September 2023

ROLLING AVAILABILITY OF PAYMENT CARD CREDIT LIMIT TO PREVENT FRAUDULENT CARD TRANSACTIONS

ALOK ROY
Visa

TITLE: ROLLING AVAILABILITY OF PAYMENT CARD CREDIT LIMIT TO PREVENT FRAUDULENT CARD TRANSACTIONS

APPLICANT: VISA INTERNATIONAL SERVICE ASSOCIATION

ADDRESS: P.O. Box 8999, San Francisco, CA, 94128, USA

Nationality: USA

INVENTOR: ALOK ROY

TECHNICAL FIELD

[0001] The present subject matter is, in general, related to payment cards, and in particular to, a system and method of preventing unauthorized high value purchases by fraudsters when card credentials are compromised.

BACKGROUND

[0002] The advancement in technology has made access to the banking system easier through multiple means. Payment cards are one of them. Payment cards are issued by banks, to a customer that enables the customer to access the funds in the customer's designated bank accounts, or through a credit account. Payments are made by electronic transfer with a payment terminal like automated teller machines (ATMs). Payment cards may also be used online through netbanking. Further payment cards may also be used for shopping online or offline. The customer is provided with some credentials to authenticate usage of the payment card.

[0003] Payment cards are of different types. The most common being credit cards, debit cards, charge cards, and prepaid cards. Most commonly, a payment card is electronically linked to an account or accounts belonging to the cardholder. These accounts may be deposit accounts or loan or credit accounts. However, stored-value cards store money on the card itself and are not necessarily linked to an account at a financial institution.

[0004] If a payment card is lost and found by a miscreant or if a fraudster gets access to the card credentials, then there are high chances of the payment card being used for unauthorized purchases. Sometimes the total amount of unauthorized purchases can be very high before it gets noticed by the cardholder, who can block the card when he knows that it is stolen. The cardholder and the card issuing banks, depending on the card protection plan, lose a lot of money due to such frauds.

[0005] Hence there exists a need to find methods to prevent unauthorized high value purchases by fraudsters when card credentials are compromised.

[0006] The information disclosed in the background section of the disclosure is only for enhancement of understanding of the general background of the invention and should not be taken as an acknowledgement or any form of suggestion that this information forms the prior art already known to a person skilled in the art.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] 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:

[0008] **Figure. 1** shows an exemplary environment **100** where the proposed method of preventing unauthorized high value purchases by fraudsters when payment card credentials are compromised may be implemented, in accordance with some embodiments of the present disclosure.

[0009] **Figure 2** shows an exemplary block diagram **200** of a cardholder's mobile device and a server as illustrated in **Figure 1**, in accordance with some embodiments of the present disclosure.

[0010] **Figure 3** illustrates a flow diagram representing an exemplary method **300** of preventing unauthorized high value purchases by fraudsters when payment card credentials are compromised, in accordance with some embodiments of the present disclosure.

[0011] **Figure 4** illustrates an example illustrating a method of preventing unauthorized high value purchases by fraudsters when payment card credentials are compromised, in accordance with some embodiments of the present disclosure.

[0012] 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

[0013] 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.

[0014] 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.

[0015] 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.

[0016] 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. The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0017] The present disclosure relates to a method of preventing unauthorized high value purchases by fraudsters when payment card credentials are compromised. This is performed by controlling an available credit limit or balance of the payment card of a cardholder through a rolling window (also, referred as rolling window limit).

[0018] In one non-limiting embodiment, the method includes adding a feature to a card issuing bank or institution’s netbanking account that may allow the cardholder to set a fixed available rolling credit limit or balance window for the cardholder’s payment card transactions. Further,

the method may allow the cardholder to set the rolling availability of credit limit feature to an ON state or an OFF state. In the ON state, the cardholder may make a transaction that is limited to the amount set in the rolling availability of credit limit. In the OFF state, payment up to the total available credit limit or balance is made i.e., the cardholder may make a transaction that may equal the total available balance in the cardholder's account.

[0019] Referring now to **Figure 1**, which illustrates an exemplary environment **100** where the proposed method of preventing unauthorized high value purchases by fraudsters when payment card credentials are compromised may be implemented, in accordance with some embodiments of the present disclosure. The environment **100** may include a cardholder's mobile device **110** and a server **120** communicatively connected over a network **130**. The cardholder's mobile device **110** comprises a banking application installed in the cardholder's mobile device **110** through which the cardholder may access their bank account. In one non-limiting embodiment, the banking application includes a feature that may allow the cardholder to set a rolling availability of credit limit for the cardholder's payment card transactions. In one embodiment, the cardholder may set the desired rolling credit limit based on their daily requirements. However, the total available credit limit window for transaction is fixed. Hence the total available credit limit or account balance for transactions always remain same even if the cardholder makes a new purchase transaction or makes payment to their card bill.

[0020] In various embodiments, the cardholder may keep the rolling window feature ON or OFF. As illustrated in **Figure 1**, the mobile application has two buttons/options **150, 152**, one button/option **150** representing an ON state of the rolling availability of credit limit and the other button/option **152** representing the OFF state of the rolling availability of credit limit. By default, this feature is set in the OFF state when a new payment card is issued by the issuing bank to the cardholder. In the ON state the cardholder may make a transaction that is limited to the amount set (this amount is set by the cardholder) in the rolling availability of credit limit. In the OFF state the cardholder may make a transaction that may equal the total available credit limit or balance in the cardholder's account. In one non-limiting embodiment, the cardholder may keep the rolling window in the ON state. When the cardholder wants to make a payment that exceeds the set rolling credit limit, the application in the cardholder's mobile device may allow the cardholder to set the rolling availability of credit limit feature to an OFF state. When the transaction is complete, the cardholder may set the rolling availability of credit limit feature back to an ON state. In various embodiments, the server **120** is a banking server. Whenever

there is a change in the state of the rolling availability of credit limit feature or for any transaction, the application in the cardholder's mobile device updates the cardholder's account in the server **120.**

[0021] When an intruder who has the cardholder's payment card and credentials tries to make a transaction using the payment card, the transaction is successful only if the transaction amount is within the set rolling availability of credit limit. In response to a successful transaction, a notification is sent to the cardholder's mobile device indicating a successful transaction. The cardholder on receiving the notification may notice the transaction that has been done without his/her consent and may realize that their payment card has been stolen or misused and may take necessary steps to block the payment card. However, if the intruder tries to make a payment transaction that is beyond the set rolling availability of credit limit, the transaction is refused, and the cardholder may receive a notification in their mobile device **110** indicating a failed transaction. Similar to the previous situation, upon receiving the notification the cardholder may realize that their payment card has been stolen or misused and may take necessary steps to block the payment card.

[0022] Referring now to **Figure 2** that shows an exemplary block diagram **200** of a cardholder's mobile device **110** and a server **120** as illustrated in **Figure 1**. As shown in **Figure 2**, the cardholder's mobile device **110** may include a memory **212**, a transceiver **216**, and a processor **214**. The transceiver **216** is configured to facilitate exchange of data between the cardholder's mobile device **110** and the server **120**. The memory **212** is configured to store necessary commands needed for the cardholder's mobile device to receive requests, to generate responses for setting rolling availability of credit limit, and/or to set the rolling availability of credit limit feature to ON state or OFF state. The processor **214** is communicatively coupled to the memory **212** and to the transceiver **216**. The processor **214** processes or performs various operations for preventing unauthorized high value purchases by fraudsters when card credentials are compromised. In an exemplary embodiment, the processor **214** may execute the instructions to run the mobile applications, to set the rolling availability of credit limit and to set the rolling availability of credit limit feature to ON state or OFF state.

[0023] As illustrated in **Figure 2**, the server **120** may include a processor **224** and a memory **222** storing instructions executable by the processor **224**. The processor **224** may execute cardholder-generated requests. In an exemplary embodiment, the processor **224** may receive a

request to set the rolling availability of credit limit. Upon receiving the request, the processor **224** may set the rolling availability of credit limit. The processor **224** may also receive a request to set the rolling availability of credit limit feature to ON state or OFF state. Upon receiving the request, the processor **224** may change the state of the rolling availability of credit limit feature to either ON state or OFF state based on the request.

[0024] The memory **222** may be communicatively coupled to the processor **224.** Further, the server **120** may includes a transceiver **228** configured to receive the request from the cardholder's mobile device **110**. The transceiver **228** is configured to send a notification to the cardholder's mobile device **110**.

[0025] The memory **212**, **222** may include a Random-Access Memory (RAM) unit and/or a non-volatile memory unit such as a Read Only Memory (ROM), optical disc drive, magnetic disc drive, flash memory, Electrically Erasable Read Only Memory (EEPROM), a memory space on a server or cloud and so forth. For the sake of illustration, it is assumed here that the memory is a non-volatile memory. Examples of the processor may include, but not restricted to, a general-purpose processor, a Field Programmable Gate Array (FPGA), an Application Specific Integrated Circuit (ASIC), a Digital Signal Processor (DSP), microprocessors, microcomputers, micro-controllers, digital signal processors, central processing units, state machines, logic circuitries, and/or any devices that manipulate signals based on operational instructions.

[0026] Referring now to **Figure 3** that depicts a flowchart illustrating a method **300** of preventing unauthorized high value purchases by fraudsters when payment card credentials are compromised, in accordance with some embodiments of the present disclosure. The various operations of the method **300** are performed by the cardholder's mobile device **110** (also, referred as user mobile device) and in particular, by the processor **214** of the cardholder's mobile device **110**. The method comprises, at block **302,** the cardholder, accessing the cardholder's bank account through a banking application installed in the cardholder's mobile device. At block **304**, the cardholder sets a rolling availability of credit limit for the cardholder's payment card transactions through a rolling availability of credit limit feature available in the banking application. The application in the mobile device may send a request to the server **120** to set the rolling availability of credit limit as entered by the cardholder. The server **120** may in response set the rolling availability of credit limit feature with the credit

limit set by the cardholder in the cardholder's account. At block **306**, the cardholder may then set the rolling availability of credit limit feature in the banking application to an ON state. The server **120** may in response set the rolling availability of credit limit in the ON state. At block **308**, when the cardholder wants to make a payment transaction that is above the set rolling availability of credit limit, the cardholder may change the rolling availability of credit limit feature in the banking application to an OFF state. The application in the mobile device may send a request to the server **120** to change the rolling availability of credit limit feature to an OFF state. The server **120** in response may set rolling availability of credit limit feature in the cardholder's account to an OFF state. Further, at block **308**, when the payment transaction is complete the cardholder may change the rolling availability of credit limit feature to an ON state in the banking application. The application in the mobile device may send a request to the server **120** to change the rolling availability of credit limit feature to an ON state and the server **120** in response may change the rolling availability of credit limit feature to an ON state in the cardholder's account.

[0027] Referring now to **Figure 4** that depicts an example illustrating the method of preventing unauthorized high value purchases by fraudsters when payment card credentials are compromised, in accordance with some embodiments of the present disclosure. In the example **401**, a cardholder has total available credit limit of $30,000. The cardholder sets the rolling window in the ON state and sets the rolling availability of credit limit as $2000. Therefore, though the cardholder has a total available credit limit of $30,000, the credit limit available for transaction is only $2000 and with the rolling window in the ON state, the cardholder may make a transaction of $2000 only. In the example **402**, the cardholder then makes a transaction of $1500 with the rolling window ON, the total available credit limit after the transaction is $28,500. In the example **403**, the cardholder makes a payment of $1000 to the payment card and the total available credit limit after the payment is $29,500. In continuation with the example **404**, the cardholder changes the rolling window to the OFF state, now the total available credit limit available for transaction is $29,500 (as shown in the example **404)**. With the rolling window in the OFF state the cardholder may make a transaction for the total available credit limit available for transaction i.e., up to an amount of $29,500.

[0028] Some of the advantages of the proposed disclosure are presented below.

[0029] The proposed method may prevent high value unauthorized and fraudulent transactions which may help card issuing banks and cardholders to uphold the positive sentiments on payment card usage.

[0030] Further, fraudsters may not be able to make unauthorized transactions more than the rolling window limit. This way the proposed method would help to minimize the financial losses incurred by the card issuing banks and cardholders.

[0031] 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 of the disclosed embodiments. 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.

[0032] 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.

[0033] 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.

[0034] 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.

ROLLING AVAILABILITY OF PAYMENT CARD CREDIT LIMIT TO PREVENT FRAUDULENT CARD TRANSACTIONS

ABSTRACT

The present disclosure relates to a method of preventing unauthorized high value purchases by fraudsters when payment card credentials are compromised. This is performed by controlling an available credit limit or balance of the payment card of a cardholder through a rolling window. The method includes adding a feature to a card issuing bank or institution's net banking account that may allow the cardholder to set a fixed available rolling credit limit or balance window for the cardholder's payment card transactions. Further, the method may allow the cardholder to set the rolling availability of credit limit feature to an ON state or an OFF state. In the ON state, the cardholder may make a transaction that is limited to the amount set in the rolling availability of credit limit. In the OFF state, payment up to a total available credit limit or balance may be made i.e., the cardholder may make a transaction that may equal the total available balance in the cardholder's account.

Figure 1

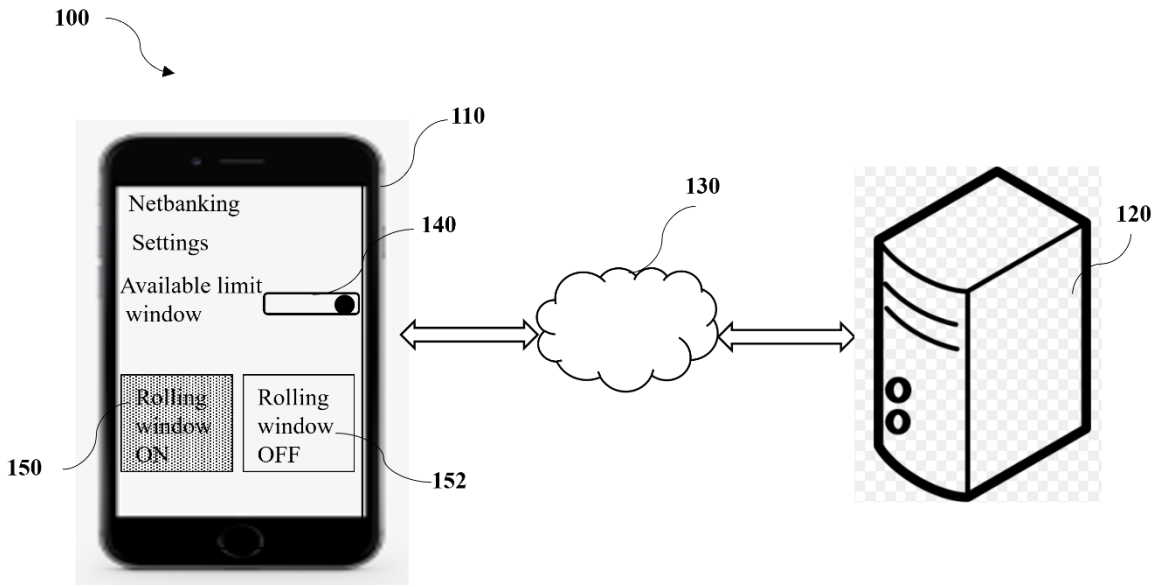
100
110
Netbanking
Settings
Available limit window
140
130
120
Rolling window ON
Rolling window OFF
150
152

Figure 1

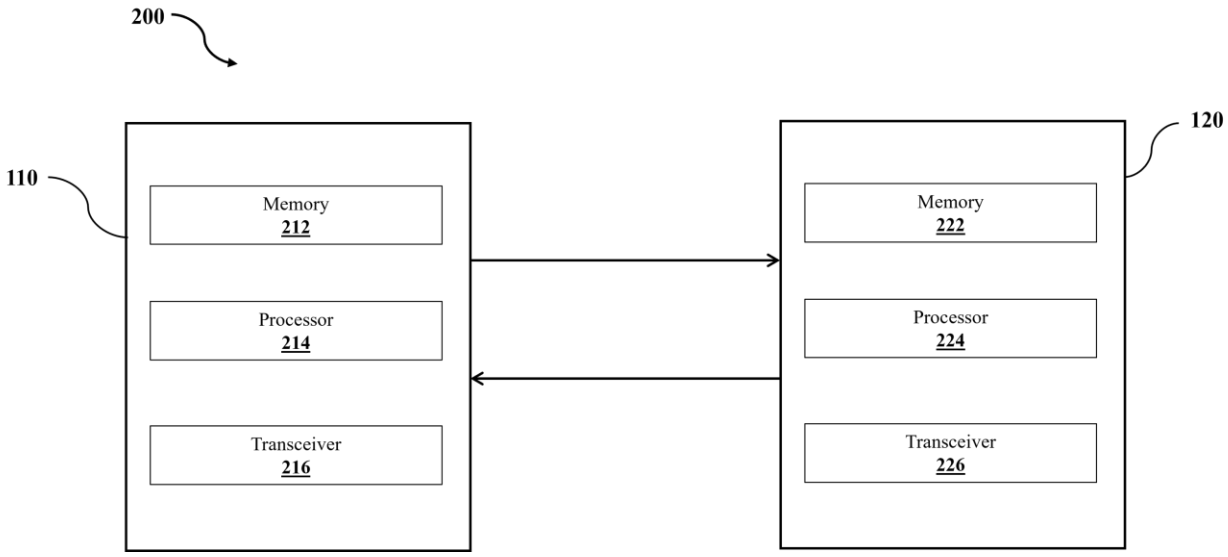
200
110
Memory
212
Processor
214
Transceiver
216
120
Memory
222
Processor
224
Transceiver
226

Figure 2

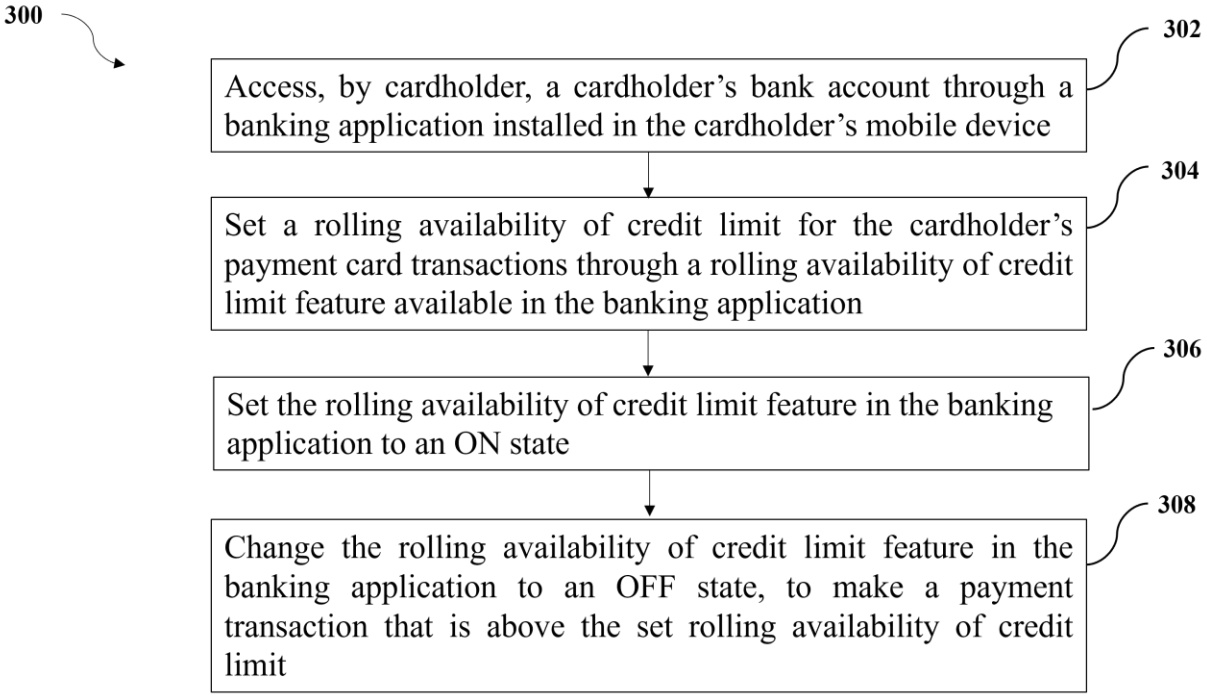
300
302
Access, by cardholder, a cardholder's bank account through a banking application installed in the cardholder's mobile device
304
Set a rolling availability of credit limit for the cardholder's payment card transactions through a rolling availability of credit limit feature available in the banking application
306
Set the rolling availability of credit limit feature in the banking application to an ON state
308
Change the rolling availability of credit limit feature in the banking application to an OFF state, to make a payment transaction that is above the set rolling availability of credit limit

Figure 3

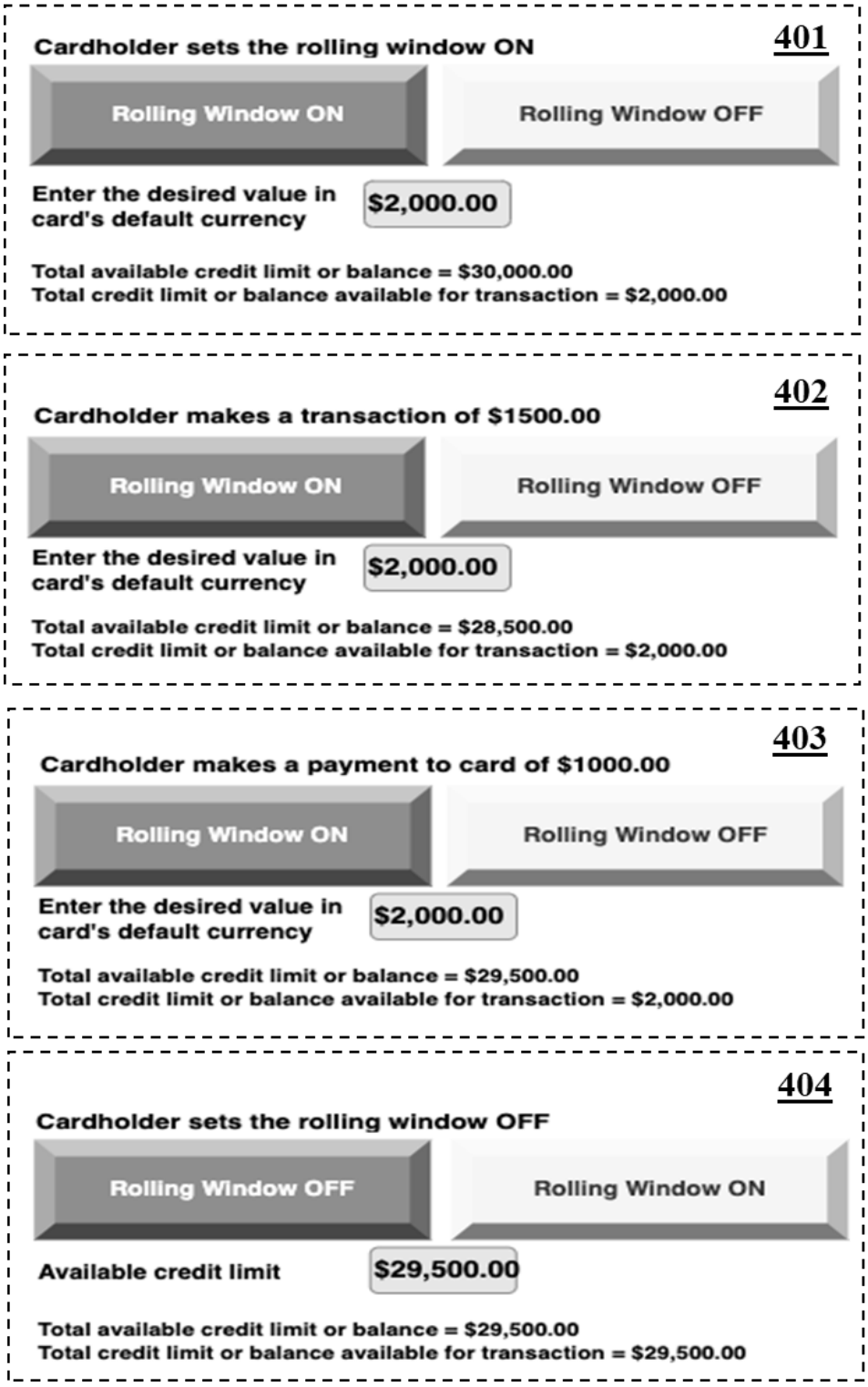
401
Cardholder sets the rolling window ON
Rolling Window ON
Rolling Window OFF
Enter the desired value in card's default currency
$2,000.00
Total available credit limit or balance = $30,000.00
Total credit limit or balance available for transaction = $2,000.00
402
Cardholder makes a transaction of $1500.00
Rolling Window ON
Rolling Window OFF
Enter the desired value in card's default currency
$2,000.00
Total available credit limit or balance = $28,500.00
Total credit limit or balance available for transaction = $2,000.00
403
Cardholder makes a payment to card of $1000.00
Rolling Window ON
Rolling Window OFF
Enter the desired value in card's default currency
$2,000.00
Total available credit limit or balance = $29,500.00
Total credit limit or balance available for transaction = $2,000.00
404
Cardholder sets the rolling window OFF
Rolling Window OFF
Rolling Window ON
Available credit limit
$29,500.00
Total available credit limit or balance = $29,500.00
Total credit limit or balance available for transaction = $29,500.00

Figure 4