US 20140337224A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2014/0337224 A1

(43) Pub. Date: Nov. 13, 2014

Mohapatra

(54) **CARDHOLDER CHANGEABLE CVV2**

(71) Applicant: **Sarada Mohapatra**, Naperville, IL (US)

(72) Inventor: **Sarada Mohapatra**, Naperville, IL (US)

(21) Appl. No.: **14/270,644**

(22) Filed: **May 6, 2014**

Related U.S. Application Data

(60) Provisional application No. 61/820,170, filed on May 7, 2013.

Publication Classification

(51) **Int. Cl.**

G06Q 20/40 (2006.01)

G06Q 20/24 (2006.01)

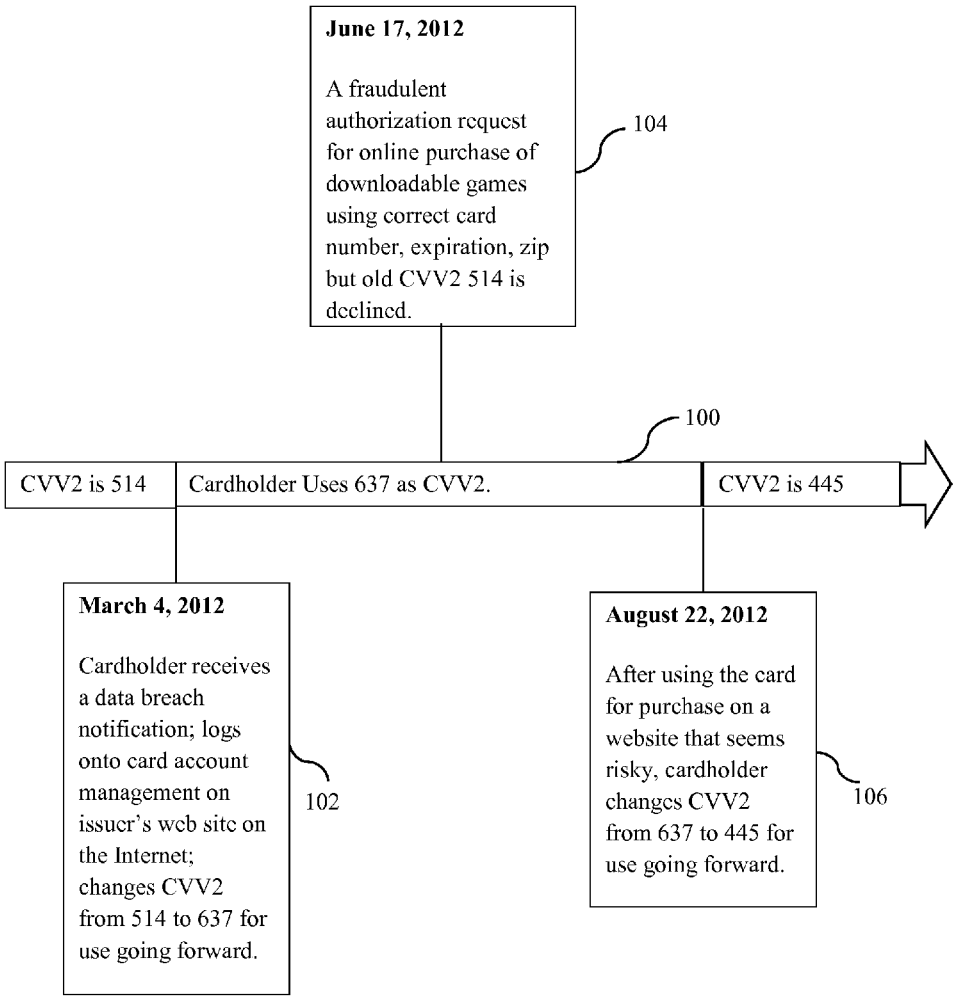
(52) **U.S. Cl.**

CPC ***G06Q 20/4018*** (2013.01); ***G06Q 20/24*** (2013.01)

USPC **705/44**

(57) **ABSTRACT**

System and methods for countering credit card fraud comprising cardholder changeable card security code CVV2 (also known as CVC2/CID). It enables cardholder to optionally choose a CVV2 different from the one printed on the card, storing/recording it on card issuer database and from then on use it as a secret separate from the card, changing it as needed, for example on being notified of financial institution data breach, or after an online transaction that seemed risky or periodically as a security practice. Fraudulent authorization requests would be rejected when CVV2 submitted does not match cardholder changed value. This system may be implemented with no or modest change in existing credit cards; terminals, equipment, computer software and communication protocols used in transaction authorization. It may facilitate adoption by making cardholders active participants in fraud prevention with modest, optional, easy to comprehend change not tied to each transaction.



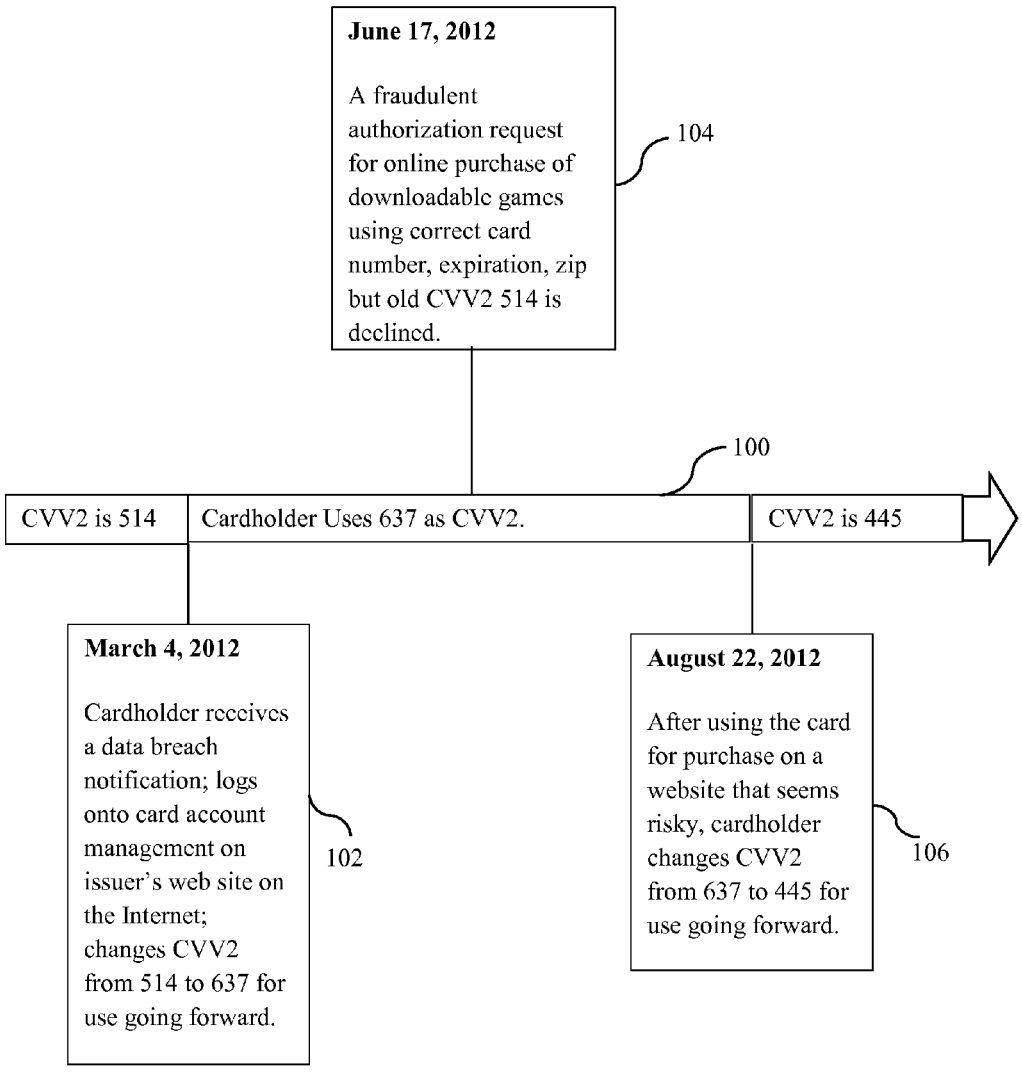

June 17, 2012
A fraudulent authorization request for online purchase of downloadable games using correct card number, expiration, zip but old CVV2 514 is declined.
104
100
CVV2 is 514
Cardholder Uses 637 as CVV2.
CVV2 is 445
March 4, 2012
Cardholder receives a data breach notification; logs onto card account management on issuer's web site on the Internet; changes CVV2 from 514 to 637 for use going forward.
102
August 22, 2012
After using the card for purchase on a website that seems risky, cardholder changes CVV2 from 637 to 445 for use going forward.
106

FIG. 1

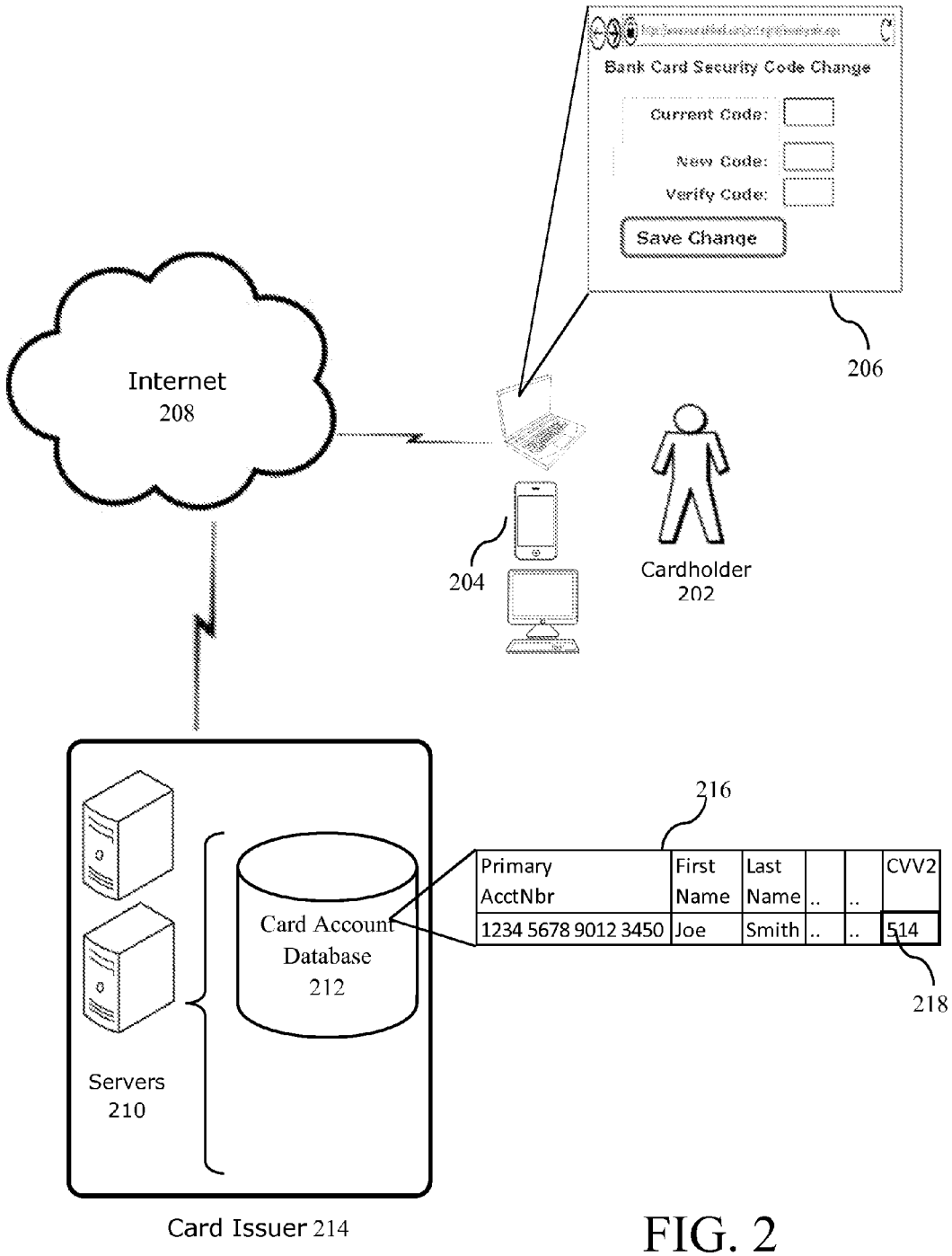

Bank Card Security Code Change
Current Code:
New Code:
Verify Code:
Save Change
206
Internet
208
204
Cardholder
202
216
Primary AcctNbr
First Name
Last Name
CVV2
1234 5678 9012 3450
Joe
Smith
514
218
Card Account Database
212
Servers
210
Card Issuer 214

FIG. 2

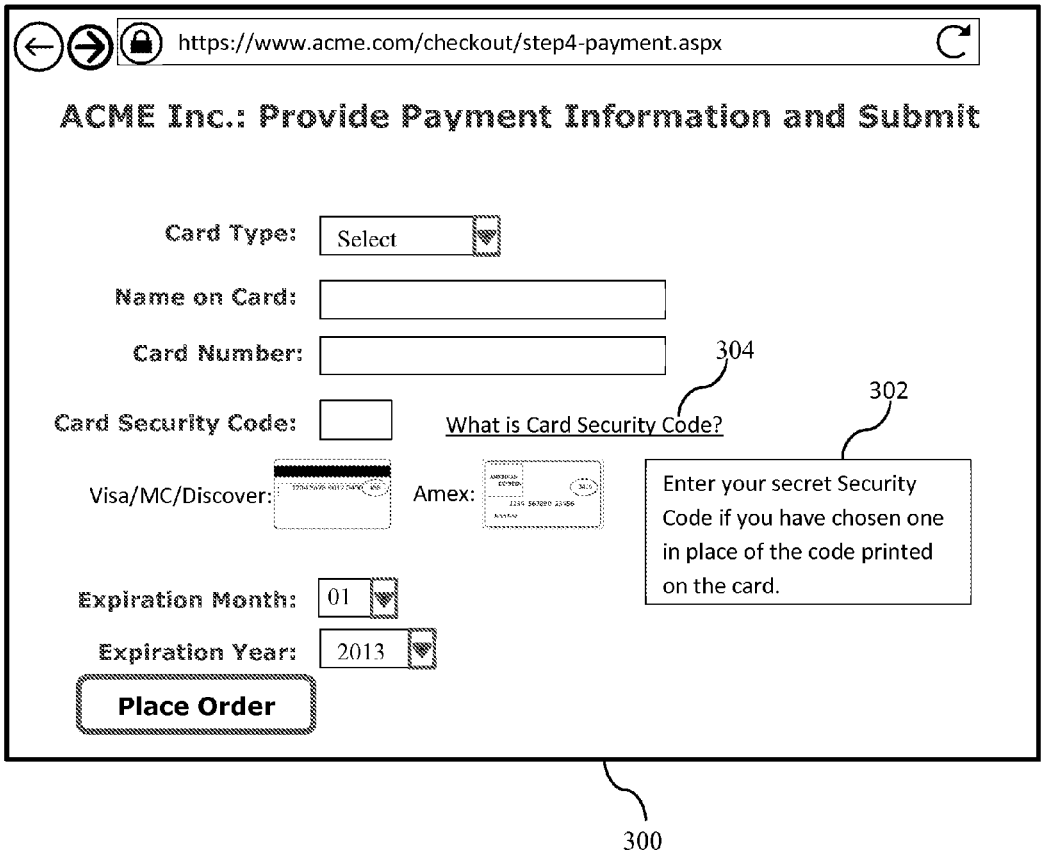

https://www.acme.com/checkout/step4-payment.aspx
ACME Inc.: Provide Payment Information and Submit
Card Type:
Select
Name on Card:
Card Number:
Card Security Code:
What is Card Security Code?
304
302
Visa/MC/Discover:
Amex:
Enter your secret Security Code if you have chosen one in place of the code printed on the card.
Expiration Month:
01
Expiration Year:
2013
Place Order
300

FIG. 3

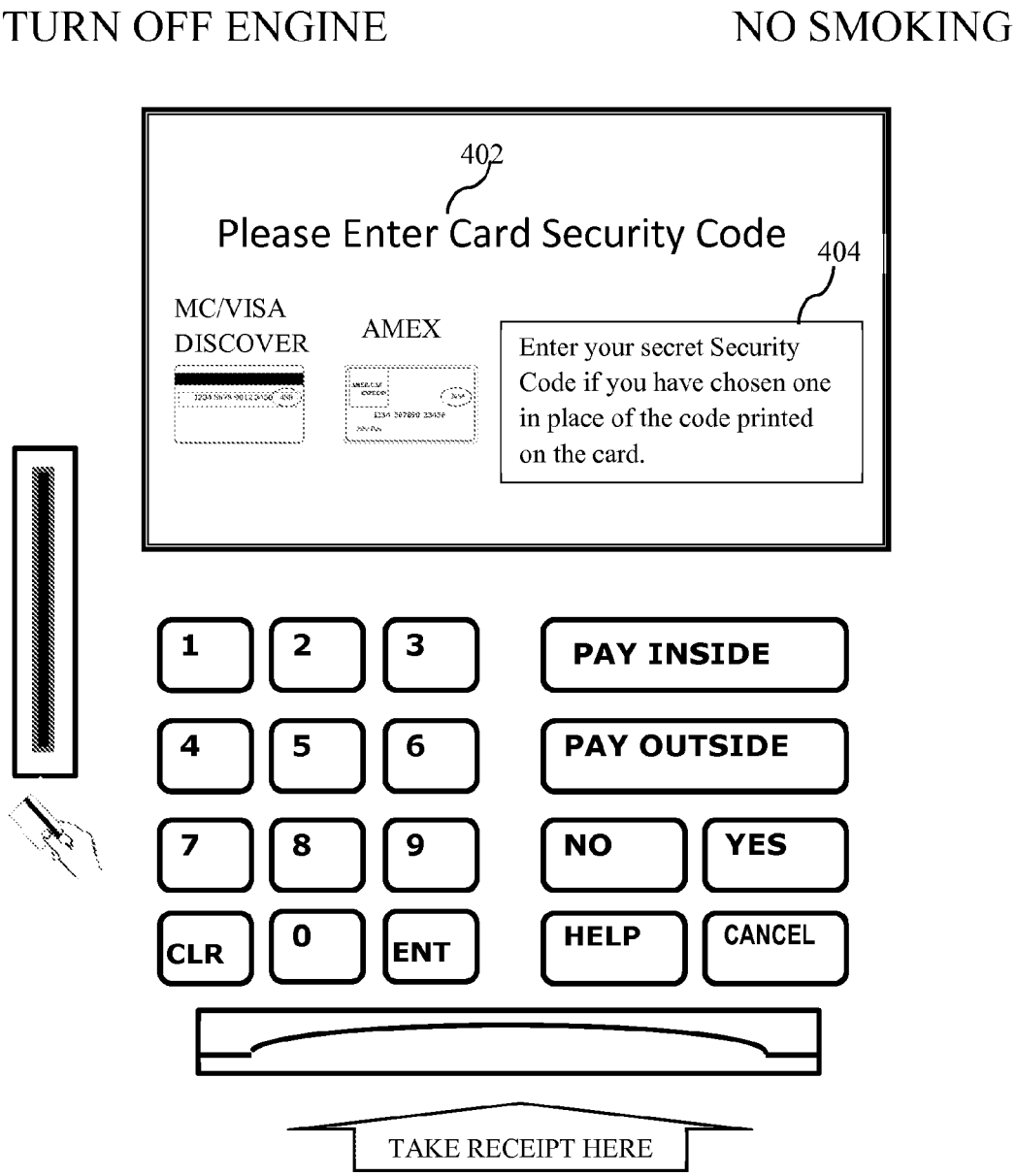
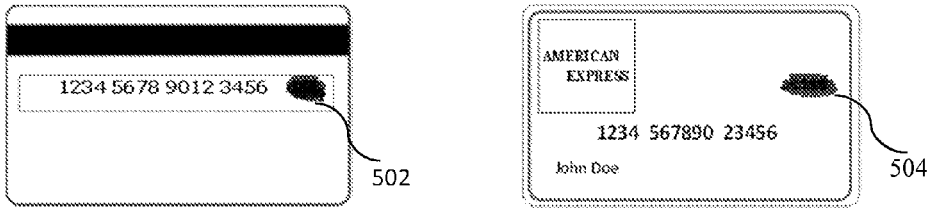

TURN OFF ENGINE
NO SMOKING
402
Please Enter Card Security Code
404
MC/VISA
DISCOVER
AMEX
Enter your secret Security Code if you have chosen one in place of the code printed on the card.
1
2
3
PAY INSIDE
4
5
6
PAY OUTSIDE
7
8
9
NO
YES
CLR
0
ENT
HELP
CANCEL
TAKE RECEIPT HERE

FIG. 4


1234 5678 9012 3456
502
AMERICAN EXPRESS
1234 567890 23456
John Doe
504

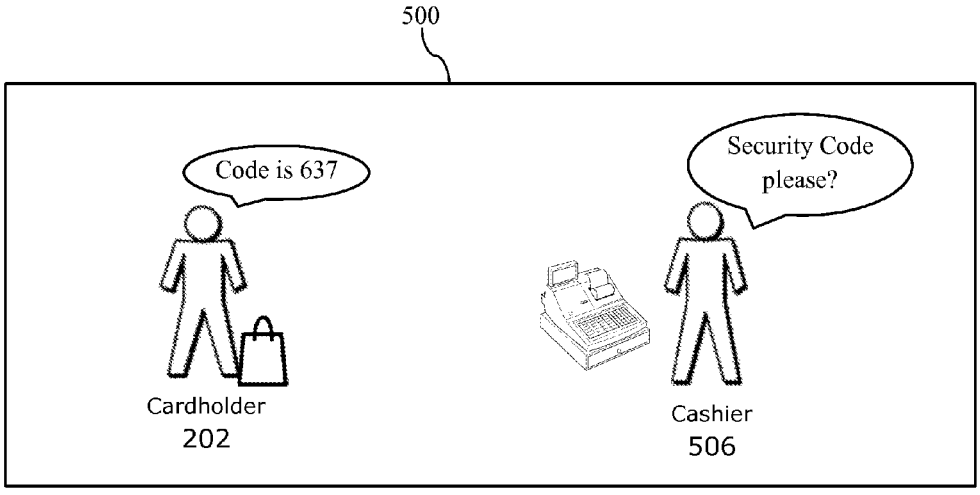

500
Code is 637
Cardholder
202
Security Code please?
Cashier
506

FIG. 5

CARDHOLDER CHANGEABLE CVV2

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of, and claims priority to, U.S. patent application Ser. No. 61/820,170, entitled "Cardholder Changeable CVV2" filed on May 7, 2013.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0002] Not Applicable

REFERENCE TO SEQUENCE LISTING, A TABLE, OR A COMPUTER PROGRAM LISTING COMPACT DISK APPENDIX

[0003] Not Applicable

BACKGROUND

[0004] Credit card use for payment of goods and services in card-present as well as card-not-present transactions has been increasing in number as well as value. Along with usage, credit card fraud has increased.

[0005] In response, measures have been and are being adopted to prevent and detect fraud. Most preventive measures involve issuers, acquiring banks, merchants and card networks with expectation from cardholders limited to fraud detection by monitoring card accounts and promptly reporting lost cards and fraudulent charges. Turning millions of cardholders into first line of defense would be an effective part of a multi-layer anti-fraud strategy. Near ubiquitous Internet connectivity and increasing use of issuer provided secure web portals for credit card account management as well as mobile device account management applications may facilitate cardholder participation in preventive anti-fraud measures on an ongoing basis.

[0006] Enlisting cardholders in fraud prevention would additionally leverage cardholder's knowledge and risk assessment specific to him/her. A cardholder may recognize increased fraud risk, for example, after clicking a link in an unexpected email which could be a phishing attack, after using an ecommerce site that is not reputable and after a vacation where card is used in unfamiliar establishments far from home and thus be motivated to undertake mitigating action if provided capability to do so.

[0007] All the data used to authenticate cardholders of regular non-chip credits cards and used during credit card authorizations are currently static. In addition to card account number, card holder name, expiration month-year that are visible on the card, the card security information in the magnetic strip and card security code (also known as CVV**2** , CVC**2** or CID) do not change from the time a card is issued. Elements of cardholder's identity often used for additional authentication such as address, billing zip code also usually do not change. This makes it possible for fraudulent charges to get authorized days, weeks and sometimes months after card details are compromised.

[0008] In recent years, there have been many computer data breaches where personal and financial information including credit card information on computer systems of merchants, ecommerce sites, corporations and government agencies were compromised. The frequency and high number of credit card accounts involved, sometimes numbering in millions, make it costly for issuers and inconvenient to cardholders to replace all the cards in each instance. The cardholders are notified of the data breach due to notification laws in many jurisdictions. These notifications may trigger mitigating action on part of cardholder if means to do so were available.

[0009] Adoption of various fraud prevention measures have often been constrained by substantial cost of technology and change requirements to issuers, merchants, acquirers and card networks. Cardholders have not embraced some of the technologies due to additional and/or unfamiliar steps.

[0010] Thus, there is a need for fraud prevention measure where cardholder plays an active role, which enables cardholder to respond to risks as they are identified, which does not greatly alter the ease and convenience of every day card use for the cardholders and reduces fraud risks without greatly increased costs and overheads.

SUMMARY

[0011] Accordingly, embodiments of the present invention may reduce credit card fraud by enabling cardholders to play an active role in fraud prevention and react to fraud risk events without greatly increased costs and overheads.

[0012] An illustrative embodiment of the present invention may provide capabilities for cardholders to choose a CVV2 different from the one printed on the card when issued, storing/recording it on card issuer database and from then on use it as a secret separate from the card, changing it as needed, for example on being notified of financial institution data breach, or after an online transaction that seemed risky or periodically as a security practice.

[0013] An embodiment of the present invention may be implemented with no or modest change in existing credit cards, terminals, equipment, computer software and communication protocols used in transaction authorization; thus reducing of cost of deployment.

[0014] An embodiment of the present invention may require no or modest change to transaction authorization and thus the impact on day to day cardholder experience may not be significant. Cardholders who choose not to change CVV2 printed on the card would see no change, thus allowing for an evolutionary adoption.

[0015] In various embodiments of the present invention, changing nature of CVV2 may protect against fraudulent charges based on compromised or stolen credit card data when CVV2 is part of authorization as effectively as card replacement—at less cost to issuer and less inconvenience to cardholder.

[0016] Various embodiments of the present invention may incorporate one or more of these and other features described herein. A better understanding of the nature and advantages of the present invention may be gained by reference to following detailed description and accompanying drawings.

BRIEF DESCRIPTION OF DRAWINGS

[0017] FIG. **1** Illustrates an exemplary timeline depicting timely change of CVV2 by cardholder preventing a fraudulent charge.

[0018] FIG. **2** Illustrates an exemplary system of cardholder changeable CVV2.

[0019] FIG. **3** Illustrates an exemplary e-commerce form used in card-not-present transaction depicting change for this invention being limited to the help information.

[0020] FIG. **4** Illustrates an exemplary automated fuel dispenser in card-not-present transaction where CVV2 is used instead of Zip code.

[0021] FIG. **5** Illustrates a card with CVV2 blacked-out to prompt merchant to ask cardholder for CVV2 in a card-present transaction where CVV2 is used in authorization.

DETAILED DESCRIPTIONS

[0022] FIG. **1** is a diagram illustrating an example timeline **100** showing one cardholder changing CVV2 value based on his knowledge and risk perception over a period. It depicts cardholder changing CVV2 in response to example event **102** receipt of data breach notification. Subsequent fraudulent attempt using compromised data **104** fails due to submitted CVV2 based on compromised data no longer being valid. This is often the case that there is a time lag between skimmers, hackers obtaining credit card data and its use by criminals who often purchase it from them. A later event **106** shows cardholder changing CVV2 after a web purchase where cardholder perceives the site to be risky.

[0023] FIG. **2** is a diagram illustrating an example system where cardholder **202** uses an internet connected device **204** which may be a personal computer or mobile device to securely communicate with software applications hosted on servers **210** in data center of card issuer **214**. Cardholder may use a web browser or an issuer provided application to choose a new CVV2. An example of user interface **206** as part of authenticated and encrypted web session is shown. The application securely stores the cardholder chosen CVV2 on issuer's card account database **212** with new CVV2 value **218** stored in account record **216** in encrypted form so as not be compromised even in case of data loss.

[0024] Cardholder may change CVV2 as often as s/he wants. Since merchants, acquirers and payment processors are prohibited from storing CVV2 for PCI DSS compliance, authorization requests will be verified with the current value of CVV2 in issuer database and will be unambiguous even when an authorization request follows soon after a CVV2 change.

[0025] In a specific embodiment, certain cardholder chosen CVV2 values may indicate specific purpose. For example, cardholder may choose CVV2 value **000** to indicate all card-not-present transactions be declined, possibly for a card that cardholder has designated only for local in-store use.

[0026] FIG. **3** illustrates a card-not-present transaction which embodies present invention. It shows an exemplary web form **300** which is usually the final step of an ecommerce site's checkout process where payment details are submitted. Cardholder changeable CVV2 adds the note block **302** informing the cardholders to use secret CVV2 if changed from one printed on the card. Help information link **304** on CVV2 commonly found on many ecommerce sites would be similarly enhanced. Thus, the changes for this embodiment to the ecommerce sites are small, simple, low-risk changes to static help content.

[0027] FIG. **4** illustrates an Automated Fuel Dispenser (AFD), widely used source of card-not-present transactions, embodying present invention. In place of using billing zip code and AVS query for verification, the software has been changed to prompt for CVV2 **402** along with help information **404** and do a CVV2 query for verification. Cardholder changing CVV2 periodically or soon after a road trip where card was used at some gas stations with inadequate security would be protected even if the CVV2 is compromised by skimming. CVV2 based verification would also help Canadian cardholders with alphanumeric billing zip code travelling in the USA.

[0028] FIG. **5** illustrates embodiment of present invention in a card-present transaction. Cardholder may black out the CVV2 printed on the card as shown in **502** and **504** using, for example, a permanent marker at the time of first change of CVV2 to a personal secret. In the exemplary check-out **500**, cashier **506** asks cardholder **202** for the "security code". Unlike zip code which has been deemed to be personally identifiable information in some jurisdictions, cardholder may tell the cashier CVV2 safe with the knowledge even if it is somehow recorded and associated with the card account number; s/he will change it before it can be exploited. The masking of CVV2 also eliminates the risk of skimming when card is out of cardholder's sight as in a restaurant. In another embodiment, the issuer may omit CVV2 or print a pattern such as XXX; letting the cardholder setup the initial CVV2.

[0029] The above description of embodiments of the invention has been presented for the purpose of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form described, and many modifications and variations are possible in light of the teaching above. The embodiments were chosen and described in order to best explain the principles of the invention and its practical applications to thereby enable others skilled in the art to best utilize the invention in various embodiments and with various modifications as are suited to the particular use contemplated. Thus, it will be appreciated that the invention is intended to cover all modifications and equivalents within the scope of following claims.

What is claimed is:

1. A method for countering credit card fraud comprising cardholder changeable card security code known as CVV2.

2. The method of claim **1** further comprising:

Cardholder choosing a CVV2 value different from the one printed on the card on first change and a different new value for subsequent changes;

Cardholder recording the chosen CVV2 value with the card issuer;

Card issuer using most recently recorded CVV2 to verify CVV2 provided in transaction authorization requests that follow.

3. The method of claim **2** wherein recording the chosen CVV2 value with card issuer step is accomplished by the cardholder using a issuer provided facility over the Internet.

4. The method of claim **3** further comprising:

A web application on issuer's server;

Cardholder accessing the application via secure web session using a browser.

5. The method of claim **4** wherein the web application is a feature of online card management system.

6. The method of claim **3** further comprising:

Issuer provided application, also known as app, for mobile devices such as smartphones, tablets;

Cardholder using the app along with internet connectivity to securely communicate with issuer's server.

7. The method of claim **6** wherein the app is a feature of card account management app.

8. The method of claim **1** further comprising cardholders using CVV2 along with the card for authentication of trans-

actions where currently there is no additional verification or additional verification is based on static information.

9. The method of claim **2** wherein certain specific chosen CVV2 values have specific purpose.

* * * * *