August 2022

GLOBAL FRAUD DETECT

SIMON HOPLEY
VISA

GLOBAL FRAUD DETECT

VISA

INVENTOR:

SIMON HOPLEY

TECHNICAL FIELD

[0001] The present subject matter is, in general, related to fraud and/or risk management, and particularly, to a method and a system for aggregating and collating failed card transactions to detect fraud globally.

BACKGROUND

[0002] Transaction cards with restricted functionality include a debit card and a credit card. The transaction cards may include, without limiting to, magnetic stripe cards, chip based cards and contactless cards. A debit card or credit card is suspended when its use is restricted by placing the card on hold. Some issuers provide ways for cardholders to put their cards to sleep.

[0003] However, currently there is no centralized mechanism in place to collect unsuccessful and/or failed transactions in order to detect fraud. Each issuer is just looking out for itself, and hence its ability to identify fraud is restricted. There is a need to reduce fraud risk on credit and debit cards.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, explain the disclosed principles. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same numbers are used throughout the figures to reference like features and components. Some embodiments of device or system and/or methods in accordance with embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

[0005] **Fig. 1** illustrates an exemplary architecture of the proposed global fraud detection system for implementing embodiments consistent with the present disclosure.

[0006] **Fig. 2a** illustrates a flow diagram illustrating a method of global fraud detection in accordance with some embodiments consistent with the present disclosure.

[0007] **Fig. 2b** illustrates a flow diagram illustrating a method performed by a fraud detection alert module in accordance with some embodiments consistent with the present disclosure.

[0008] **Fig. 3** illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0009] The figures depict embodiments of the disclosure for purposes of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the disclosure described herein.

DESCRIPTION OF THE DISCLOSURE

[0010] In the present document, the word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or implementation of the present subject matter described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[0011] While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternative falling within the spirit and the scope of the disclosure.

[0012] The terms “comprises”, “comprising”, or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a device or system or apparatus proceeded by “comprises… a” does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[0013] The terms "an embodiment", "embodiment", "embodiments", "the embodiment", "the embodiments", "one or more embodiments", "some embodiments", and "one embodiment"

mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise.

[0014] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0015] The present disclosure proposes a method and a system for aggregating/collating failed card transactions to detect fraud globally. The proposed method is used to collate rejected transactions from suspended cards (for example when the card is in an asleep state) in order to detect fraudulent activity more rapidly and to establish a community-led response to fraud. Due to the possibility that an aggregator may not observe all transactions, the proposed method divides the transaction procedure into two parts. One for the transaction which the aggregator observes and then an overlay for issuers to share the events, which issuers may observe within their own ecosystem. Further, the aggregator may collate all the observed failed transaction data and deliver detection capabilities that may quickly identify when the fraudulent activities occur.

[0016] **Fig. 1** illustrates an exemplary environment of a global fraud detection system for performing embodiments consistent with the present disclosure. A fraudulent transaction (i.e., payment) made with a credit or debit card by an unauthorized user is referred to as credit card fraud. A 'failed transaction' is the one that was not fully completed for any reason other than the customer's connectivity breaks during online payment. In an embodiment, the exemplary environment may include one or more components for fraud detection by collating failed card transactions. These components include, without limiting to, a cardholder 101, an issuer 103, a Visa Transactions Recorder (VTR) 107, an Issuer Transactions Recorder (ITR) 109, and a record database 113.

[0017] In an embodiment, any individual user or customer who holds a credit card or debit card which is used for payment, or any financial transaction is referred to as a cardholder 101. The cardholder 101 attempts a payment via card network’s server, for example, VisaNet or with any other server to complete a financial transaction. The payment process ‘authentication’ or ‘decline’ may be different from one card network to another card network and may vary among different issuer types. The payment transaction may be processed in two different approaches, which are completely dependent on the card network server. For example, consider a scenario

of a cardholder 101_1 attempting to complete any financial transaction or payment using VisaNet and an issuer 103 checking the card status as shown in Fig. 2a.

[0018] In an embodiment, the issuers 103 are gatekeepers to cardholder's 101 payment account details for any transaction. Issuer 103 is in charge of ensuring that the cardholder 101 has sufficient funds for the transaction as well as customer authentication during the transaction process. Along with processing card applications, collecting cardholder 101 payments, and offering customer service, the issuing bank is also responsible for accepting or rejecting card transactions. Once the issuer 103 verifies the card status, for example, whether the card is asleep, on hold, or suspended, then the issuer 103 collects the information and records it in the VTR database 107.

[0019] In an embodiment, consider another scenario of a cardholder 101_2 attempting to complete any financial transaction or payment which may not utilize VisaNet and an issuer 103 verifies the card status as shown in Fig. 2a. After issuer 103 verifies, the issuer 103 declines the card transaction and sends the card transaction details via card network's server to record it in ITR database 109. Thereafter, the method initiates a procedure to verify the ITR 109 by comparing the ITR 109 transaction details with the transaction details stored on the card network's database 107, based on the information collected from two scenarios. Further, the method eliminates purge duplicates 207 of the failed transactions and creates a common transaction by entering the validated data in the record database 113.

[0020] In an embodiment, if the number of declined transactions that occur from a specific account from a specific merchant exceeds an adjustable threshold, then a potential fraud alert is created that triggers 223 an investigation and the account or merchant is placed on a watchlist 209 for a definable time period of interest. As a result, the method allows for the central detection of a fraudulent merchant not just by monitoring transactions through a specific card network, but also by leveraging data from other card issuers.

[0021] **Fig. 2a** illustrates a flow diagram illustrating a method of global fraud detection by collating failed transactions. For example, consider a scenario when cardholder 101_1 attempts card payment using VisaNet 201 server. Thereafter, issuer 103_1 initiates the process of determining if the card is in an asleep state (which indicates suspended cards) or not. If the card status is 'sleeping' state 203, the transaction may be declined to the cardholder and the process of recording the information or data through the database writing to VTR 107 may begin. The

VTR 107 includes, without limiting to, transaction amount details, transaction date, transaction time, a card issuer bank details, cardholder 101 card number, cardholder 101 card name, type of transaction (i.e., cardholder may not present etc.), a merchant ID, a merchant name, merchant location, currency details and reasons for decline of transaction. Further, the transaction may be processed as normal 205 by validating/authenticating the payment process or declining the payment process if the card status is not in the 'sleeping' state 203.

[0022] In an embodiment, consider another scenario when the cardholder 101_2 attempts card payment which may be using a non-VisaNet 211 server as shown in Fig. 2a. Here, the issuer 103_2 initiates the process of determining if the card is in an asleep state or not. The transaction may not be permitted to cardholder 101_2 and the issuer may reject the payment transaction 217 if the card status is asleep 213. Additionally, the issuer communicates the details of the declined transaction via the non-VisaNet server or Application Programming Interface (API) for recording the details or data into ITR 109 and also stores the data in a local issuer card management and risk system 219 database. The ITR 109 includes, without limiting to, transaction amount details, transaction date, transaction time, the card issuer's bank details, cardholder's 101 card number, cardholder's 101 card name, type of transaction (for example, the cardholder 101 may not present), a merchant ID, the merchant's name, the location of the merchant, currency details and the reasons for declining the transaction. Further, the transaction may be processed as normal 215 by authenticating the payment process or declining the payment process if the card status is not in the sleeping state.

[0023] In an embodiment, the ITR 109 transaction is compared to the transaction details stored on the card network's database using the data gathered from the two situations to initiate the process to validate declined transactions. These declines may be aggregated with equivalent declines that occur within a card network's system. The aggregating process may be deduplicated to avoid "double counting". If the number of the declines that occur from a specific account from a specific merchant exceeds an adjustable threshold, then a potential fraud alert module 221 is triggered as shown in Fig. 2b. The fraud alert module 221 triggers an investigation based on fraud rules and the account or merchant is placed on a watchlist 209 for a definable time period of interest. In the payment transactions process, for example, merchant ID number 10 matches in the last 30 minutes or card number matches multiple merchants in the last 6 hours and so on, are evaluated for triggering the alert module 221. The watchlist 209 is a configurable time period of interest, for example, archive entries from the database, which

don’t match within the given time period (say time = 60 minutes). The watchlist 209 may also include a purge database value, for example, purge database value = 1,00,00 records.

[0024] In an embodiment, the alert module 221 is triggered against the Visa transaction database to look at the historical activities of cardholder’s 101, and historical activities of merchants to apply a smarter alerting system 223. The historical activities of merchants include, without limiting to, reviewing merchant failure rates, looking for transaction spikes against merchants on the watchlist, looking for merchant matches across declined cards, merchants with raised failure rates across Visa and non-Visa payment cards and so on. The smarter alerting system may include an advanced fraud analytics add-on 231 to the alert system. Further, the alert module 221 triggers notification alerts for suspicious merchant alters 225, suspicious cardholder alerts 227 and non-visa dashboard 229. The suspicious merchant alters 225 display an alert message in an acquirer dashboard 233, wherein the acquirer dashboard 233 is available to acquirers with API feed option to issuer 103.

[0025] In an embodiment, the suspicious cardholder alerts 227 display an alert message in an issuer dashboard 235, wherein the issuer dashboards 235 is available to the issuer 103 and an API feed option is provided to the issuer 103. The non-visa dashboard 229 displays and alerts messages in a dashboard 237, wherein these dashboards 237 are available to other card networks. As a result, the feed reports issued to acquirers are associated with suspicious merchants, and the reports submitted to the issuers 103 are associated with suspicious accounts. Further, reports sent to card schemes are associated with the type of account which they support. Also, the central detection of a fraudulent merchant involves both the use of data from other card issuers as well as the monitoring of Visa transactions.

Advantages of the present invention:

[0026] In an embodiment, the present invention becomes independent of any particular card network as long as different issuers that enroll in the service may support different card networks. In other words, the present invention is no longer reliant on a single payment method or user interface.

[0027] In an embodiment, the present invention eliminates reliance of analysis from any one card network by integrating a number of issuer risk systems.

[0028] In general, the present invention increases speed of detection of frauds and reduces fraud on non-sleeping cards. Also, the invention reduces the number of false-positive reports. The invention provides an ability to change thresholds based upon acquiring merchant trust level and size of merchant. Also, the invention provides better analytics on fraud behaviors, in contrast to an arrangement where each issuer has a narrow view of the data. Moreover, the invention provides an ability to integrate with other risk scoring systems and an ability for individual issuers to share/tag ongoing investigation with wider cardholder community, affording them an option of reducing exposure or increasing monitoring as they deem fit.

General computer system:

[0029] Fig. 3 illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0030] In an embodiment, the computer system 300 may be used to implement the system. The computer system 300 may include a central processing unit (“CPU” or “processor”) 302. The processor 302 may include at least one data processor developing a common transaction database based on cardholder 101 payment attempts. The processor 302 may include specialized processing units such as, integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

[0031] The processor 302 may be disposed in communication with one or more Input/Output (I/O) devices (312 and 313) via I/O interface 301. The I/O interface 301 employ communication protocols/methods such as, without limitation, audio, analog, digital, monoaural, radio corporation of America (RCA) connector, stereo, IEEE-1394 high speed serial bus, serial bus, universal serial bus (USB), infrared, personal system/2 (PS/2) port, bayonet neill-concelman (BNC) connector, coaxial, component, composite, digital visual interface (DVI), high-definition multimedia interface (HDMI), radio frequency (RF) antennas, S-Video, video graphics array (VGA), IEEE 802.11b/g/n/x, Bluetooth, cellular e.g., code-division multiple access (CDMA), high-speed packet access (HSPA+), global system for mobile communications (GSM), long-term evolution (LTE), worldwide interoperability for microwave access (WiMax), or the like, etc.

[0032] Using the I/O interface 301, the computer system 300 may communicate with one or more I/O devices such as input devices 312 and output devices 313. For example, the input devices 312 may be an antenna, keyboard, mouse, joystick, (infrared) remote control, camera,

card reader, fax machine, dongle, biometric reader, microphone, touch screen, touchpad, trackball, stylus, scanner, storage device, transceiver, video device/source, etc. The output devices 313 may be a printer, fax machine, video display (e.g., cathode ray tube (CRT), liquid crystal display (LCD), light-emitting diode (LED), plasma, plasma display panel (PDP), organic light-emitting diode display (OLED) or the like), audio speaker, etc.

[0033] In some embodiments, the processor 302 may be disposed in communication with a communication network 309 via a network interface 303. The network interface 303 may communicate with the communication network 309. The network interface 303 may employ connection protocols including, without limitation, direct connect, ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. The communication network 309 may include, without limitation, a direct interconnection, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, etc. Using the network interface 303 and the communication network 309, the computer system 300 may communicate with a database 314, which may be the enrolled templates database 313. The network interface 303 may employ connection protocols include, but not limited to, direct connect, ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc.

[0034] The communication network 309 includes, but is not limited to, a direct interconnection, a peer to peer (P2P) network, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, Wi-Fi and such. The communication network 309 may either be a dedicated network or a shared network, which represents an association of the different types of networks that use a variety of protocols, for example, hypertext transfer protocol (HTTP), transmission control protocol/internet protocol (TCP/IP), wireless application protocol (WAP), etc., to communicate with each other. Further, the communication network 309 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc.

[0035] In some embodiments, the processor 302 may be disposed in communication with a memory 305 (e.g., RAM, ROM, etc. not shown in Fig. 3) via a storage interface 304. The storage interface 304 may connect to memory 305 including, without limitation, memory drives, removable disc drives, etc., employing connection protocols such as, serial advanced technology attachment (SATA), integrated drive electronics (IDE), IEEE-1394, universal serial

bus (USB), fiber channel, small computer systems interface (SCSI), etc. The memory drives may further include a drum, magnetic disc drive, magneto-optical drive, optical drive, redundant array of independent discs (RAID), solid-state memory devices, solid-state drives, etc.

[0036] The memory 305 may store a collection of program or database components, including, without limitation, user interface 306, an operating system 307, etc. In some embodiments, computer system 300 may store user/application data, such as, the data, variables, records, etc., as described in this disclosure. Such databases may be implemented as fault-tolerant, relational, scalable, secure databases such as Oracle or Sybase.

[0037] The operating system 307 may facilitate resource management and operation of the computer system 300. Examples of operating systems include, without limitation, Apple™ Macintosh ™ OS X™, UNIX™, Unix-like system distributions (e.g., Berkeley Software Distribution (BSD), FreeBSD™, Net BSD™, Open BSD™, etc.), Linux distributions (e.g., Red Hat™, Ubuntu™, K-Ubuntu™, etc.), International Business Machines (IBM™) OS/2™, Microsoft Windows™ (XP™, Vista/7/8, etc.), Apple iOS™, Google Android™, Blackberry™ operating system (OS), or the like.

[0038] In some embodiments, the computer system 300 may implement web browser 308 stored program components. Web browser 308 may be a hypertext viewing application, such as Microsoft™ Internet Explorer™, Google Chrome™, Mozilla Firefox™, Apple™ Safari™, etc. Secure web browsing may be provided using secure hypertext transport protocol (HTTPS), secure sockets layer (SSL), transport layer security (TLS), etc. Web browsers 308 may utilize facilities such as AJAX, DHTML, Adobe™ Flash, Javascript, Application Programming Interfaces (APIs), etc. In some embodiments, the computer system 300 may implement a mail server stored program component. The mail server may be an Internet mail server such as Microsoft Exchange, or the like. The mail server may utilize facilities such as ASP, ActiveX, ANSI C++/C#, Microsoft .NET, Common Gateway Interface (CGI) scripts, Java, JavaScript, PERL, PHP, Python, WebObjects, etc. The mail server may utilize communication protocols such as Internet Message Access Protocol (IMAP), Messaging Application Programming Interface (MAPI), Microsoft Exchange, Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), or the like.

[0039] In some embodiments, the computer system 300 may implement a mail client stored program component. The mail client may be a mail viewing application, such as Apple Mail, Microsoft Entourage, Microsoft Outlook, Mozilla Thunderbird, etc.

[0040] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer-readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., be non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, Compact Disc (CD) ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0041] The described operations may be implemented as a method, system or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof. The described operations may be implemented as code maintained in a “non-transitory computer readable medium”, where a processor may read and execute the code from the computer readable medium. The processor is at least one of a microprocessor and a processor capable of processing and executing the queries. A non-transitory computer readable medium may include media such as magnetic storage medium (e.g., hard disk drives, floppy disks, tape, etc.), optical storage (CD-ROMs, DVDs, optical disks, etc.), volatile and non-volatile memory devices (e.g., EEPROMs, ROMs, PROMs, RAMs, DRAMs, SRAMs, Flash Memory, firmware, programmable logic, etc.), etc. Further, non-transitory computer-readable media may include all computer-readable media except for a transitory. The code implementing the described operations may further be implemented in hardware logic (e.g., an integrated circuit chip, Programmable Gate Array (PGA), Application Specific Integrated Circuit (ASIC), etc.).

[0042] The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of

illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items or meant to be limited to only the listed item or items. It must also be noted that as used herein, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise.

[0043] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., are non-transitory. Examples include random access memory (RAM), read-only memory (ROM), volatile memory, non-volatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0044] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

[0045] With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

GLOBAL FRAUD DETECT

ABSTRACT

The present disclosure relates to a method and a system for aggregating card transactions to detect fraud globally, wherein transactions that take place when the issuer's accounts are known to be in a sleep state condition or comparable condition. The present disclosure suggests collecting data from an issuer, where there is a failure to detect system-wide fraud. Thereafter, the issuers are enabled to share fraud findings that may include more than simply one card network's cards. Also, the present disclosure enables cross-card program frauds to be detected and stopped considerably more quickly, consequently reducing the size of a fraud and providing law authorities with an earlier warning.

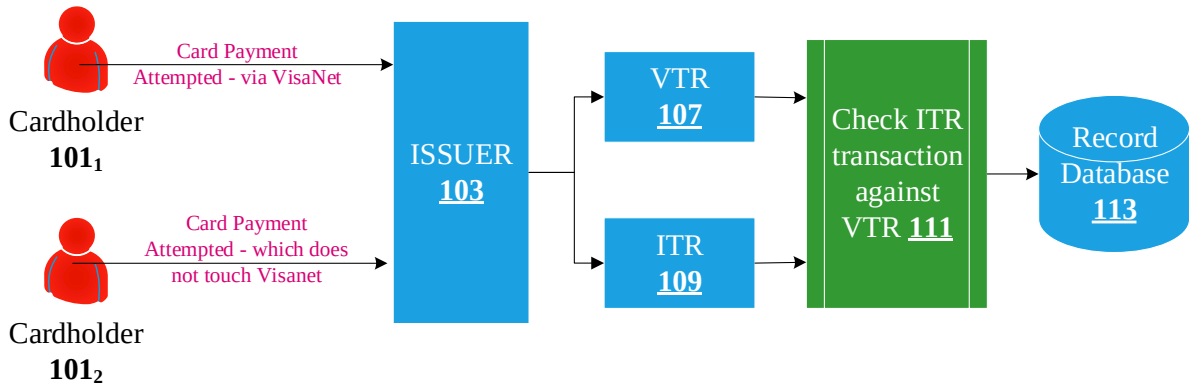
Card Payment
Attempted - via VisaNet
Cardholder
101₁
Card Payment
Attempted - which does
not touch Visanet
Cardholder
101₂
ISSUER
103
VTR
107
ITR
109
Check ITR
transaction
against
VTR 111
Record
Database
113

Fig. 1

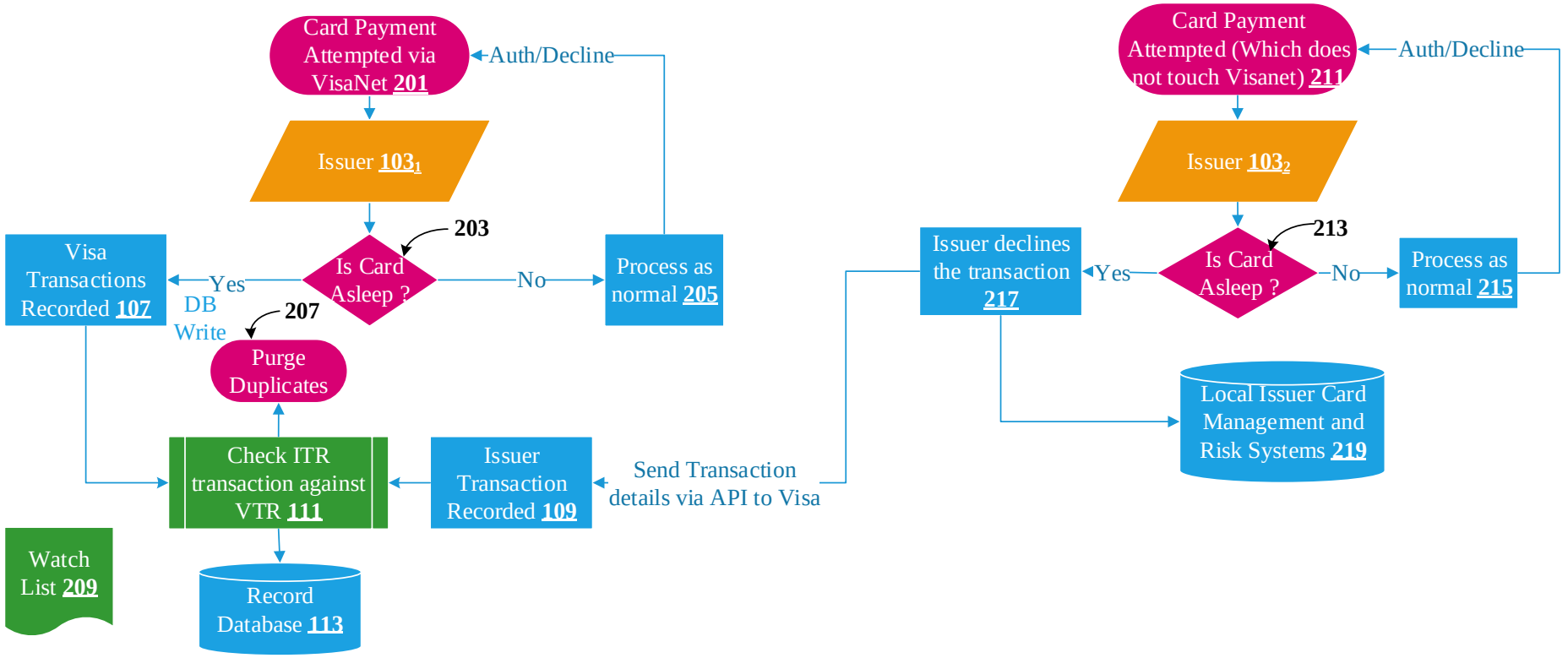
Card Payment Attempted via VisaNet 201
Auth/Decline
Issuer 103₁
203
Is Card Asleep ?
Yes
No
Visa Transactions Recorded 107
DB Write
207
Purge Duplicates
Process as normal 205
Check ITR transaction against VTR 111
Issuer Transaction Recorded 109
Send Transaction details via API to Visa
Watch List 209
Record Database 113
Card Payment Attempted (Which does not touch Visanet) 211
Auth/Decline
Issuer 103₂
213
Is Card Asleep ?
Yes
No
Issuer declines the transaction 217
Process as normal 215
Local Issuer Card Management and Risk Systems 219

Fig. 2a

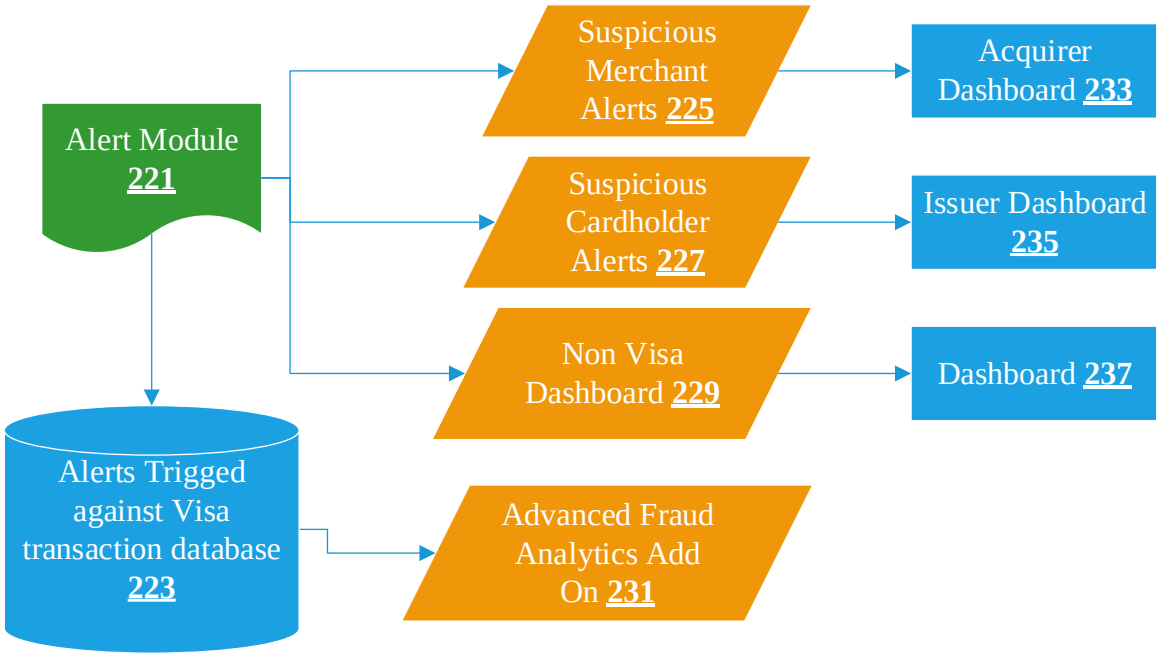
Alert Module
221
Suspicious
Merchant
Alerts 225
Acquirer
Dashboard 233
Suspicious
Cardholder
Alerts 227
Issuer Dashboard
235
Non Visa
Dashboard 229
Dashboard 237
Alerts Trigged
against Visa
transaction database
223
Advanced Fraud
Analytics Add
On 231

Fig. 2b

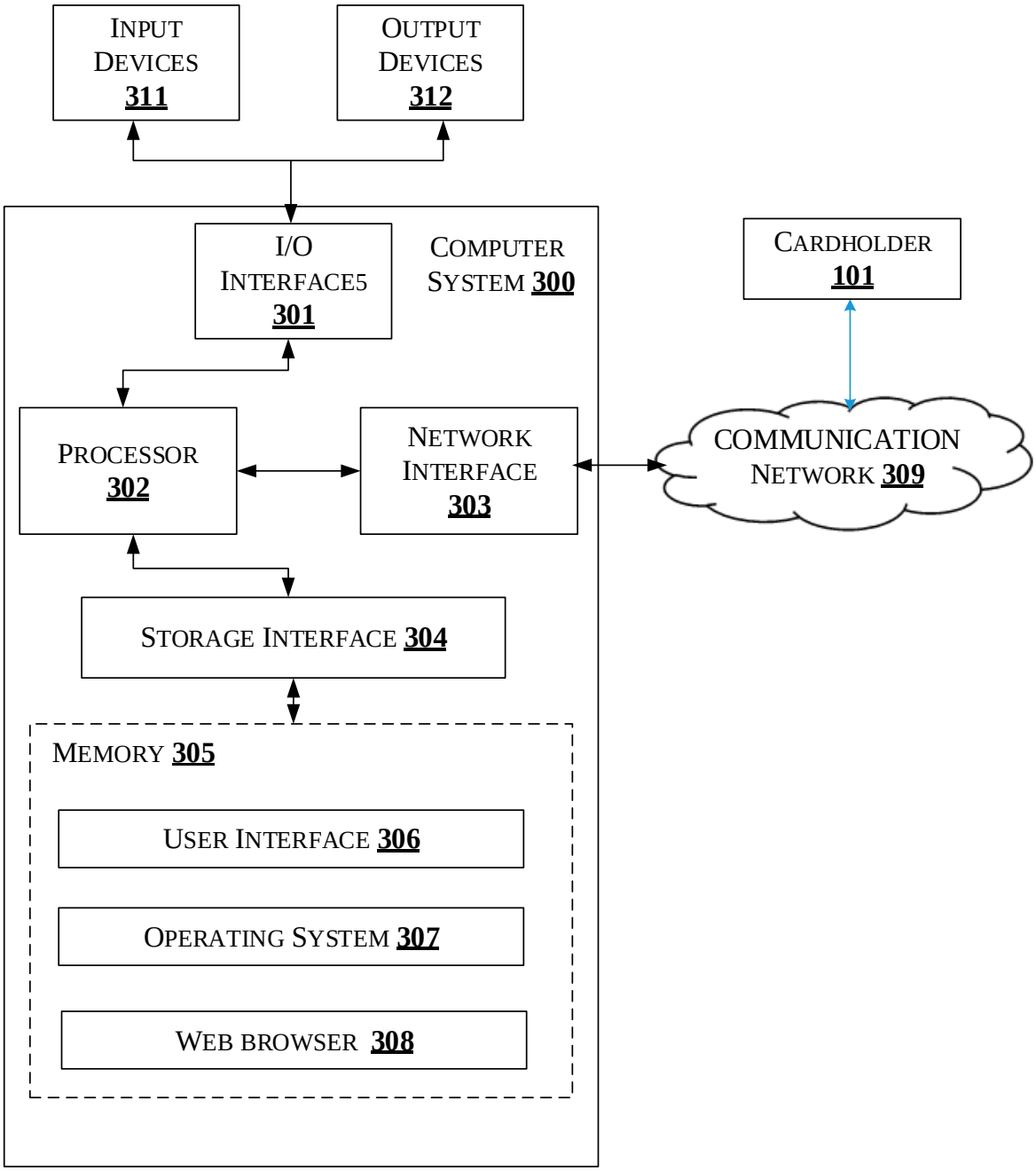
INPUT DEVICES 311
OUTPUT DEVICES 312
I/O INTERFACE5 301
COMPUTER SYSTEM 300
CARDHOLDER 101
PROCESSOR 302
NETWORK INTERFACE 303
COMMUNICATION NETWORK 309
STORAGE INTERFACE 304
MEMORY 305
USER INTERFACE 306
OPERATING SYSTEM 307
WEB BROWSER 308

Fig. 3