December 2021

METHOD AND SYSTEM FOR FACILITATING AUTHENTICATION OF SECONDARY ACCOUNT HOLDER DEVICE FOR TRANSACTIONS ORIGINATED AGAINST PRIMARY CARDHOLDER'S ACCOUNT

PRAGHATHI M S Ms.
Visa

AMIT KUMAR MISHRA Mr.
Visa

TITLE: "METHOD AND SYSTEM FOR FACILITATING AUTHENTICATION OF SECONDARY ACCOUNT HOLDER DEVICE FOR TRANSACTIONS ORIGINATED AGAINST PRIMARY CARDHOLDER'S ACCOUNT"

VISA

PRAGHATHI M S

AMIT KUMAR MISHRA

TECHNICAL FIELD

[0001] The present disclosure relates generally to the field of financial transactions. Specifically, the present disclosure provides method and system for facilitating authentication of secondary account holder device for transactions originated against primary cardholder's account.

BACKGROUND

[0002] Generally, in the field of financial transactions, majority of the transactions are based on only one phone number that is attached to all the bank accounts and all the One Time Password (OTPs) for second factor authentication are sent to the same single number which adds dependency on a single person to share OTP to other members, the primary account holder may make use of a primary device such as mobile phone, tablets, laptops, desktops and the like.

[0003] Currently, there are techniques which enables the primary account holder to use a family member's phone (secondary account holder device) to access SingPass account of the account holder; session switching from a primary account holder device to a secondary account holder device with dynamic connections across systems and the like. But the authentication of the secondary account holder is the key aspect while making the transactions. Therefore, there is a need fora comprehensive and robust method that addresses the issue of authentication of the second account holder for processing transactions originated by the primary account holder's account. Such method should be capable of taking into consideration individual business problems and bring all of them together for identifying target segments with a suitable action.

SUMMARY

[0004] According to some non-limiting embodiments, the present disclosure facilitates primary card holder to update issuer system with valid secondary account holder device, which has to be approved by the primary account holder. Also, the present disclosure facilitates a process through which transaction processing through merchant portal is taken care when second factor authentication is provided by secondary account holder device. Therefore, the present disclosure avoids repeated transactions through primary account holder device, and

hence improved overall Pre-settlement Risk (PSR) rate. A secondary account holder device will initiate and complete the transaction with authentication without depending on the actual card holder to share the One Time Password (OTP). . The objective of the present disclosure is to develop authentication method of second account holder that can:

- Reduce the dependency on a single person to share OTP to other members.
- That enables the primary account holder to authorize (to issuer) to use additional number (secondary account holder) on which OTP can be shared. The primary account holder can also customize the type and number of transactions for which such OTP sharing can be done.
- Authenticate the second account holder with the help of back-end verification of the cryptogram from the stored information, check rules such as transaction limit, expiry date and accept it as valid secondary account holder device to which OTP can be sent.

[0005] In some non-limiting embodiments, the present disclosure decomposes a business problem into individual components, builds a solution and stitches all of them together to generate an optimal solution for each individual component. In other words, each of the flows developed to implement the aforementioned objectives may be clustered together using Authentication and Mapping techniques, to build a strong, powerful, robust and a comprehensive model that can facilitate transactions to originate from a secondary account holder. In some embodiments, the method associated with the developed transaction models are packaged in such a way that, it can be deployed in both conventional and latest framework at ease.

[0006] In some non-limiting embodiments, the present disclosure registers the secondary account holder's number with the help of the primary account holder in the banking application. On the device where secondary SIM is present, issuer's mobile banking application is used to generate a digital fingerprint of the device. This fingerprint includes International Mobile Equipment Identity (IMEI) which is a 15-digit number unique to each device, International Mobile Subscriber Identity (IMSI) which is a 15-digit number for every user in a Global System for Mobile communication (GSM) and Phone number information and may be represented in the form of Quick Response (QR) code. However, QR code representation should not be construed to be a limitation of the present disclosure. In some embodiments, the secondary account holder device may be configured with issuer's mobile banking application. The primary account holder uses issuer's mobile banking application, logs into it and selects

option to authorize secondary account holder device if the account is eligible for having a secondary account holder. The primary account holder scans the QR code that is generated with the secondary account holders' details with the help of camera configured in the device of the primary account holder. The primary account holder has the leverage of customizing the parameters of the secondary account holder. For instance, the parameters may include type, amount of transaction, date range for which this secondary account holder device will be active and the like. Later, the captured information is sent securely to the issuer's backend and provisions are made accordingly. In some embodiments, when the issuer has ability to add two devices and phone numbers for authentication, then while provisioning Visa Token Service (VTS) should provide an option to the Cardholder (C/H) to select the number to be used for authentication. It can be added in the VTS User Interface (UI) as follows:

- Use Primary account holder device (mobile # xxxxxx1234) for OTP reception
- Use secondary account holder device (mobile # xxxxxx4321) for OTP reception

In some embodiments, the method of the present disclosure includes obtaining data from one or more data sources such as Visa Net, issuer's backend data and so on. In some embodiments, the Visa Net may provide transaction data such as issuer country, market segment, merchant name, source and destination amount, plastic type, channel and so on. In some embodiments, the issuer may provide the details of the secondary account holder transactions with the primary account holder in order to make the primary account holder aware about the same. Therefore, though the payment initiated from primary account, payment completion happened with secondary account and settlement happened through secondary account. Merchant and customer would be communicated regarding such transaction. The awareness is achieved by tracking of primary and secondary account holder device/account mapping. In some embodiments, payment is initiated from primary account but say if primary account has insufficient funds, then top-up of primary account is made through secondary account where issuer manages the debit of secondary account and credit to primary account, and completion happened with primary account and settlement happening through primary account itself. Merchant and customer would be made aware of the transaction.

[0007] The present disclosure provides an advantage of eliminating the dependency on a single person to share the OTP to other members, thereby having a secondary account holder who can make use of the bank transactions easily with just registering the digital fingerprint with the secondary account holder device parameters. This facilitation is done with optimal

authentication of the secondary account holder by verifying the cryptogram details at the issuer's back end.

[0008] These and other features and characteristics of the present disclosure, as well as the methods of operation and functions of the related elements of structures and the combination of parts and economies of manufacture, will become more apparent upon consideration of the following description and the appended claims with reference to the accompanying drawings, all of which form a part of this specification, wherein like reference numerals designate corresponding parts in the various figures. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only and are not intended as a definition of the limits of the invention. As used in the specification and the claims, the singular form of "a," "an," and "the" include plural referents unless the context clearly dictates otherwise.

BRIEF DESCRIPTION OF THE DRAWINGS AND APPENDICES

[0009] Additional advantages and details of non-limiting embodiments are explained in greater detail below with reference to the exemplary embodiments that are illustrated in the accompanying schematic figures, in which:

[0010] Figure 1 discloses a schematic diagram of a method of registration of the second account holder device with the primary account holder device.

[0011] Figure 2 discloses an illustration of an exemplary embodiment in which payment is initiated from the secondary account holder.

[0012] Figure 3 shows a flowchart that illustrates a method for registration of the second account holder device with the primary account holder device.

[0013] Figure 4 shows a flowchart that illustrates a method for transactions in which the payment is initiated from the secondary account holder.

DESCRIPTION OF THE DISCLOSURE

[0014] 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.

[0015] 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.

[0016] 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.

[0017] 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.

[0018] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0019] For purposes of the description hereinafter, the terms “end,” “upper,” “lower,” “right,” “left,” “vertical,” “horizontal,” “top,” “bottom,” “lateral,” “longitudinal,” and derivatives thereof shall relate to the invention as it is oriented in the drawing figures. However, it is to be understood that the invention may assume various alternative variations and step sequences, except where expressly specified to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings, and described in the following specification, are simply exemplary embodiments or aspects of the invention. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

[0020] As used herein, the terms “communication” and “communicate” may refer to the reception, receipt, transmission, transfer, provision, and/or the like of information (e.g., data,

signals, messages, instructions, commands, and/or the like). For one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to be in communication with another unit means that the one unit is able to directly or indirectly receive information from and/or transmit information to the other unit. This may refer to a direct or indirect connection (e.g., a direct communication connection, an indirect communication connection, and/or the like) that is wired and/or wireless in nature. Additionally, two units may be in communication with each other even though the information transmitted may be modified, processed, relayed, and/or routed between the first and second unit. For example, a first unit may be in communication with a second unit even though the first unit passively receives information and does not actively transmit information to the second unit. As another example, a first unit may be in communication with a second unit if at least one intermediary unit (e.g., a third unit located between the first unit and the second unit) processes information received from the first unit and communicates the processed information to the second unit. In some non-limiting embodiments, a message may refer to a network packet (e.g., a data packet and/or the like) that includes data. It will be appreciated that numerous other arrangements are possible.

[0021] As used herein, the term "merchant" may refer to an individual or entity that provides goods and/or services, or access to goods and/or services, to customers based on a transaction, such as a payment transaction. The term "merchant" or "merchant system" may also refer to one or more computer systems operated by or on behalf of a merchant, such as a server computer executing one or more software applications. A "point-of-sale (POS) system," as used herein, may refer to one or more computers and/or peripheral devices used by a merchant to engage in payment transactions with customers, including one or more card readers, near-field communication (NFC) receivers, RFID receivers, and/or other contactless transceivers or receivers, contact-based receivers, payment terminals, computers, servers, input devices, and/or other like devices that can be used to initiate a payment transaction.

[0022] The term "portable financial device" may be used to refer to a payment card (e.g., a credit or debit card), a gift card, a smartcard, smart media, a payroll card, a healthcare card, a wrist band, a machine-readable medium containing account information, a keychain device or fob, an RFID transponder, a retailer discount or loyalty card, a mobile device executing an electronic wallet application, a personal digital assistant, a security card, an access card, a wireless terminal, and/or a transponder, as examples. The portable financial device may include

a volatile or a non-volatile memory to store information, such as an account identifier or a name of the account holder.

[0023] As used herein, the term "computing device" may refer to one or more electronic devices that are configured to directly or indirectly communicate with or over one or more networks. A computing device may be a mobile or portable computing device, a desktop computer, a server, and/or the like. Furthermore, the term "computer" may refer to any computing device that includes the necessary components to receive, process, and output data, and normally includes a display, a processor, a memory, an input device, and a network interface. A "computing system" may include one or more computing devices or computers. An "application" or "Application Program Interface" (API) refers to computer code or other data sorted on a computer-readable medium that may be executed by a processor to facilitate the interaction between software components, such as a client-side front-end and/or server-side back-end for receiving data from the client. An "interface" refers to a generated display, such as one or more graphical user interfaces (GUIs) with which a user may interact, either directly or indirectly (e.g., through a keyboard, mouse, touchscreen, etc.). Further, multiple computers, e.g., servers, or other computerized devices, such as an autonomous vehicle including a vehicle computing system, directly or indirectly communicating in the network environment may constitute a "system" or a "computing system".

[0024] It will be apparent that systems and/or methods, described herein, can be implemented in different forms of hardware, software, or a combination of hardware and software. The actual specialized control hardware or software code used to implement these systems and/or methods is not limiting of the implementations. Thus, the operation and behavior of the systems and/or methods are described herein without reference to specific software code, it being understood that software and hardware can be designed to implement the systems and/or methods based on the description herein.

[0025] Some non-limiting embodiments or aspects are described herein in connection with thresholds. As used herein, satisfying a threshold may refer to a value being greater than the threshold, more than the threshold, higher than the threshold, greater than or equal to the threshold, less than the threshold, fewer than the threshold, lower than the threshold, less than or equal to the threshold, equal to the threshold, etc.

[0026] Figure 1 discloses a schematic diagram of a method for registration **100** of the secondary account holder **104** device with the primary account holder device **102**. The method of registration **100** shows a launchpad 1**10**, login screen **112**, addition of secondary account holder tab **114**, scanning QR code with camera block **116**, generation of QR code **120**,

customizing registration **118**, information forwarding **106** and the issuer's backend **108**. The primary account holder device **102** can authorize (to issuer) to use additional number on which OTP can be shared. The primary account holder device **102** can also customize the type, amount and number of transactions for which this sharing can be done. On the device where secondary SIM is present, issuer's mobile banking application is used to generate a digital fingerprint of the device. Further, fingerprint includes International Mobile Equipment Identity is a 15-digit number unique to each device (IMEI), International Mobile Subscriber Identity (IMSI) is a 15-digit number for every user in a Global System for Mobile communication (GSM) and Phone number information and is represented in the form of Quick Response (QR) code. The mobile banking application needs to be configured in the secondary account holder device **104.** The primary account holder device **102** uses issuer's mobile banking application, logs in to it and selects option to authorize secondary account holder **104** device. Further, the camera of the primary account holder device **102** is used to scan the QR code that is generated in the secondary account holder **104** device. Using the same mobile banking application, the primary account holder device **102** can customize information related to the account. For instance, the amount in transactions, number of transactions, duration until which the secondary account holder device **104** will be active, and the like. Thereafter, the captured information is sent securely to the issuer's backend **108** and provisions are made accordingly.

[0027] Figure 2 discloses an illustration **200** of an exemplary embodiment in which payment is initiated from the secondary account holder. The illustration **200** shows a secondary account holder device **202**, merchant application tab **204**, information forwarding **206**, acquirer system **208**, issuer system **210** and approval block **212.** The secondary account holder device **202** opens the merchant application **204** clicks and adds items to the cart, under the payment option against a particular card. When customer chooses the card and clicks on payment, a request from the merchant flows **206** to the gateway of the respective issuer to allow secondary account holder device **202** to receive a One Time Password (OTP) via SMS. Secondary account holder device **202** fingerprint can be sent along with the request. Merchant can embed same device fingerprinting Software Developing Kit (SDK) within merchant's application. During Payment flow merchant app can get the device fingerprint and send it to the backend gateway, and gateway will transmit that to the issuer system **210** for verification before sending the OTP to the secondary account holder device **202**. In some embodiments, issuer system **210** is enhanced to take care of secondary registration process, sending OTP to secondary account holder device **202** and honor authentication request from secondary account holder device **202**. Customer issuer application needs to be enhanced to facilitate secondary account holder **202**

device registration process. Merchant systems needs to be enhanced to handle additional parameter to enable secondary account holder device **202** One Time Password (OTP) reception preference and to pass it downstream. Also, merchant Application Programming Interface (API) needs to be enhanced to accept additional parameter to enable secondary account holder device **202** OTP reception preference and to pass it downstream.

[0028] Figure 3 shows a flowchart **300** that illustrates a method for registration of the second account holder device with the primary account holder device **102**. At block **302**, the method comprises installing the banking application in secondary account holder device **104**. Upon installation, at block **304** a digital fingerprint is generated with the help of International Mobile Equipment Identity is a 15-digit number unique to each device(IMEI), International Mobile Subscriber Identity (IMSI) is a 15-digit number for every user in a Global System for Mobile communication (GSM)) and Phone number information and is represented in the form of Quick Response (QR) code. At block **306,** the primary account holder device **102** scans the QR code generated in the secondary account holder device **104** by primary account holder device's **102** camera. At block **308**, the primary account holder can customize the amount in transactions, type, number of transactions and the like. At block **310,** sending the customized information to the Issuer's end and provisioning is done.

[0029] Figure 4 shows a flowchart **400** that illustrates a method for transactions in which the payment is initiated from the secondary account holder to the gateway and respective issuer to allow secondary account holder device **104** to receive SMS with OTP. At block **402, the** secondary account holder device **104** opens the merchant application, clicks and adds items to the cart, under the payment option against a particular card. Upon choosing the card and clicking on payment, at block **404,** a request for the merchant flows to the gateway and is forwarded towards the acquirer's bank. At block **406,** the acquirer's bank forwards the information to the issuer's bank. At block 408, the issuer's bank receives the cryptogram or digital fingerprint and performs a back-end verification of the same. At block **410,** a One Time Password (OTP) has to be entered by the secondary account holder device **104**, after which the payment will be approved.

[0030] The method of registration **100** may facilitate operations in multiple operating systems. Examples of operating systems include, without limitation, APPLE® MACINTOSH® OS X®, UNIX®, UNIX-like system distributions (E.G., BERKELEY SOFTWARE DISTRIBUTION® (BSD), FREEBSD®, NETBSD®, OPENBSD, etc.), LINUX® DISTRIBUTIONS (E.G., RED HAT®, UBUNTU®, KUBUNTU®, etc.), IBM®OS/2®, MICROSOFT® WINDOWS® (XP®, VISTA®/7/8, 10 etc.), APPLE® IOS®, GOOGLE™ ANDROID™, BLACKBERRY® OS, or

the like. The banking application may facilitate display, execution, interaction, manipulation, or operation of program components through textual or graphical facilities. For example, user interfaces may provide computer interaction interface elements on a display system operatively connected to the computer system, such as cursors, icons, checkboxes, menus, scrollers, windows, widgets, etc. Graphical User Interfaces (GUIs) may be employed, including, without limitation, Apple® Macintosh® operating systems' Aqua®, IBM® OS/2®, Microsoft® Windows® (e.g., Aero, Metro, etc.), web interface libraries (e.g., ActiveX®, Java®, Javascript®, AJAX, HTML, Adobe® Flash®, etc.), or the like.

[0031] In some embodiments, the method of registration **100** may be an implement on the web browser. The web browser 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 1308 may utilize facilities such as AJAX, DHTML, ADOBE® FLASH®, JAVASCRIPT®, JAVA®, Application Programming Interfaces (APIs), etc. In some embodiments, the computer system 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 Active Server Pages (ASP), ACTIVEX®, ANSI® C++/C#, MICROSOFT®, .NET, 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. In some embodiments, the computer system 1300 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.

[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., non-transitory. Examples include Random Access

Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, Compact Disc (CD) ROMs, Digital Video Disc (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.

[0035] Although the invention has been described in detail for the purpose of illustration based on what is currently considered to be the most practical and preferred embodiments, it is to be understood that such detail is solely for that purpose and that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the spirit and scope of the appended claims. For example, it is to be understood that the present invention contemplates that, to the extent possible, one or more features of any embodiment can be combined with one or more features of any other embodiment.

METHOD AND SYSTEM FOR FACILITATING AUTHENTICATION OF SECONDARY ACCOUNT HOLDER DEVICE FOR TRANSACTIONS ORIGINATED AGAINST PRIMARY CARDHOLDER'SACCOUNT

ABSTRACT

The present disclosure provides a method and system to facilitate authentication of secondary account holder device **104** for transactions originated against primary cardholder's account. The present disclosure facilitates primary card holder to update issuer system **210** with valid secondary account holder device **104**, which to be approved. Also, the present disclosure facilitates a process through which transaction processing through merchant portal is taken care when second factor authentication is provided by secondary account holder device **104**. Therefore, the present disclosure avoids repeated transactions through primary account holder device **102**, and hence improved overall Pre-settlement Risk (PSR) rate. A secondary account holder device **104** will initiate and complete the transaction with authentication without depending on the actual card holder to share the One Time Password (OTP).

Fig. 2

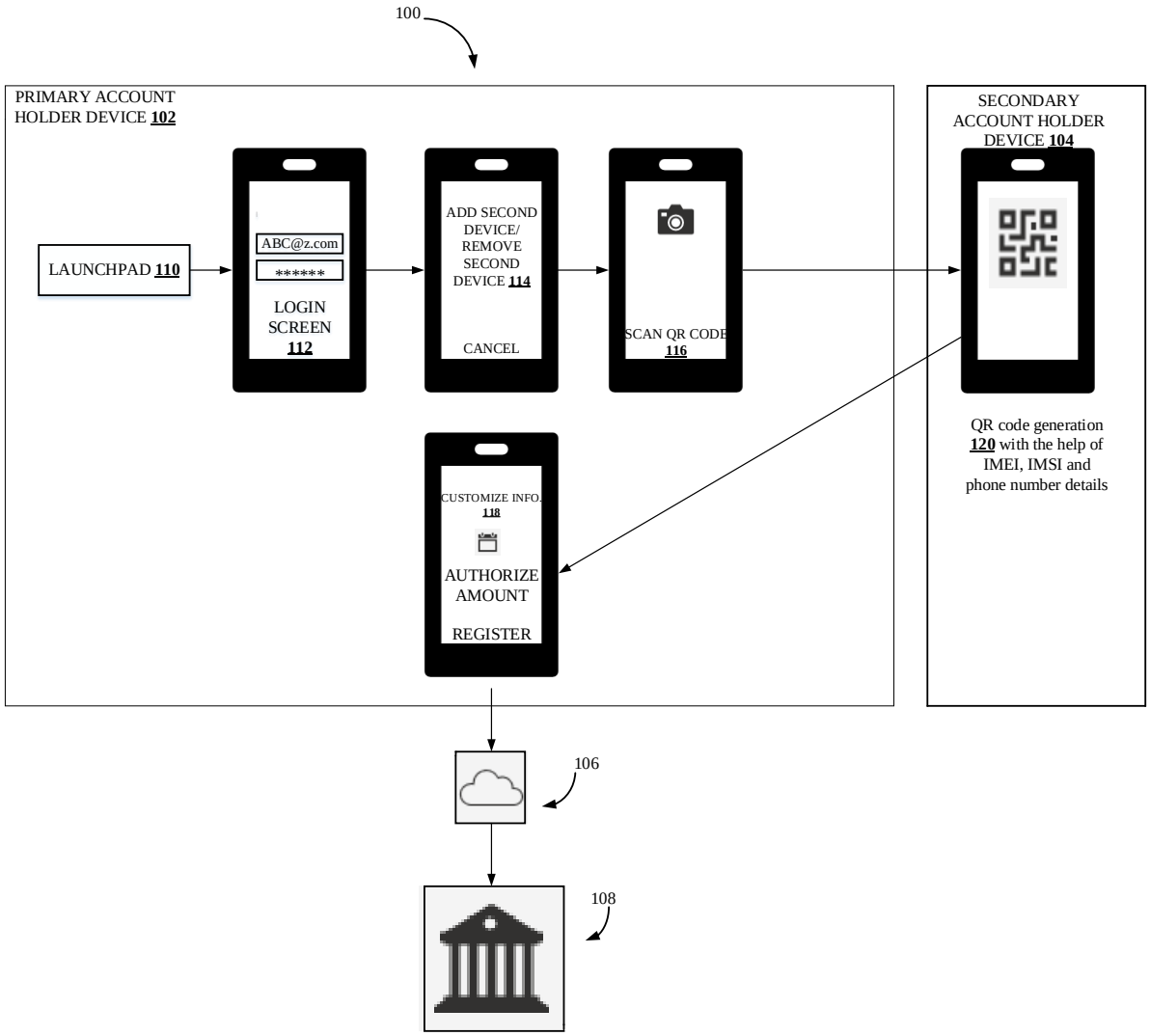

Figure 1: Registration of Secondary account holder device with primary account holder device

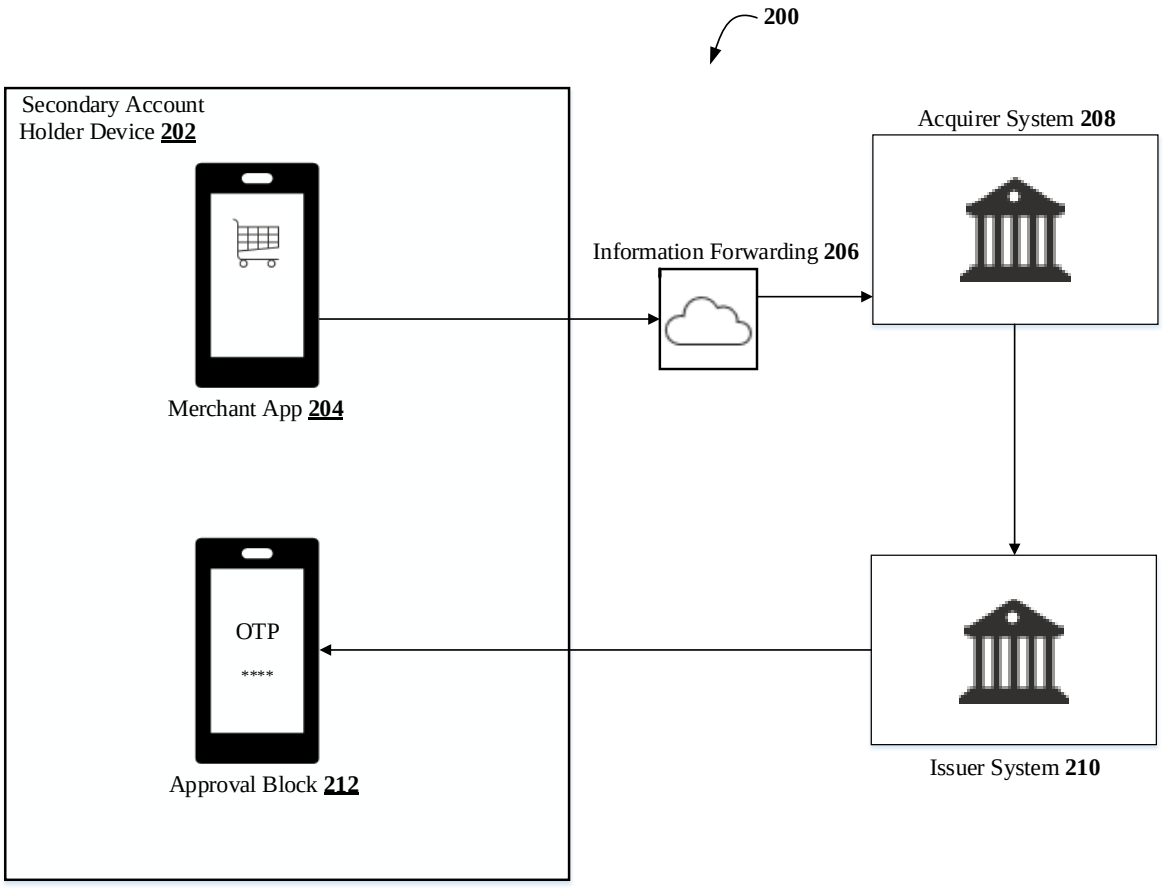

Figure 2: Payment is Initiated from Secondary Account Holder Device

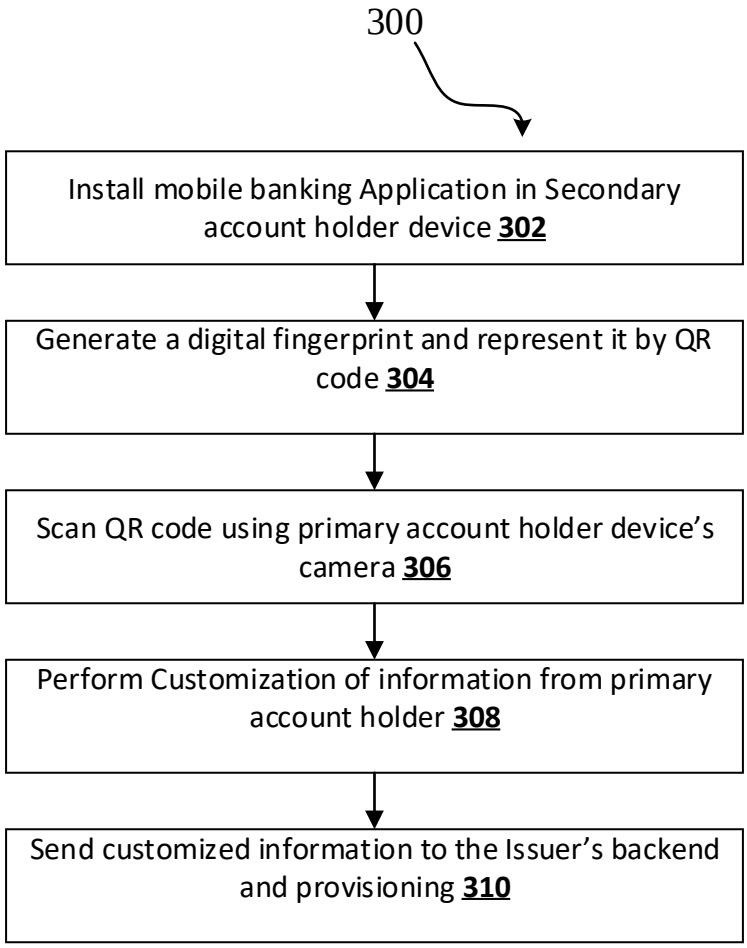

Figure 3: Flowchart for method of Registration of Secondary account holder device

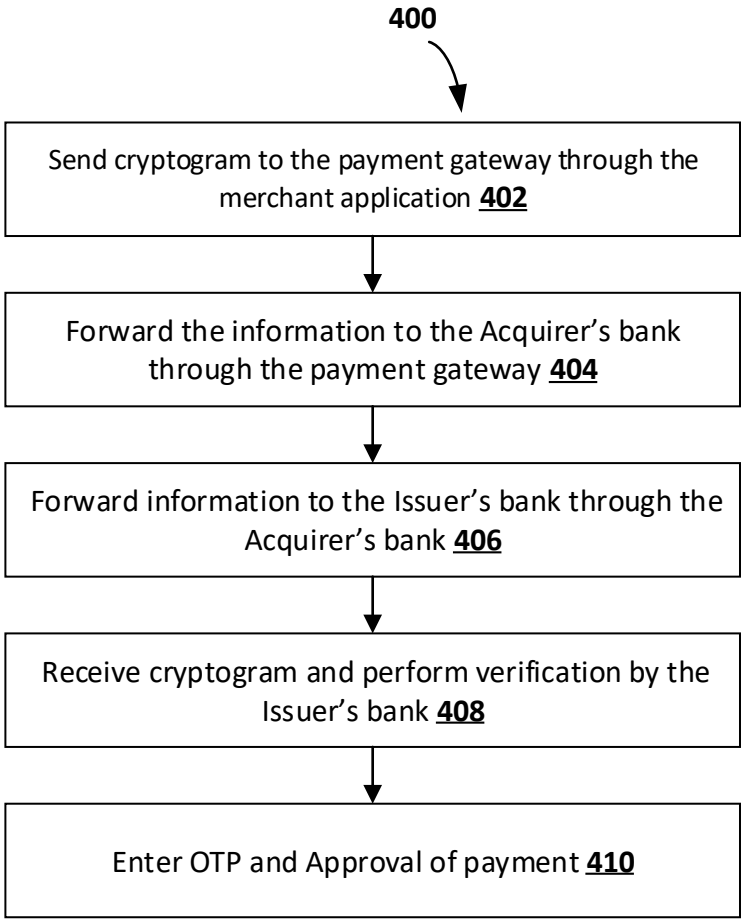

Figure 4: Flowchart for Payment initiated from secondary device