in response thereto, will receive from the card provider **3** a STN **15** that is associated with his PCC **20**. The front end **13** system also utilizes at least one application server **5** that processes incoming information, applies the appropriate business rules/condition sets as necessary, and generates appropriate outgoing responses. The application server **5** is configured to support interaction with, inter alla, the user interface system **4** and a STN database **6**. An exemplary STN database **6** is a relational database comprising various tables for managing and translating a variety of information, such as cardholder **1** profiles, charge card data, transaction data, merchant data, conditions/rules set profiles, etc. **FIG. 9** illustrates two examples of exemplary tables within the STN database **6**. STN table **166** may contain a variety of database fields **170** relating to the cardholder's STN account. These fields may contain, in addition to general STN **15** and PCC **20** account information, the business rule/condition set profiles associated with use of the STN **15**. A STN Transaction Information Table **168** contains database fields **172** for storing information relating to a particular transaction. As a skilled programmer can appreciate, the processing mechanisms and data structure methods can be structured in a variety of ways. In short, the user interface system **4**, application server **5**, and the STN database **6** are suitably connected to facilitate the generation and issuance of a STN **15** and are further associated with a card authorization system (CAS) **7**, in order to process from the merchant **2** an authorization request involving a STN **15**.

[**0060**] When processing a merchant's request for settlement, i.e., to be paid for a transaction, the financial capture (FINCAP) **10** system receives and captures the financial information (e.g., transaction amount, date, merchant identification (SE) number, STN **15**, etc.). The back end application service **8** interfaces with the STN transaction system **18**, as necessary, to determine if the number is a valid STN **15** (i.e., not a phony number). If the STN **15** is valid, the AP system **9** pays the merchant **2**. The STN database **6** is updated to reflect the transaction information. The STN transaction system **18** (or alternatively the backend application service **8**) substitutes the PCC **20** number for the STN **15** and forwards to the AR system **11** for billing.

[**0061**] Although the present system for facilitating transactions may exist within one card provider system, exemplary embodiments contemplate use with other third party authorization and settlement systems and networks. **FIGS. 8 and 11**, for example, depict third party authorization networks (**FIG. 11, 91** and **92**) and settlement networks (**FIG. 8, 93-95**) that may be integrated to form parts and/or processes of the present invention.

[**0062**] Exemplary processes of the present invention are discussed in greater detail below.

[**0063**] Registration (**FIG. 2**, step **100**)

[**0064**] Two exemplary screen shots relating to an exemplary registration process are shown at **FIGS. 3 and 4**. **FIG. 3** depicts a splash page for an American Express® Private Payments^{SM} program. The Private Payments^{SM} program is an exemplary embodiment of the present invention. Here, a new user **23** may enroll to use the program or an existing user may access a number of program features **25**, e.g., review account, request a new STN **15** number or download software. The cardholder **1** generally enters this site by entering an appropriate card provider URL into her browser, by clicking on a link provided by a merchant's website, or alternatively, by an automatic pop-up feature that may appear upon recognizing particular URL or HTML codes.

[**0065**] To enroll (or register), the cardholder **1** is linked to a registration page (**FIG. 4**) and prompted for information. Information may include the cardholders name **30**, email address **31**, card account number **32** (e.g., PCC **20**), last four digits of social security number **33**, cardholder's date of birth **34**, etc. Any suitable authenticating information will suffice. By selecting "continue," the cardholder **1** is provided with a username and password, or preferably, the cardholder is allowed to select her own username and password. The user interface system **4** processes this information and suitably interfaces with the STN transaction system **18** (**FIG. 8**) to register the cardholder. As one of skill in this art

will appreciate, registration may take many forms and may be accomplished in a variety of ways. For example, a card provider **3** may choose to automatically enroll all new charge card applicants and return to the cardholder a username and password with the physical credit card. Although **FIGS. 3 and 4** show an online registration process, it should be appreciated that this process may take place via any suitable user interface system.

[**0066**] In one embodiment, during the registration process, the cardholder **1** may choose to select or define various parameters, preferences, and programs to tailor the transaction system to the cardholder's particular needs. Additional embodiments allow the cardholder **1** to select or define parameters, preferences or programs at any point in the transaction process. In other words, the cardholder **1** has the flexibility to select parameters each time (e.g., during registration, log-in, upon STN request, etc.) a STN **15** is generated or may apply universal parameters to every STN **15** generated. With these selections, for example, the cardholder **1** may (i) designate a specific credit card to function as the primary charge card number; (ii) associate the transaction system with other programs such as a non-currency based membership rewards program, an online digital wallet, an online shopping gateway (e.g., American Express's "ShopAMEX"), an online gift check program (e.g. E-Gift), preferred buyer's programs, etc.; (iii) provide password protected access to family members; (iv) activate a smartcard feature allowing remote random generation of secondary transaction numbers; (v) designate cell phone, email or pager numbers to utilize with the voice or automated response secondary transaction number generation feature; (vi) and other banking and transaction features that may be apparent to those skilled in the art. For more information on loyalty systems, transaction systems, electronic commerce systems and digital wallet systems, see, for example, the Shop AMEX™ system as disclosed in Serial No. 60/230,190 filed Sep. 5, 2000; the MR as Currency™ System disclosed in Serial No. 60/200,492 filed Apr. 28, 2000 and Serial No. 60/201,114 filed May 2, 2000; Wireless MR as disclosed in Serial No. 60/192,197,296 filed on Apr. 14, 2000; a digital wallet system disclosed in U.S. Ser. No. 09/652,899 filed Aug. 31, 2000; a stored value card as disclosed in Ser. No. 09/241,188 filed on Feb. 1, 1999, all of which are herein incorporated by reference.

[**0067**] Log-in and Request for STN **15** (**FIG. 2**, step **105**):

[**0068**] A registered cardholder **1** generally accesses the card provider's transaction system by logging into the system via any suitable user interface system **4**. **FIG. 5** depicts an exemplary online log-in screen **130**, where the cardholder **1** is prompted for authenticating information such as a usemame **132** and password **134**. Alternative systems contemplate authentication via any suitable user interface system. For example, an embodiment employing a portable data device such as a smart card facilitates authentication by swiping the smart card through a smart card reader and providing the appropriate PIN. After entering the appropriate authenticating information and clicking the log in button **135**, the information is routed through the user interface system **4** (e.g., web server) to the application server **5**, where, as shown in **FIG. 5**, the application server **5** retrieves information relating to the cardholder's account from the STN database **6**. If the cardholder **1** has registered multiple charge card accounts, in one embodiment **136**, as depicted in **FIG. 6**, the program prompts the cardholder **1** to choose from a list of accounts from a pull-down menu **138**. The cardholder **1** then selects at least one account to be the primary account or to be included in a primary group of accounts (when it is desired for the STN **15** to be associated with more than one account). In other embodiments, the user interface system **4** (e.g., web server) will return additional options for the cardholder **1**, such as prompting the cardholder **1** to choose from several condition fields such as those previously mentioned (e.g., restricting use to a particular merchant, amount, allowing use by other recipients, etc.).

[**0069**] STN **15** Generation and Issuance (Distribution) to Cardholder **1** (Step **110**):

[**0070**] An exemplary online transaction process begins with a cardholder **1** desiring to purchase products or services from an online merchant's website. In this exemplary online system, the cardholder **1** selects products from a merchant's online website **2**, is routed or clicks to the merchant's payment page **2***a* (**FIG. 5**). The cardholder **1** is hyperlinked (manually or automatically) to a card provider's web site to log in **130** (**FIG. 5**), which resides on and is managed by the card provider's user interface system **4** (e.g., web server), and, upon logging in, obtains a STN **15** that may then be "cut and pasted,""dragged and dropped" (or alternatively, automatically filled by the card provider **3** or downloaded from a digital wallet) into the payment fields **144**, **146**, **148** (**FIG. 7**) on the payment web page **2***b* (**FIG. 7**). In alternative embodiments, the system includes one or more of the following: the card provider **3** sends the STN **15** directly to the merchant **2**, the STN **15** is encrypted or encoded, the cardholder **1** enters additional security numbers or other indicia or a biometric sample is required from the card provider **3**. In an exemplary embodiment, the STN **15**, as will be discussed next, is generated by the card provider's application server **5** and STN database **6**.

[**0071**] After authenticating a cardholder **1** during the log-in process, and receiving a request for a STN **15**, the process begins for generating a STN **15**. The user interface system **4** prompts the initiation of the number generation process in the STN transaction system **18**. In an exemplary random number generation process, the STN **15** is generated (preferably immediately) and provided to the cardholder **1** (preferably contemporaneous with the cardholder's request). As previously noted, this allows the number to be usable immediately upon receipt by the cardholder **1** without the need for separate activation (although separate activation features are contemplated by the present invention), while minimizing any increased risk of theft or fraud.

[**0072**] An exemplary random number generation process is depicted in **FIG. 10**. In this exemplary embodiment, each card provider **3** (**FIG. 1**) is generally identified by a range of numbers on the physical card, typically called the bank identification number (BIN). Each card possesses a product identifier (e.g., first 6 digits. BIN, etc) that is not part of the random number generation process, but in order to initiate the process, this number must first be selected (step **40**). It may be preferable for a card provider **3** to set aside a set of product identification numbers relating to secondary transaction numbers for specific use with the transaction system. Alternatively, however, some card providers may find it desirable to use the same BIN number designation for both

STNS **15** and regular charge card numbers so that one cannot distinguish between the two types of numbers. As depicted in **FIG. 10, a** random eight digit number is generated by the card provider's application server **5** using an algorithmic process (step **41**). The application server **5** verifies that the randomly generated number is available (i.e., it is not in use nor has it been used within a certain period of time) (step **42**). If the transaction number is free (i.e., not in use), a check digit and the selected product identification number is appended to the number (step **43**). This newly created STN **15** is then associated with the cardholder's PCC **20** and is provided to the cardholder **1** (step **45**), whereupon the STN database **6** is updated to reflect that this particular STN **15** is in use and associated with a PCC **20** account. If, during step **42**, it is determined that the number is in use, the number generation process is repeated up to a preset number of times (e.g., 3) (step **44**). After attempting and failing to generate a non-used random number for a preset number of times, a non-used random number is physically selected from the STN database **6** (step **46**).

[**0073**] After the STN **15** is generated, conditions of use parameters are applied, and are associated with the PCC **20**, the STN **15** is then distributed (i.e., issued) to a cardholder **1** for use in facilitating a transaction. Communication of the STN **15** may occur via a number of use interface systems **4**. For example, **FIG. 7** depicts an exemplary online interface where the STN **15** (Private Payment number) is returned to the cardholder **1**. This embodiment shows how the card provider window **140** overlays a merchant's online payment page **2***b*. The cardholder **1** selects the appropriate charge card (e.g., American Express®) from the credit type filed **144**. The cardholder **1** is then able to "cut and paste" or "drag and drop" the STN **15** (present in the STN field **142**) into the credit card field **146** on the webpage **2***b*. Finally, the cardholder **1** chooses the appropriate expiration date **148** and completes the transaction by selecting the "purchase now" button **150**. Although this embodiment describes linking to a card provider's web site to receive a STN **15**, an additional embodiment configures the user interface **4** (e.g., web server) and STN transaction system **18** to seamlessly interact with the merchant's website to eliminate the need to separately link to the card provider **3**. In this instance, the generation and issuance of the STN **15** would use the merchant **2** as a gateway to the card provider **3**. Any number of interface systems **4** can be used to facilitate the processes described above (**FIG. 2** steps **100**, **105**, **110**).

[**0074**] For example, as just described, distribution of the STN **15** may occur via a "server to desktop" arrangement where a connection is established between the card provider's web-server **4** and the cardholder's **1** desktop computer, using SSL 3.0. With this exemplary system, the number is generated by the application server **5** (according to an algorithmic processing feature) utilizing a random number generation process such as that previously described and delivered to the web server **4**. The number is then displayed on the cardholder's **1** desktop. While pre-registration is not required, in an exemplary embodiment, a cardholder **1** will have previously registered at the card provider's **3** online web site providing all required personal information, primary charge card account numbers, and establishing a cardholder ID and password (if not already established). The cardholder ID and password are then used for verification of cardholder **1** identity when logging into the card provider's web server **4**.

[**0075**] Distribution of STNs **15** may also occur via a "server to IVR" arrangement, where a cardholder **1** calls the card provider **3** in order to obtain a STN **15**. In this exemplary embodiment, a voice response menu enables the cardholder **1** to choose the transaction option, and allows the cardholder **1** to enter a main account number. Once identity is verified, a link to the application server **5** is established, prompting generation and delivery of a STN **15** over the phone. In this embodiment, the cardholder **1** provides authenticating information by providing date of birth (DOB), a PIN, etc. Once this verification number is matched to customer's records, the STN **15** is distributed. Of course, this process would also work with a live operator arrangement.

[**0076**] Additional distribution embodiments include a number of different delivery vehicles and/or portable data devices, such as use of wireless devices, smart chip encoded devices, personal digital assistants (PDAs), pagers, interactive TVs, etc. For example, a "server to wireless device" is used where a wireless phone with internet browser is able to access the card provider's transaction site via the card provider's online service web site. The STN **15** can be delivered via text or voice. Additionally, with the use of encryption keys, the wireless device can be used as payment vehicles (e.g., STN **15** is delivered from the cardholder **1** to merchant **2** or other customer with Blue Tooth or other beaming technology). Again, verification of identity can be accomplished by a variety of means, including cardholder ID and password, DOB, PIN number, SIM cards in phones, etc.

[**0077**] Another exemplary embodiment of the transaction system, utilizing one or more of the distribution arrangements above, includes situations where a Point of Sale terminal (POS) is not present (e.g., submitting a STN **15** to a merchant **2** such as, for example, a plumber at home). In this exemplary embodiment, the cardholder **1** may not have cash or may not want to provide her PCC **20** number to the vendor due to concerns about unauthorized re-use. As such, the cardholder **1** calls the card provider **3** seeking to obtain a STN **15** with either pre-defined conditions of use or cardholder determined conditions of use. A voice recognition system asks for a PCC **20** number, the amount she wants to authorize, a merchant ID (e.g., SE number), or any other conditions of use. The voice recognition system communicates with the application server **5** and, alternatively, also CAS **7**, to generate the STN **15**. The STN **15** is then transmitted to the cardholder **1** who in turn provides to the merchant **2**. Additionally, the merchant **2** can also receive, if desired, an immediate call from the voice response unit to provide an approval code. One skilled in the art will appreciate that this system can be used in association with landline phones, cellular phones, pagers, handheld computers or any other PDA devices.

[**0078**] Another exemplary embodiment of the present invention utilizes a smart card system or similar portable data device to generate and/or distribute a STN **15** to the card provider **1** or merchant **2**. The smart card may facilitate the generation of a STN **15** in a number of different ways. In one embodiment, the smart card device itself generates

the STN **15** from a self-contained processing chip. In another embodiment, the smart card interfaces with the card provider's user interface system **4** to cause the card provider **3** to generate a number. In another embodiment, the smart card supports interaction with a merchant's transaction processing system. "Smart card" is referred to herein to include any microchip enabled transaction card that is capable of being read by a smart card reader, and is also referred herein to generally refer to any portable data device that is capable of processing information. In an online embodiment, the cardholder **1** installs a smart card reader and associated software to be used with the cardholder's computer system that is capable of connecting to the internet. When desiring to make an online purchase, the cardholder **1** swipes or inserts his smart card through a card reader and enters an appropriate PIN. Once properly authenticated, the card provider transaction system generates and issues a STN **15** to the cardholder **1**. In another embodiment, the merchant **2** may have a smart card reader capable of interfacing with the card holder's smart card. In this embodiment, the cardholder **1** swipes or inserts the smart card through the merchant's reader, a PIN is entered and the STN **15** is displayed to the merchant **2**. Additional information relating to smart card and smart card reader payment technology is disclosed in Serial No. 60/232,040, filed on Sep. 12, 2000, and U.S. Pat. Nos. 5,742,845; 5,898,838 and 5,905,908, owned by Datascape; which are hereby incorporated by reference.

[**0079**] With an exemplary online smart card embodiment, the cardholder **1** interfaces with the card provider's user interface system **4** (e.g., website) and registers the smart card for use with the transaction system option. The cardholder **1** downloads a program and the program is stored on the cardholder's computer. A STN transaction icon (e.g., Private Payments^{SM} button) appears on the cardholder's browser or an icon appears on the display (e.g., Microsoft Windows® system tray). This button, driven by a card provider specific application (activator) that resides on the cardholder's computer, appears each time the cardholder **1** launches the browser (or alternatively the button appears at any predetermined intervals, cycles or URLs).

[**0080**] The cardholder **1** suitably links to an online shopping site, orders a product or service or fills a shopping cart and goes to the payment page. The cardholder **1** clicks the STN payments button on the browser or the icon on the display (or the activator automatically launches the STN button) and a pop-up window appears, asking the cardholder **1** to enter the smart card into the smart card reader and, in a preferred embodiment, enter his PIN number. In an alternative embodiment, a PIN may not be necessary. In another embodiment, any other security data or functionality may be included. Upon entering this information, the STN **15** will be generated by the card provider's STN transaction system **18** (**FIG. 8**), or, in another embodiment (discussed below) will be generated directly from the smart card chip; and a pop-up screen containing the STN **15** number will be displayed on the computer. The cardholder **1** then "drags and drops" or "cuts and pastes" the randomly generated STN **15** and other transaction information (e.g., card type, expiration date) into the online order form and completes the transaction. In an alternative embodiment, the STN **15** and other transaction information are automatically filled into the web shopping page by the card provider's web server.

[**0081**] Another exemplary embodiment of the present invention integrates a smart card with an online merchant's website, which may or may not be utilized by the cardholder **1**. For example, in one aspect of this embodiment the smart card cardholder goes to a merchant website and a "smartchip" payments checkout button appears on the credit card payments page. The card provider's transaction system will be invoked if the card holder **1** checks out via the smartchip payments button. In a preferred embodiment, the transaction system option is "behind the scenes." The cardholder **1** goes to an online shopping site, orders a product or service or fills a shopping cart and goes to checkout page. The cardholder **1** clicks the smartchip payments button on the browser and a pop-up window appears, asking the cardholder **1** to enter the smart card into the smart card reader and, optionally, enter his PIN number. Upon entering this information, the system logs the cardholder **1** into smartchip payments checkout process. The cardholder **1** will hit "check out" and the smartchip payments checkout process may auto-generate and auto-fill the STN **15** and transaction information into the appropriate payment field (an applet may be read off of the smartcard to transfer number to merchant site.) In this embodiment, the STN **15** will be auto-generated off the chip, where the smart card chip may use the Java or Multos operating systems and may use a random number generating algorithm. In one embodiment, the smart card chip is able to access the card provider's transaction system or, alternatively, contain a pool of possible numbers (in order to avoid generating the same number twice). The number is also need sent back to the STN transaction system **18** in order to match the PPC **20** number with the STN **15**.

[**0082**] In another embodiment using a smart card, a secure electronic transaction (SET) protocol is used to avoid or minimize system/server contact. In this embodiment, the PCC **20** number is on the chip but is encoded. The SET protocol is preferably an encryption algorithm on the chip where part of the initial data would be the cardholder's PCC **20** number. The algorithm could be decoded by the card provider **3** but not by the merchant **2** to come up with the real account number. In one embodiment, the merchant **2** routes the authorization to the card provider via a BIN number rather than the PCC **20** number. When the transaction is sent from the merchant **2** to the card provider **3** for authorization, the CAS **7** preferably triggers the decode algorithm to complete the process, linking the STN **15** to the PCC **20** account.

[**0083**] Another embodiment contemplates the use of the STN **15** with a transponder system comprising a first means for generating or storing a signal that includes an encoded STN **15** and a second means for reading or receiving the signal. In an exemplary embodiment, a cardholder **1** waves a small transponder unit in front of the merchant's **2** receiving unit. The STN **15** information can be sent/received by a number of known methods (e.g. optical, magnetic, infrared, radio frequency, etc). The merchant **2** reader captures the STN **15** and forwards the STN **15** (with the associated transaction information) to the card provider's CAS **7** as previously described. The transponder units may be set up in a number of ways. Each transponder device may hold one STN **15** with certain predefined parameters or each transponder device may have several STNs **15**.

[0084] STN **15** Authorization Process (**FIG. 2**, step **115**):

[0085] Referencing **FIGS. 1 and 11**, after the secondary transaction number (STN **15**) is provided to the merchant **2**, the merchant **2** submits an authorization request to the card provider **3**, as it would with any other credit card transaction. This request is routed to a card authorization system (CAS) **7** for authorization (step **80**). The CAS **7** recognizes the transaction as involving a STN **15** and forwards the transaction information to the Authorization Request Listener. **77** program on the application server **5** (step **81**). The Authorization Request Listener **77** passes the transaction information to a CAS Authentication Component **78** (step **82**). The CAS Authentication Component **78** determines if use of the STN **15** has satisfied the previously defined conditions of use parameters. To determine this, the CAS Authentication component **78** looks to the STN database **6** for the conditions-of-use rules and the primary charge card number (PCC **20**) that are associated with the particular STN **15** (step **83**). If the use of the STN **15** complies with the rules of use, the CAS Authentication component **78** returns an authorization message and the associated PCC **20** to CAS **7** (step **84**). CAS **7** then performs an authorization request for the PPC **20**, as is typically done with any physical charge card, to ensure that the primary charge card conditions (e.g., credit limit, expiration date, etc.) have been met.

[0086] If CAS **7** authorizes use of the PCC **20**, the transaction involving the STN **15** is approved and an approval code will be generated. However, the PCC **20** must first be replaced with the STN **15** and the STN database **6** must be updated to reflect this transaction data. This is accomplished by CAS **7** returning to the CAS Authentication component **78** an approval message with the transaction data (step **85**) and CAS Authentication component **78** forwarding to a reversal processing engine **79** (step **86**). The reversal processing engine **79** interfaces with the STN database **6** to re-substitute the STN **15** for the PCC **20** and also to update the STN database **6** to reflect the transaction information (step **87**). For example, if the conditions of use parameters associated with the STN **15** authorized two transactions, this step **87** updates the cardholder account in the STN database **6** to reflect that only one transaction remains. The reversal engine **79** substitutes the PCC **20** with the STN **15** and forwards to CAS **7** (step **88**). CAS **7** then provides the results to the merchant **2** (step **89**). If the CAS Authentication Component **78** does not authorize use under the STN **15** conditions or if CAS **7** does not authorize use under the PCC **20** conditions, the transaction will not be approved. When the use conditions of both the primary charge card and the secondary transaction numbers are satisfied, the transaction is approved. In this preferred embodiment, however, the STN **15** is not deactivated to prevent settlement. To the contrary, settlement may proceed (as discussed next) even when an authorization was declined.

[0087] Additionally, use of other third party networks and systems are contemplated by the present system. One exemplary system allows a card provider **3** to associate STNs to third party accounts, offering the same fraud reduction benefits to external card issuers. Here, in this exemplary system for authorizing STN, a merchant **2** submits an authorization request to a card provider **3**. CAS **7**, recognizing the STN **15** forwards the request to application server **5**. The conditions of use are checked and the authorization request is modified to substitute the STN **15** with the associated primary account (PCC **20**). In some cases a merchant identifier may be included in the authorization request. Therefore a translation may occur to substitute the card provider **3** merchant ID with the corresponding third party card issuer merchant ID. The request is then returned back to CAS **7** for a normal authorization. CAS **7** then recognizes the account as originating from another issuer (third party issuer **92**), forwards the authorization request to a third party issuer's network for processing (step **84***a*). The network **91** routes the request to the appropriate third party issuer **92** for an authorization determination. The third party issuer **92** processes the authorization request and returns the result to CAS **7** for forwarding back to application server **5** (step **84***b*). Application server **5** saves the authorization result (approval or denial) and substitutes the PCC **20** with the STN **15** and returns to CAS **7** for forwarding to the merchant **2**.

[0088] The authorization and settlement processes may occur as separate steps or as a single step. In one embodiment, referred to herein as an electronic data capture (EDC) system, the merchant **2** sends an authorization request and if the authorization request is approved, a receipt of charges is created and submitted for the merchant **2**. Separate sequences of file transmissions or messages are therefore not required. Various embodiments, hybids, and modifications of these processes should be apparent to one skilled in this art.

[0089] STN **15** Transaction Settlement (**FIG. 2**, step **120**):

[0090] Prior art systems typically deactivate a temporary transaction number during the authorization process if limited-use conditions are not met. As previously explained, because of the uncertainty and variability of the authorization processing, this often results in a transaction numbers being unintentionally deactivated, thereby bringing the transaction processing to a sudden halt. An exemplary embodiment of the present invention overcomes this problem by not "deactivating" the secondary transaction number when predetermined conditions are not met. But instead, allowing the transaction to proceed through settlement, albeit without a valid approval code, where the merchant bears the risk that the amount will later be charged back by the card provider **3** if the transaction is disputed by the cardholder **1**.

[0091] An exemplary settlement process of this invention involves the backend systems shown in **FIG. 8**. Specifically, referencing **FIGS. 1 and 8**, the backend process utilizes a financial capture system (FINCAP) **10** to capture the settlement information (e.g., receipt of charges "ROC" and summary of charges "SOC") from the merchant **2**, a backend application service **8** to ensure that proper account information is processed, an accounts payable system **9** to pay the merchant **2**, and an accounts receivable system **11** to process the account statement that is provided to the cardholder **1**. An exemplary embodiment of the settlement process involves a settlement request being made by a merchant **2** for a transaction involving a STN **15**. All settlement requests are forwarded to the card provider's back end system **14** for processing where the request is initially sent to FINCAP **10**. FINCAP **10** captures the ROC and SOC data and identifies, via the card product identifier (or by any other suitable means), the transaction as involving a STN **15**. In another

embodiment, the product identifier (or BIN number) does not differentiate between a STN **15** and a regular charge card number. In that instance, it will be necessary for FINCAP **10** to call the backend application service **8** (which interfaces with the STN database **6**) to identify the STN **15** from other charge numbers. After the STN **15** is distinguished from the ordinary physical charge cards, FINCAP **10** verifies that the number is valid (i.e., exists in the STN database **6**). If the STN **15** is a valid number, FINCAP **10** creates a payment (accounts payable) file including the transaction data and sends a payment message to the AP system **9** instructing the merchant **2** to be paid. In paying the merchant **2**, the card provider **3** references only the STN **15** and does not release the PCC **20** or any other regular charge card numbers.

[**0092**] The back-end system **14** processes the cardholder **1** STN account information as follows. After capturing the transaction information (ROC and SOC) from the merchant **2**, FINCAP **10** creates a cardholder account (accounts receivable) file and sends a message to the back-end application service **8** to process the information for cardholder billing. Recognizing that the transaction involves a STN **15**, the back-end application service **8** replaces the STN **15** with the PCC **20**, updates the cardholder STN account information in the STN database **6** to reflect the appropriate transaction settlement information, and processes the transaction as with any other transaction. The backend application service **8** sends the transaction details to the AR system **11**, where the AR system **11** sends the proper statement to the cardholder **1**, typically referencing only the PCC **20** number. In another embodiment, the AR system **11** may process the statement where the transactions are further categorized and itemized by both the PCC **20** number and the STN **15**.

[**0093**] As previously noted, it may often be the case with prior art systems, that the temporary transaction number is inadvertently deactivated during the authorization phase and completion of the transaction is not possible. e.g., multiple payment purchases. The present transaction system overcomes this problem by ensuring that valid transaction numbers will be processed. If the conditions-of-use parameters are not met, the cardholder **1** is, under an exemplary embodiment of the present system, able to dispute the transaction and have the transaction charged back to the merchant **2** during the dispute handling process (discussed next). During this dispute handling phase, the card provider **3** will retrieve information from the STN database **6** to determine if the disputed information was "authorized", i.e., has an associated approval code. If the transaction was not "authorized" because the conditions of use parameters were not satisfied, the amount will be charged back to the merchant **2** according to predefined business rules.

[**0094**] Another embodiment provides for checking the approval codes and other conditions during settlement. Here, transaction information (approval code, SE number, or other information) may be checked during settlement. For example, the backend application service **8** (or the application server **5**) may compare transaction information to a business rule or conditions set associated with a cardholder **1** STN account. If conditions of use have not been met or if a valid approval code is missing, the service **8** or server **5** may cause a charge back to be issued to the merchant to offset the previous merchant payment. In other words, in this alternative embodiment, where an STN **15** transaction is processed through settlement, the following events may occur in sequence. First, a payment file is established once it is determined that the STN **15** is a valid number. Second, the merchant is paid. Third, the system applies the business rules or conditions for the particular account associated with the STN **15**. Fourth, if it is determined that the merchant **2** should not have been paid in the first instance because the transaction conditions were not met or an approval code was not present, the system will execute a charge back to the merchant **2**. This settlement processing may be transparent to the cardholder **1** since, before the AR system releases a cardholder billing statement, the merchant is paid and then charged-back resulting in no outstanding balance to the cardholder **1**.

[**0095**] As shown in **FIG. 8**, the present invention contemplates the interaction of clearing and settlement systems other than those of the card provider **3**. This exemplary system allows a card provider **3** to clear and settle STN transactions where an STN **15** is associated to a third party account, meaning that the merchant **2** is paid and the charge is billed to the cardholder **1**. As such, an exemplary embodiment of the present invention is configured to support interaction with third party networks and systems. Here, the backend application service **8**, upon receiving a STN **15**, recognizes that the associated PCC **20** originated with another card issuer **92**. The backend service **8** separates the transaction into two transactions (a clearing transaction and a settlement transaction). A substitution occurs in the clearing transaction where the STN **15** is replaced by the associated PCC **20**. Also, a translation may occur to substitute the card provider **3** merchant ID with the corresponding third party card issuer ID. The transactions are then forwarded to a third party clearing and settlement network **93**. The third party clearing and settlement network **93** handles the routing, as appropriate, to a merchant acquirer's accounts payable system **91** and an issuer's accounts receivable system **92**. As noted above, the accounts payable system ensures that all correspondence with the merchant **2** references the STN **15**.

[**0096**] Dispute Handling and Customer Service Process (step **125**):

[**0097**] The dispute handling process of the present invention involves situations where a cardholder **1** or merchant **2** disputes charge that is associated with a transaction involving a STN **15**. Generally, a cardholder **1** disputes a charge by contacting the charge card provider **3** via phone, mail, or internet. As previously noted, an exemplary AR system **11** typically bills the cardholder **1** with reference to only the PCC **20** number. The computer systems of the present invention allow the card provider's customer service representatives to lookup information based on, inter alia, the STN **15** or the PCC **20** number. **FIG. 12** depicts an exemplary look-up screen **175** for reviewing the primary charge card account **20** and the transactions associated with the STNs **15**.

[**0098**] With respect to a cardholder initiated dispute, the representative initiates a dispute through a dispute handling system (DHS) to obtain the case avoidance or case set rules for cardholder disputed transactions. One of the case avoidance or case set rules provides for a look up from the STN database **6** to verify that the transaction was processed with an approval code. The rule set may provide for, inter alia, an automatic charge back of the transaction amount to the

merchant if an STN **15** transaction is submitted without an approval code. The DHS or the representative initiates a cardholder **1** or merchant **2** contact (via phone, mail, internet). Disputes involving STNs **15** may be automatically routed to predefined STN queues based on industry type (i.e., airline, car rental, etc). Contact letters may be automatically filled with information retrieved from the STN database **6**. The adjustment file accesses the application server **5** (or backend application service **8**) to substitute the PCC **20** number with the STN **15**. A letter file is then generated and an electronic transmission system routes electronic contacts to and from various merchant interfaces.

[**0099**] In an exemplary system for handling disputes from merchant **2**, a merchant **2** contacts the card provider **3** via normal channels. The card provider's representative generally accesses a customer service application that is used to service merchants. This customer service application identifies the account by a STN **15** in dispute. A case is set-up with the STN **15** and is managed via adjustment management systems. The adjustment management system and a letter generating system access the STN transaction system **18** for the account number swap, where the PCC **20** number is replaced with the STN **15** for financial adjustments intended for the cardholder **1**. The remaining inquiry is processed as with existing dispute handling systems.

[**0100**] Although the previously described embodiments generally relate to a cardholder's **1** request for a STN **15**, the merchant **2** may also find it desirable to request secondary transaction numbers from the card provider **3** in order to limit exposure to credit card fraud. In traditional transaction processes, upon completing a transaction, the merchant **2** stores transaction information (including the customer's credit card number) in a merchant database. This database of information is subject to credit card fraud in that a thief could hack into the merchant's computers to steal its customer's credit card numbers. To limit exposure, the merchant **2** may desire to replace those customer credit card numbers with STNs **15** that are associated with the cardholder's primary credit card number (e.g., PCC **20**), i.e., the merchant may not want its database filled with actual customer credit card numbers. In this situation, only the card provider **3** maintains the actual credit card number and the merchant **2** retains only the STN **15**. In an exemplary process, the merchant **2** receives a regular credit card number from a cardholder **1** to facilitate a transaction. The merchant **2** submits the number to a card provider **3** for authorization, requesting that the card provider **3** instead of returning the regular credit card number, return a STN **15** (and approval code) that is associated with the regular credit card. In response, the card provider generates a STN **15**, associates the number to the regular credit card number (which becomes the primary account (e.g., PCC **20**)), checks to see if authorization is appropriate and returns the authorization record (only referencing the STN **15**) to the merchant **2**. The merchant **2** processes the transaction through the normal settlement channels, referencing the STN **15** instead of the regular credit card number. When retaining transaction records, the merchant **2** replaces the primary credit card number with the STN **15** and maintains the STN **15** in its database.

[**0101**] In another embodiment, the merchant **2** accepts only STNs **15**—not regular credit card numbers—from cardholder's to complete transactions. For the same reasons stated above, the merchant **2** may desire to limit receipt of regular charge card numbers to limit exposure to credit card fraud. In one exemplary embodiment, the merchant **2** computer system differentiates between STNs and regular charge card numbers and will not allow customers to use regular charge card numbers to facilitate a transaction (i.e., will refuse the transaction). As previously described, however, the STN **15** and the regular charge card may be transparent to the merchant **2** making it difficult for the merchant **2** to differentiate between the STN **15** and the regular charge card. In this situation, in an exemplary embodiment, the STN **15** will be identified during the authorization process by the card provider **3**, where if the STN **15** does not meet certain conditions defined by the merchant **2**, the transaction will not be authorized. For example, the merchant could require that all customer transactions be completed with a STN **15** that has limited-use conditions restricting use to the amount of the transaction or restricting use to the particular merchant. During the authorization process, the STN **15** is compared with the merchant-defined conditions where if the conditions are not satisfied, the authorization request will be denied. After completion of the transaction, and upon satisfying the merchant **2** conditions, the STNs **15** have little to no value and would be of minimal value to a potential thief.

[**0102**] Several additional embodiments of the transaction system are provided below.

[**0103**] In one embodiment, the STN database **6** is used to facilitate the merging of a newly acquired cardholder base with an established cardholder base. For example, when a bank or other institution sells a cardholder base to a card provider **3**, the card provider **3** creates new physical accounts for the acquired cardholders and does not issue new cards. The STN database **6** is updated to associate the acquired cardholder account numbers to the newly created accounts. This allows the cardholders' existing physical cards to still be used and processed appropriately. The card provider (BIN) routing is modified for the acquired accounts so authorization requests and settlements are sent to the card provider **3** instead of to the bank or other institution. CAS **7** and FINCAP **10** recognize these acquired accounts as STN **15** accounts and translate the numbers appropriately. The end result is that charges made by the acquired cardholders end up on a statement generated by the card provider **3**.

[**0104**] In another exemplary embodiment of the transaction system, a card provider **3** may provide a line of credit to a customer or to a merchant **2** or group of merchants who can private label for use by their customers. This allows the merchant **2** to provide a branded line of credit with minimal or no changes to the credit card authorization and settlement process. In one embodiment, the merchant **2** approves a line of credit or asks the card provider **3** to approve a line of credit for the customer. The card provider would then issue a STN **15** to the customer via the merchant **2**. This STN **15** is generally used with the merchants **2** who are issuing the line of credit. When the customer wants to make a purchase using the merchant's line of credit, the merchant forwards a standard credit request to the card provider **3** with the STN **15** used as the credit card number in the transaction protocol. The card provider **3** verifies that the line of credit is authorized and was submitted by the merchant **2** issuing the line of credit associated with this STN **15**. The card provider transaction system (via the STN transaction system **18**) is capable of denying usage of this line of credit at another

non-participating site. The card provider **3** may provide a private label or co-branded web site to apply for the line of credit. The card provider's back end system **14** then bills the customer and pays the merchant. The merchant **2** may keep the electronic line of credit privately at their site, or provide it to the customer. The authorization system would not authorize usage at other sites.

[**0105**] **FIG. 13** depicts an exemplary transaction process for use in providing lines of credit to merchants **2**. A cardholder **1** or customer (who may or may not be an existing card member of the participating card provider **3**) applies for an electronic line of credit (ELOC) with a merchant **2** (step **221**), the merchant **2** redirects the cardholder **1** to the card provider's **3** website to fill out the ELOC application **30** (step **222**). A fraud check **31** is performed (step **223**) and a credit inquiry is typically performed by any credit bureau company **33** (step **224**). If a card processing system **32** determines that credit is acceptable, an account is set up (step **225**). A physical card **34** is not generated as with typical processes and may need to be purged depending on the particular system set-up (step **226**). The account is sent to the account management system **35** (step **227**) and then forwarded to the STN database **6** and the application server **5** (step **228**). The cardholder **1** account is then related to a valid merchant identification number such as the SE number **36** (step **229**). An account is then set-up with a ELOC profile **37** and at this point the secondary transaction ELOC number is passed back to the cardholder **1** (step **230**). The merchant **2** submits the ELOC payment request to CAS **7** (step **231**), and CAS **7** routes the ELOC to the STN system (step **232**), where the STN system verifies that the SE number is approved for this particular ELOC (step **233**). The STN system translates the ELOC STN to the related account in the account management system and returns the ELOC STN to merchant (step **234**). The merchant is then required to submit the authorization code with the receipt of charges (ROC) and summary of charges (SOC). The merchant submits the ROC and/or SOC to the card provider's FINCAP **10** (step **235**), whereupon FINCAP forwards the ELOC to the STN system (step **236**). The STN system verifies that (i) this SE number is valid for the particular ELOC account (step **237**) and (ii) the particular transaction was authorized for the specific ELOC account (step **238**). The STN system then flips the card number, returns it to FINCAP **10**, whereupon, the number is forwarded to the card provider's accounts receivable system **11** (step **239**). FINCAP forwards the ELOC STN and associated information to the Accounts Payable system **9** (step **240**) and pays the merchant **2** (step **241**).

[**0106**] Another exemplary embodiment allows a cardholder to fund an online digital wallet with the secondary transaction number. In this embodiment, after generation and association with the primary charge card, the secondary transaction number is provided to the cardholder to use within a designated digital wallet, which may reside locally at the cardholder's computer or may be stored in an online password protected account.

[**0107**] In yet another alternative embodiment, the secondary transaction system may be used to facilitate programs involving non-currency tender, such as the American Express® Membership Rewards as Currency™ system that is detailed in U.S. Provisional Application No. 60/200,492, filed on Apr. 28, 2000, and U.S. Provisional Application No. 60/201,114, filed on May 2, 2000, which are hereby incorporated by reference. One embodiment of this system, depicted in **FIG. 14**, allows a cardholder **1** to create a STN **15** to be used to spend membership rewards points. In general, a membership or incentive rewards program is a loyalty program that rewards cardholders for using their charge card to make purchases. Cardholders accumulate points by using a participating charge card or by purchasing products at a participating merchant. These points may then be converted to a monetary value and redeemed to purchase merchandise.

[**0108**] As depicted in **FIG. 14, a** cardholder **1** accesses and logs onto the card provider's services via a user interface system **4** (e.g., an Internet connection) (step **251**). The cardholder **1** proceeds (clicks on hyperlink) to the membership rewards (MR) system **95**, where she indicates that she would like to use her membership reward points that are available in her MR account (step **252**). The MR system **95** reports to the cardholder **1** how much the available MR points are worth (step **253**). The cardholder **1** indicates how many of the MR points (converted to monetary value) should be loaded info an account that can be used for purchases (step **254**). In an exemplary embodiment, the STN **15** can be associated with a MR account, i.e., a primary charge card account that is funded with these MR points. Use of this MR account may be limited by the card holder **1** or the card provider **3**, or could be further limited by the MR system rules of use that may have been predefined by participating merchants (step **255**). Once the MR system **95** has approved the request and allocated the requested MR points, the STN system **18** associates a STN **15** and establishes an MR-STN **15** profile (**256**). The MR-STN profile contains the options that will be applied and the amount that will be available to the resulting STN **15**. The STN system **18** returns the STN **15** (and other account information) to the MR system **95** to provide to the cardholder **1** for use in completing subsequent transactions (e.g., online purchases) (step **257**).

[**0109**] When desiring to purchase products using the MR point-funded STN **15**, the cardholder **1** proceeds to a merchant site (e.g., online website), selects goods and is requested by the merchant to provide payment information (e.g., via an online payment web page). The cardholder **1** chooses the appropriate card provider **3** as the form of payment (e.g., American Express®, Visa®, etc.) and enters the STN **15** (and other needed information) into the appropriate payment fields (step **258**). The merchant processes the STN **15** authorization as discussed above (step **259**), where the card provider CAS **7** recognizes the transaction as involving a STN **15**, and forwards the request to the STN system **18** containing, inter alia, an application server (**FIG. 8**, number **5**) and a STN database (**FIG. 8**, number **6**). It should be appreciated that profile information may be stored in a MR database, STN database **6** or any other suitable database (step **260**). The STN system **18** recognizes the account as a MR account, and verifies that optional conditions, if any, are met. If the conditions are not met, an error is returned to CAS **7** and then to the merchant (step **261**). If the conditions are met, the balance available on the MR-STN profile is reduced by the purchase amount, a record of the purchase is recorded in the MR-STN profile, and an approval code is returned to the authorization system (step **262**) and then to the merchant (step **263**). Although additional CAS **7** processing is contemplated by this embodi-

ment, application of additional rules and validations—which would typically be applied—are not required for this type of account. The approved purchase is finalized by the merchant with the STN **15** transaction being submitted through the merchant's existing POS network for settlement (step **264**). The STN **15** transaction is received by the card provider's financial capture system (FINCAP) **10** (step **265**). The FINCAP **10** forwards the STN transaction to the appropriate AP system **9** (step **266**). The AP system **9** then pays the merchant according to the appropriate settlement terms and conditions (step **267**). The FINCAP **10**, having identified the transaction as involving an STN **15**, sends the transaction information to the STN system **18** (via a backend application service **8**) to identify the actual account number (i.e, PCC **20**) (step **268**). The STN system **18** recognizes that the STN **15** is associated with a MR account, searches for the MR-STN profile and passes a credit request to the appropriate cardholder **1** MR account to reduce the available MR points (step **269**), and (ii) the transaction record is used to build a credit against the actual charge card account (e.g., PCC **20**) that will offset the charged STN **15** transaction (step **269***b*). In the first instance (step **269**), the STN system **18** passes a request to the MR system **95** to deduct the appropriate number of MR points. In the second instance (step **269***b*), both the original transaction and the credit are passed back to FINCAP **10** with the actual charge card account number (e.g., PCC **20** number). The FINCAP **10** then forwards the charge and credit transactions to the appropriate AR system **11** for normal billing processing.

[**0110**] As shown, the embodiment depicted in **FIG. 14** allows the cardholder **1** to spend the MR points in at least two ways. First, the membership reward points can be deducted at the time of the transaction processing, or second, the transaction can be reflected on the cardholder's bill along with an associated credit that reflects the payment with reward points. It should also be appreciated that a cardholder **1** may choose to use MR points on a transaction by transaction basis, and preferably, is able to combine variations of currency (e.g., credit, debit cards etc.) and non-currency tender (MR points), as desired, to effectuate a transaction. Additionally, both currency and non-currency tender may be integrated into a STN gift, where a first party gifts to a second party a secondary transaction number that has some currency or non-currency value.

[**0111**] Another membership rewards embodiment is shown in **FIG. 15**. Here, the cardholder **1** is able to choose to use membership reward points when shopping at a merchant **2** site that supports the membership rewards as a payment option. Referencing **FIG. 15**, the cardholder **1** goes to a participating merchant's site (e.g., online website) to shop for goods or services. The cardholder **1** selects merchandise and continues to a payment site, where the card provider's MR points is one of the payment options (step **301**). When the cardholder selects this option, a secure connection is established with the card provider **3** that authenticates both the cardholder **1** and the merchant **2** (step **302**). The card provider **3** requests the cardholder's user ID and Password, either through a pop up screen, a http redirect link, or an applet downloaded by the merchant (step **303**). The cardholder **1** supplies the User ID and Password which is returned to the card provider with the purchase amount (step **304**). The card provider user interface **4** (e.g., online services) causes the cardholder **1** to be authenticated, collects the associated registered card accounts and invokes the MR system **95** (step **305**). The MR system **95** uses these card accounts to identify the cardholder's MR account (step **306**). If none of the registered accounts are related to a MR account, the cardholder **1** is not able to use MR points to pay for her purchase and an error is returned to the cardholder **1**. After identifying the MR account, the MR points available are converted to the corresponding cash equivalent and compared to the purchase amount being requested. If the purchase amount is greater than the MR cash equivalent, an error is returned to the cardholder **1** (step **307**). If the MR cash equivalent is greater than the purchase amount, all card accounts participating in the MR account are collected and returned to the cardholder **1** (step **308**). The cardholder **1** designates the card account to be used to house all succeeding financial activity, which is then returned to the card provider **3** (step **309**). The card provider **3** then triggers the STN system **18** to establish a STN **15** that is associated to the selected MR account number and a MR-STN account profile is set-up (step **310**). The STN system **18** returns the STN **15** to the User Interface System **4** and then onto the cardholder **1** (step **311**), the cardholder **1** cuts and pastes, drags and drops, or auto-fills the STN **15** (and needed information) nto the appropriate merchant payment field (step **312**).

[**0112**] As previously noted, the merchant uses the existing authorization network to request authorization for the STN transaction (step **313**). The CAS **7** recognizes the transaction as one involving a STN **15** and forwards to the STN system **18** (step **314**). The STN system **18** identifies the associated actual account number (e.g., PCC **20** number) for the STN **15** (step **315**) and also recognizes the account as a MR account. At this point, although all MR transactions would have been previously verified, the MR account balance is again checked to minimize possible fraud (e.g., fraud involving two requests using the same MR points). The cash equivalent for the MR points for the actual account are then retrieved from the MR system **95** and if the purchase amount is greater than the available amount, a denial is returned to the authorization system and to the merchant **2** (step **316**). If the cash equivalent value of the MR points exceeds the purchase amount, the STN system records the purchase in the MR-STN profile and returns the STN **15** to the CAS **7** (step **317**). The CAS **7** then completes the authorization for the actual account (e.g., ensuring that the limits for the PCC **20** are complied with) (step **318**), and returns the results (e.g., approval code) to the merchant **2** (step **319**).

[**0113**] The approved transaction is finalized by the merchant **2** with the STN transaction being submitted through the existing point of sale network for settlement (step **320**). As before, the transaction information is received by the card provider FINCAP **10** (step **321**) and then forwarded to the appropriate AP system **9** (step **322**) for payment (step **323**). Since the transaction involves a STN **15**, FINCAP **10** directs the transaction to the STN system **18** to identify the PCC **20** (step **324**). The STN system **18** identifies the PCC**20** (step **325**) and also recognizes the STN **15** account is set up using MR points, where the STN system **18** searches the MR-STN profile for the associated purchase record (step **326**). The STN system either (i) passes a credit request to MR to reduce the MR points (step **326***a*), or (ii) creates a credit against the billing transaction (step **326***b*). In step **326***a*, the STN system **18** passes a request to the MR system **95** to deduct the appropriate number of MR points. Here it is not necessary to return the AR transaction information to FINCAP for forwarding to the AR system **11**, but a recon-

ciliation entry is created to reconcile the AR for FINCAP **10**. In step **326***b*, a transaction record is used to build a credit against a real account number (e.g., PCC **20**) that will offset the charge transaction. The STN system **18** forwards this credit to the FINCAP **10**. The original billing transaction is returned to the FINCAP to appear on the cardholder's **1** statement. The FINCAP **10** then forwards the charge transaction to the appropriate AR system for normal processing. The FINCAP **10** forwards the credit issued by the MR system **95** to the appropriate AR system **11** for normal billing processing. Accordingly, the cardholder **1** will see on her statement a credit reflecting the currency value of the MR points used and a charge in the amount of the transaction.

[**0114**] Another embodiment provides for the generation of one or more STNs that are subordinate to and associated with a main secondary transaction number that, as described above, is associated with the cardholder's PCC **20** account. As noted above, these subordinate numbers may also be digitally stored in devices such as wireless telephones, PDAs, handheld computers, and the like. Providing multiple layers of secondary transaction number provides the cardholder **1** with greater flexibility. For example, a cardholder on vacation could structure the main STN **15** to be valid for the duration of the vacation. The cardholder **1** is then able to generate subordinate secondary transaction numbers (or tertiary numbers) with varying preferences to take into account various activities that may occur during the vacation. A cardholder **1** could structure the main secondary transaction number to have a maximum credit limit of $3,000 (this assumes that the associated primary charge card credit limit is equal to or greater than $3,000) that is good for the duration of the vacation. A subordinate secondary transaction number may then be provided to the spouse with a $1,000 limit and additional secondary transaction numbers, restricted to $500 limits, could be provided to the children. Each subordinate card would be valid only for the duration of the vacation and would only be valid for the maximum dollar amount specified.

What is claimed is:

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

identifying at least one primary account;

generating a secondary transaction number that is configured to facilitate a transaction;

associating the secondary transaction number with said at least one primary account; and

issuing the secondary transaction number to a first party to facilitate a transaction with a second party, wherein the secondary transaction number is configured to be immediately usable for facilitating the transaction.

2. The method of claim 1, wherein the step of identifying said at least one primary account further comprises the steps of receiving information from the first party specifying a particular account; and verifying that the account exists and is valid.

3. The method of claim 1, wherein the step of generating a secondary transaction number further comprises the steps of:

generating a random number;

determining if the random number is available for use; and if available for use,

appending appropriate formatting and product identifier numbers to the random number to achieve a secondary transaction number that is configured to have the same format as the primary account number.

4. The method of claims **1** or **3**, wherein the secondary transaction number is generated by a computer system.

5. The method of claims **1** or **3**, wherein a portable data device is configured to generate the secondary transaction number.

6. The method of claims **1** or **3**, wherein a portable data device is configured to support interaction with a card provider's user interface system to generate the secondary transaction number.

7. The method of claim 5, wherein a portable data device reader is configured to support interaction with the portable data device.

8. The method of claim 1 or **3**, wherein the secondary transaction number is generated by a first party's computer system configured to support interaction with a card provider's user interface system.

9. The method of claim 1, wherein the step of associating the secondary transaction number with the primary account further comprises the step of recording the secondary transaction number in a database associated with the primary account.

10. The method of claim 1, wherein the primary account is associated with a physical charge card.

11. The method of claim 1, wherein the step of issuing the secondary transaction number to a first party is facilitated by a user interface system.

12. The method of claim 11, wherein the user interface system comprises at least one of the following: a web server system, a telephone system, and a mail handling system.

13. The method of claim 1, further comprising the steps of registering a first party to use a transaction system configured to generate and issue a secondary transaction number; and upon proper registration, providing the first party with authentication information;

14. The method of claim 13, where the authentication information is a username and password.

15. The method of claim 1, further comprising the steps of:

prompting the first party for authentication information to confirm that the first party is a registered user; and

receiving authenticating information from the first party, and upon verifying that the first party is registered, providing the first party access to a transaction system.

16. The method of claim 15, further comprising the step of receiving a request from the first party for a secondary transaction number.

17. The method of claim 1, further comprising the steps of:

allowing the first party to select and define conditions-of-use parameters, wherein the parameters place limits on how the secondary transaction number may be used; and

associating the conditions-of-use parameters with the secondary transaction number.

18. The method of claim 17, further comprising the step of storing the condition of use parameters in one or more account database fields associated with the secondary transaction number.

19. The method of claim 17, wherein the conditions of use parameters comprise at least a secondary transaction number credit limit and an expiration date.

20. The method of claim 1, comprising the following steps:

receiving transaction information from a second party for authorization;

forwarding the transaction information to a card authorization system for authorization processing;

processing the transaction information with the card authorization system, wherein the card authorization system interfaces with a secondary transaction number system to determine if authorization is appropriate.

21. The method of claim 20, further comprising the steps of:

recognizing that the transaction information comprises a secondary transaction number;

retrieving account information that is associated with the secondary transaction number;

determining if conditions of use associated with the primary account are satisfied;

determining if conditions of use associated with the secondary transaction number are satisfied;

returning an appropriate approval code to the second party, if conditions of use parameters associated with the secondary transaction number and the primary account are satisfied; and,

declining the authorization request if either the conditions associated with the primary account or the secondary transaction number are not satisfied.

22. The method of **21**, wherein the conditions of use parameters associated with the primary account include at least an expiration date.

23. The method of claim 1, comprising the following steps:

receiving transaction settlement information from a second party, wherein the transaction was facilitated using a secondary transaction number;

identifying the transaction settlement information as a transaction involving a secondary transaction number; and verifying that the secondary transaction number is a valid number;

capturing the transaction settlement information in a financial capture system, and causing the second party to be paid.

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

identifying the primary account that is associated with the secondary transaction number;

replacing the secondary transaction number with the primary account number;

processing the transaction settlement information in an accounts receivable system; and

generating a billing statement that includes at least the primary account number.

25. The method of claim 24, further comprising the steps of comparing the transaction settlement information with conditions of use parameters associated with the secondary transaction number to determine if the conditions of use have been satisfied.

26. The method of claim 1, further comprising the step of configuring the secondary transaction number for use with an electronic line of credit system.

27. The method of claim 1, further comprising the step of configuring the secondary transaction number for use with a stored value card system.

28. The method of claim 1, further comprising the step of configuring the secondary transaction number for use with a non-currency based account program.

29. The method of claim 1, further comprising the step of configuring the secondary transaction number to be used as a gift product.

30. The method of claim 1, further comprising the step of configuring the secondary transaction number to be used in an online wallet system.

31. A method of processing authorization and settlement requests in a transaction system comprising the steps of:

receiving an authorization request from a second party, where the authorization request involves a secondary transaction number with limited-use conditions associated therewith;

routing the authorization request to a card authorization system to determine if limited use conditions have been satisfied;

returning to the second party a message declining authorization if the conditions have not been satisfied; and

returning to the second party a message approving authorization request if conditions have been satisfied.

32. The method of claim 31, further comprising the step of receiving from the second party a settlement request for payment of a transaction involving a secondary transaction number; wherein the second party is paid if the secondary transaction number is valid.

33. A method of claim 32 further comprising the steps of:

routing the second party settlement request for payment to a financial capture system,

creating an accounts payable file and routing the accounts payable file to an accounts payable system for payment processing; and

creating an accounts receivable file and routing the accounts receivable file to a service that retrieves the associated primary account number and replaces the secondary transaction number with the primary account number and forwards the resulting accounts receivable file to an accounts receivable system to generate the first party billing statement.

34. A host computer system for facilitating transactions comprising:

a user interface system configured to allow a first party to interact with a host computer's transaction services; and

a number generating and processing mechanism, including at least one application server and at least one database, configured for receiving input from the user interface system to generate a secondary transaction number and to associate therewith a designated primary account.

35. The host computer system in claim 34, further comprising a card authorization processing mechanism configured to receive transaction information from a second party, wherein the authorization mechanism interfaces with at least the number generating and processing mechanism to determine if the second party authorization request should be approved or denied.

36. The host computer system in claim 34 or **35**, further comprising a settlement processing mechanism including at least a financial capture system configured for capturing transaction information relating to use of secondary transaction numbers, an accounts receivable system for billing the first party and an accounts payable system for paying the second party.

37. The system of claim 34, wherein the user interface system comprises at least one of the following: web server system, telephone system, and mail handling system.

38. A method for facilitating a transaction comprising the steps of:

registering with a card provider to use a transaction system;

logging-in to the card provider's transaction system by providing authenticating information, and causing card provider to verify that a first party is a registered and authorized user;

designating at least one transaction account as at least one primary account;

requesting a secondary transaction number from the card provider, causing the card provider to generate a secondary transaction number and to associate the secondary transaction number with the previously selected said at least one primary account; and,

receiving the secondary transaction number from the card provider.

39. The method of claim 38, further comprising the step of providing the secondary transaction number to a second party to facilitate a transaction.

40. The method of claim 38, further comprising the step of selecting conditions of use parameters to be associated with the secondary transaction number.

41. The method of claim 38, further comprising the step of defining conditions of use parameters to be associated with the secondary transaction number.

42. The method of claim 38, wherein the steps occur online.

43. The method of claim 38, wherein said at least one primary account is a non-currency based account.

44. The method of claim 38, wherein said at least one primary account is associated with an electronic line of credit system.

45. The method of claim 39, further comprising the step of disputing a charge for a transaction involving a secondary transaction number, and causing the card provider to charge back the charge to the second party.

46. A method for facilitating a non-currency based transaction system involving a secondary transaction number comprising the steps of:

designating a non-currency based account as at least one primary account;

generating a secondary transaction number and associating said secondary transaction number with at least one primary account, wherein said at least one primary account includes at least the designated non-currency based account;

converting accumulated non-currency based tender into currency to fund the primary account.

47. The method of claim 46 further comprising the step of designating condition of use parameters and associating said parameters to the secondary transaction number.

48. The method of claim 47 further comprising the step of processing an authorization request from a second party relating to a transaction involving a secondary transaction number associated with at least a non-currency based account comprising the further steps of:

recognizing the transaction as involving a non-currency based account;

verifying the conditions of use have been satisfied; and if satisfied,

reducing the non-currency based account balance by the transaction amount.

49. The method of claim 47 further comprising the step of processing a transaction settlement request from a second party relating to a transaction involving a secondary transaction number associated with at least a non-currency based account further comprising the steps of:

capturing transaction settlement information in a financial capture system, wherein an accounts payable file is created and the second party is paid.

forwarding the transaction settlement information to an accounts receivable system;

recognizing that the transaction settlement information comprises a secondary transaction number that is associated with at least a non-currency based account;

issuing a credit equal to the transaction charge amount from the non-currency based account to the accounts receivable system; wherein the credit from the non-currency based account offsets at least part of the transaction charge.

50. A method for facilitating an electronic line of credit system involving a secondary transaction number comprising the following steps:

issuing a line of credit to a participating first or second party;

causing to be processed an application from the first party requesting to be issued a secondary transaction number;

causing to be issued to the first party a secondary transaction number that is associated with the line of credit; wherein the secondary number is used to facilitate a transaction.

51. The method of claim 50 further comprising the steps of:

providing the secondary transaction number to a first party, wherein the secondary transaction number may only be used with a specified second party to facilitate a transaction.

52. A dispute handling method for facilitating a disputed transaction involving a

secondary transaction number, comprising the steps of:

receiving a dispute from a first party relating to a transaction involving a secondary transaction number associated with at least one primary account;

retrieving transaction information from a database;

replacing the primary account number with the secondary transaction number in order to initiate a second party inquiry; wherein the second party inquiry references only the secondary transaction number.

53. The method of claim 52, further comprising the steps of:

determining if a valid approval code is associated with the secondary transaction number; and

charging back to the second party the amount of the transaction, if a valid approval code does not exist.

54. A method for facilitating a transaction, comprising the steps of:

receiving a primary account number from a first party to initiate a transaction;

sending the primary account number to a card provider, requesting that the card provider generate and return a secondary transaction number that is associated with the primary account number;

receiving from the card provider the secondary transaction number associated with the primary account, wherein the secondary number is then used to facilitate a transaction settlement.

55. A method of claim 54, wherein the step of sending the primary account number to a card provider occurs during a card authorization process.

56. A method of claim 54, further comprising the step of purging the primary account number from the second party's records and replacing with the associated secondary transaction number.

* * * * *