22 Aug 2024

ON DEMAND DIGITAL CARD DISPLAY

ANUP TRIPATHI
VISA

IMO AKPAN
VISA

HAVEN VU
VISA

SURESH KALAKRISHNAN
VISA

TITLE: ON DEMAND DIGITAL CARD DISPLAY

APPLICANT: VISA INTERNATIONAL SERVICE ASSOCIATION

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

Nationality: USA

INVENTORS: ANUP TRIPATHI

IMO AKPAN

HAVEN VU

SURESH KALAKRISHNAN

TECHNICAL FIELD

[0001] The present disclosure in general relates to payment systems. In particular, the subject matter relates to performing ecommerce transactions independent of an issuer interface.

BACKGROUND

[0002] E-commerce transactions are rapidly evolving as technology continues to advance. The emergence of new payment methods, such as digital wallets, cryptocurrencies, and contactless payments, has significantly transformed the way people buy and sell goods online. With the increasing prevalence of mobile devices, consumers now have greater flexibility in completing transactions anytime and anywhere, fostering a more seamless and convenient shopping experience.

[0003] To conduct eCommerce transactions, cardholders are required to input their payment card details. However, to retrieve account information linked to the payment card, cardholders must either be enrolled in an issuer interface (such as an issuer application or website) supporting digital card display or possess the physical payment card. Without these options, cardholders are unable to access the account information related to their payment cards. This challenge becomes particularly evident in cases where a merchant, such as an airline company without direct involvement in issuing payment cards, seeks to provide cash equivalent credentials like vouchers. In such scenarios, the merchant is unable to offer a digital solution because it lacks a direct association with an issuer interface capable of disclosing the account information.

[0004] Moreover, in instances where a payment card is provisioned onto a cardholder's mobile device such as, for example, into a native wallet, the cardholder is permitted to make digital payments through the native wallet but is not permitted to access the account information associated with the provisioned payment card within the native wallet. Therefore, there is a need to overcome the above-mentioned limitations.

[0005] 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

[0006] 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 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:

[0007] Fig. 1 illustrates an exemplary method of accessing account information associated with a payment card through second link.

[0008] Fig. 2 illustrates an exemplary method of accessing account information associated with a payment card within native wallet through an application clip.

[0009] Fig. 3 illustrates an exemplary method of accessing account information associated with a payment card within the native wallet.

[0010] Fig. 4 illustrates an exemplary sequence diagram for accessing account information associated with a payment card.

[0011] 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

[0012] The following disclosure may provide exemplary systems, devices, and methods for conducting a financial transaction and related activities. More specifically, the present disclosure provides methods and systems for providing on demand access to account information associated with a payment card requested for a user by a merchant, wherein the on-demand access is achieved independent of an issuer interface. Although reference may be

made to such financial transactions in the examples provided below, aspects are not so limited. That is, the systems, methods, and apparatuses may be utilized for any suitable purpose.

[0013] Before discussing specific embodiments, aspects, or examples, some descriptions of terms used herein are provided below.

[0014] A "payment card" can refer to any device that may be used to conduct a transaction, such as a financial transaction. For example, a payment card may be used to provide payment information to a merchant. A payment card can include a substrate such as a paper, metal, or plastic card, and information that is printed, embossed, encoded, and/or otherwise included at or near a surface of the payment card. A payment card can be hand-held and compact so that it can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). A payment card can be a smart card, a debit device (e.g., a debit card), a credit device (e.g., a credit card), a stored value device (e.g., a stored value card or "prepaid" card), a magnetic stripe card, a security card, an access card, a memory card, and/or an identification card, among others. A payment card may operate in a swipe, contact and/or contactless mode. For example, a payment card may be an electronic payment device, such as a smart card, a chip card, an integrated circuit card, and/or a near field communications (NFC) card, among others. An electronic payment device may include an embedded integrated circuit and the embedded integrated circuit may include a data storage medium (e.g., volatile and/or non-volatile memory) to store information associated with the electronic payment device, such as an account identifier and/or a name of an account holder. A payment card may interface with an access device such as a point-of-sale device to initiate the transaction.

[0015] The terms "user device" and "user device" refer to any electronic device that is configured to communicate with one or more servers or remote devices and/or systems. A user device or a user device may include a mobile device, a network-enabled appliance (e.g., a network-enabled television, refrigerator, thermostat, and/or the like), a computer, a POS system, and/or any other device or system capable of communicating with a network. A user device may further include a desktop computer, laptop computer, mobile computer (e.g., smartphone), a wearable computer (e.g., a watch, pair of glasses, lens, clothing, and/or the like), a cellular phone, a network-enabled appliance (e.g., a network-enabled television, refrigerator, thermostat, and/or the like), a point of sale (POS) system, and/or any other device, system, and/or software application configured to communicate with a remote device or system.

[0016] As used herein, the term “communication” and “communicate” may refer to the reception, receipt, transmission, transfer, provision, and/or the like of information (e.g., data, signals, messages, instructions, calls, commands, and/or the like). A communication may use a direct or indirect connection and may be wired and/or wireless in nature. As an example, for one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to communicate 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. The one unit may communicate with the other unit even though the information may be modified, processed, relayed, and/or routed between the one unit and the other unit. In one example, a first unit may communicate with a second unit even though the first unit receives information and does not communicate information to the second unit. For example, a first unit may be in communication with a second unit even though the first unit passively receives data and does not actively transmit data to the second unit. As another example, a first unit may communicate with a second unit if an intermediary unit (e.g., a third unit located between the first unit and the second unit) receives information from the first unit, processes the information received from the first unit to produce processed information, and communicates the processed information to the second unit. In some non-limiting embodiments or aspects, a message may refer to a packet (e.g., a data packet, a network packet, and/or the like) that includes data. It will be appreciated that numerous other arrangements are possible.

[0017] A “communication channel” or “connection” may refer to any suitable path for communication between two or more entities. Suitable communications channels may be present directly between two entities such as a payment processing network and a merchant or issuer computer or may include a number of different entities. Any suitable communications protocols may be used for generating a communications channel. A communication channel may in some instances comprise a “secure communication channel” or a “tunnel,” either of which may be established in any known manner, including the use of mutual authentication and a session key and establishment of a secure communications session. However, any method of creating a secure communication channel may be used, and communication channels may be wired or wireless, as well as long-range, short-range, or medium range. By establishing a secure channel, sensitive information related to a payment device (such as account number, CVV values, expiration dates, etc.) may be securely transmitted between the two entities to facilitate a transaction.

[0018] As used herein, the term “computing device” or “computer 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 device, a desktop computer, and/or the like. As an example, a mobile device may include a cellular phone (e.g., a smartphone or standard cellular phone), a portable computer, a wearable device (e.g., watches, glasses, lenses, clothing, and/or the like), a personal digital assistant (PDA), and/or other like devices. The computing device may not be a mobile device, such as a desktop computer. Furthermore, the term “computer” may refer to any computing device that includes the necessary components to send, receive, process, and/or output data, and normally includes a display device, a processor, a memory, an input device, a network interface, and/or the like.

[0019] Reference to “a device,” “a server,” “a processor,” and/or the like, as used herein, may refer to a previously recited device, server, or processor that is recited as performing a previous step or function, a different server or processor, and/or a combination of servers and/or processors. For example, as used in the specification and the claims, a first server or a first processor that is recited as performing a first step or a first function may refer to the same or different server or the same or different processor recited as performing a second step or a second function.

[0020] An “interface” may include any software module configured to process communications. For example, an interface may be configured to receive, process, and respond to a particular entity in a particular communication format. Further, a computer, device, and/or system may include any number of interfaces depending on the functionality and capabilities of the computer, device, and/or system. In some embodiments or aspects, an interface may include an application programming interface (API) or other communication format or protocol that may be provided to third parties or to a particular entity to allow for communication with a device. Additionally, an interface may be designed based on functionality, a designated entity configured to communicate with, or any other variable. For example, an interface may be configured to allow for a system to field a particular request or may be configured to allow a particular entity to communicate with the system.

[0021] “Provisioning” may include a process of providing data for use. For example, provisioning may include providing, delivering, or enabling a token on a device. Provisioning

may be completed by any entity within or external to the transaction processing system. For example, in some embodiments or aspects, tokens may be provisioned by an issuer or a payment processing network onto a mobile device of a consumer (e.g. account holder). The provisioned tokens may have corresponding token data stored and maintained in the token vault or token registry. In some embodiments or aspects, a token vault or token registry may generate a token that may then be provisioned or delivered to a device. In some embodiments or aspects, an issuer may specify a token range from which token generation and provisioning can occur. Further, in some embodiments or aspects, an issuer may generate and notify a token vault of a token value and provide the token record information (e.g., token attributes) for storage in the token vault.

[0022] As used herein, the term “server” may include one or more computing devices which can be individual, stand-alone machines located at the same or different locations, may be owned or operated by the same or different entities, and may further be one or more clusters of distributed computers or “virtual” machines housed within a datacentre. It should be understood and appreciated by a person of skill in the art that functions performed by one “server” can be spread across multiple disparate computing devices for various reasons. As used herein, a “server” is intended to refer to all such scenarios and should not be construed or limited to one specific configuration. Further, a server as described herein may, but need not, reside at (or be operated by) a merchant, a payment network, a financial institution, a healthcare provider, a social media provider, a government agency, or agents of any of the aforementioned entities. The term “server” may also refer to or include one or more processors or computers, storage devices, or similar computer arrangements that are operated by or facilitate communication and processing for multiple parties in a network environment, such as the Internet, although it will be appreciated that communication may be facilitated over one or more public or private network environments and that various other arrangements are possible. Further, multiple computers, e.g., servers, or other computerized devices, e.g., point-of-sale devices, directly or indirectly communicating in the network environment may constitute a “system,” such as a merchant's point-of-sale system. Reference to “a server” or “a processor,” as used herein, may refer to a previously recited server and/or processor that is recited as performing a previous step or function, a different server and/or processor, and/or a combination of servers and/or processors. For example, as used in the specification and the claims, a first server and/or a first processor that is recited as performing a first step or function

may refer to the same or different server and/or a processor recited as performing a second step or function.

[0023] As used herein, the term “system” may refer to one or more computing devices or combinations of computing devices (e.g., processors, servers, client devices, software applications, components of such, and/or the like).

[0024] A “token” or “payment token” may include an identifier for a payment account that is a substitute for an account identifier, such as a primary account number (PAN). For example, a token may include a series of numeric and/or alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token “4900 0000 0000 0001” may be used in place of a PAN “4147 0900 0000 1234.” In some embodiments or aspects, a token may be “format preserving” and may have a numeric format that conforms to the account identifiers used in existing payment processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments or aspects, a token may be used in place of a PAN to initiate, authorize, settle or resolve a payment transaction or represent the original credential in other systems where the original credential would typically be provided. In some embodiments or aspects, a token value may be generated such that the recovery of the original PAN or other account identifier from the token value may not be computationally derived. For example, a token may have a random association with a particular real PAN so that the real PAN is not computationally derivable from the token. A lookup table may be used to associate a real PAN and a corresponding random token. Further, in some embodiments or aspects, the token format may be configured to allow the entity receiving the token to identify it as a token and recognize the entity that issued the token.

[0025] A “token request message” may be an electronic message for requesting a token. A token request message may include information usable for identifying a payment account or digital wallet, and/or information for generating a payment token. For example, a token request message may include payment credentials, mobile device identification information (e.g. a phone number or MSISDN), a digital wallet identifier, information identifying a tokenization service provider, a merchant identifier, a cryptogram, and/or any other suitable information. Information included in a token request message can be encrypted (e.g., with an issuer-specific key). In some embodiments or aspects, a token request message may be formatted as an authorization request message (e.g., an ISO 8583 message format). In some embodiments or

aspects, the token request message may have a zero-dollar amount in an authorization amount field. As another example, the token request message may include a flag or other indicator specifying that the message is a token request message.

[0026] A "token response message" may be a message that responds to a token request. A token response message may include an indication that a token request was approved or denied. A token response message may also include a payment token, mobile device identification information (e.g. a phone number or MSISDN), a digital wallet identifier, information identifying a tokenization service provider, a merchant identifier, a cryptogram, and/or any other suitable information. Information included in a token response message can be encrypted (e.g., with an issuer-specific key). In some embodiments or aspects, a token response message may be formatted as an authorization response message (e.g., an ISO 8583 message format). In some embodiments or aspects, the token response message may have a zero-dollar amount in an authorization amount field. As another example, the token response message may include a flag or other indicator specifying that the message is a token response message.

[0027] A "token service provider" may refer to an entity including one or more server computers in a token service system that generates, processes and maintains tokens. The token service provider may include or be in communication with a token vault where the generated tokens are stored. Specifically, the token vault may maintain one-to-one mapping between a token and a primary account number (PAN) represented by the token. The token service provider may have the ability to set aside licensed BINs as token BINs to issue tokens for the PANs that may be submitted to the token service provider. Various entities of a tokenization ecosystem may assume the roles of the token service provider. For example, payment networks and issuers or their agents may become the token service provider by implementing the token services according to embodiments or aspects of the present disclosure. A token service provider may provide reports or data output to reporting tools regarding approved, pending, or declined token requests, including any assigned token requestor IDs. The token service provider may provide data output related to token-based transactions to reporting tools and applications and present the token and/or PAN as appropriate in the reporting output.

[0028] A "token vault" may refer to a repository that maintains established token-to-PAN mappings. According to various embodiments or aspects, the token vault may also maintain other attributes of the token requestor that may be determined at the time of registration and

that may be used by the token service provider to apply domain restrictions or other controls during transaction processing. For example, the token vault may maintain one-to-one mapping between a token and an account identifying number represented by the token. The token vault may be a part of the token service system. In some embodiments or aspects, the token vault may be provided as a part of the token service provider. Alternatively, the token vault may be a remote repository accessible by the token service provider. Token vaults, due to the sensitive nature of the data mappings that are stored and managed in them, may be protected by strong underlying physical and logical security.

[0029] As used herein an application clip can be a lesser-memory application that may use or otherwise include an application module of a greater-memory application. For example, the lesser-memory application may be stored as an Android Instant App™ or an iOS App Clip™, where the lesser-memory application may use one or more APIs used by a greater-memory application sharing an identifier with the lesser-memory application. The application clip may display a UI element. In some instances, the Application clip can be communicated in a message, or a deep link, that may include program code for a lesser-memory application, such as program code for an iOS App Clip or an Android Instant App.

[0030] The present disclosure provides a system and method to enable on-demand access to account information linked to a payment card requested by a user through a merchant.

[0031] A detailed explanation of the proposed solution is disclosed in the forthcoming paragraphs.

[0032] **Fig.1** illustrates an exemplary method (100) of accessing account information associated with a payment card. In the illustrated example, the merchant is an airline, the payment card is associated with a voucher issued to the user in connection with a flight. The customer may receive voucher as an email in a computing device. An application clip requires a flight record locator and a user’s last name for user identity verification, prior to permitting access to the account information associated with the payment card. The reader will appreciate that since the access method (100) is independent of an issuer interface, merchant specific user-identity verification data can be utilized. In other words, the digital card display flow, provided by the application clip, can be especially tailored to the merchant’s industry and/or preference. Such freedom is not afforded through a typical issuer interface.

[0033] Further to the above, the computing device displays, for example through the application clip, the account information, in response to a successful user-identify verification. In the illustrated example, the computing device displays the cardholder's name, the card number, expiration date, and security code. More or less account information can be displayed.

[0034] In some embodiments, the method (100) further includes receiving, by the computing device, a second communication, which can be in the form of a second deep link generated by the payment network on behalf of the merchant. The method (100) further includes receiving, by the computer device, a second input from the user. The second input can be provided through any suitable user interface such as, for example, a mouse, a keyboard, a touch screen, or microphone, for example. In some instances, the cardholder provides the second input by clicking on the second deep link. In response to the second input, the computing device invokes a second application clip for provisioning a token associated with the payment card. The user is prompted, by the computing device, for example through the second application clip, to complete an authentication protocol with the merchant cobrand issuer. Upon confirming a successful authentication, the merchant cobrand issuer communicates the successful authentication to the payment network. In response, the payment network, for example, uses the second application clip for initiating a payment card provisioning flow on the computing device. A token associated with the payment card can be provided into a digital wallet associated with the user.

[0035] Further to the above, in certain instances, the deep links generated by the payment network are directly sent by the payment network to the cardholder. In other instances, the deep links are sent to the issuer that sends the deep links to the cardholder. In other instances, the deep links are sent to the issuer that sends a message to the merchant to pass the deep links to the cardholder.

[0036] **Fig. 2** illustrates an exemplary method (200) of accessing account information associated with a payment as another embodiment of the disclosure. The method (200) is similar in many respects to the method (100). However, the method (200) runs the application clip for card display on a digital wallet associated with the user, which facilities interactions with the payment network for displaying the account information of a payment card. In the illustrated example, the cardholder prompts access to the account information, for example by clicking on an icon within the digital wallet, accessing the card number. The cardholder then

selects an option, for example from a dropdown menu, to access the account information. In response, the digital wallet prompts the user to perform a device authentication such as, for example, a Fast Identification Online (FIDO) authentication. In at least one example, the device authentication comprises a face identification, or a fingerprint identification. Moreover, the method (200) includes presenting, by the digital wallet, a Uniform Resource Locator (URL) card-reveal domain link, in response to successfully completing the device authentication. The URL Domain link may include an encrypted payload with a card ID associated with the payment card. The method (200) further includes receiving, by the digital wallet, a second input, and invoking, by the digital wallet, an application clip for displaying the account information independent of an issuer interface, in response the second input.

[0037] The digital wallet passes information to the payment network through the application clip in the form of an encrypted payload Blob. The cardholder then completes an issuer authentication protocol, and the payment network reveals the account information to the card holder.

[0038] Like the method (100), the method (200) may further include provisioning a token associated with the payment card into the digital wallet.

[0039] **Fig. 3** illustrates an exemplary method (300) of accessing the account information associated with a payment card in accordance with some embodiments. In **Fig 3**, the method (300) is similar in many respects to the method (100) and the method (200). However, the method (300) achieves accessing the account information within a digital wallet, without deep links, and without invoking an application clip. In the method (300), the digital wallet directly calls the payment network API to retrieve the account information. The digital wallet acting as an intermediary between the user and the payment system, initiates a direct call to the payment API to retrieve relevant details pertaining to the user’s account.

[0040] In the illustrated example, the method (300) includes receiving, by the digital wallet, an input from the user, prompting, by the digital wallet, the user to perform a device authentication, and transmitting, by the digital wallet, a message to a payment network indicative of successfully completing the device authentication by the user. In various instances, the digital wallet directly calls the payment network API to retrieve the account

information. The method further includes displaying, by the digital wallet, the account information.

[0041] Like the method (100), the method (200) may further include provisioning a token associated with the payment card into the digital wallet. In some instances, a token request message can be sent to the payment network to provision the token into the digital wallet. A token response message may be received by the digital wallet in response to the token request.

[0042] This revision emphasizes the direct interaction between the digital wallet and the payment network API, streamlining the process for efficient retrieval of account information while maintaining a focus on security and user authentication.

[0043] The order in which method (300) is described is not intended to be construed as a limitation, and any number of the described method steps may be combined in any order to implement the method. Additionally, individual steps may be deleted from the methods without departing from the scope of the subject matter described.

[0044] **Fig. 4** is an exemplary sequence diagram for accessing account information associated with a payment card. This sequence diagram may be referred to as an overall view for accessing account information associated with the payment card. This sequence diagram may describe the operations involved between the entities such as cardholder, merchant, merchant cobrand issuer, pay wallet back end and visa. The cardholder provides personal information, including their name, address, phone number, and email, to the merchant. The merchant forwards the cardholder's information to the issuer. The issuer stores this cardholder information on its backend system. The merchant may contact their cobrand issuer to obtain access to the 16-digit Personal Account Number (PAN) associated with the card. The issuer enrols the PAN in a UCE system and shares the cardholder's contact information with Visa. Visa returns a unique Card ID to associate with the PAN. Visa generates two Deep links and sends a message (via SMS or Email) to the cardholder's device on behalf of the merchant where the first link is Visa In-App Provisioning Application Clip Business As Usual (VIAP App Clip BAU) and the second link reveals card information (PAN, expiry Card Verification Value 2 (CVV2)). The second link can be a white label app clip used for Visa Digital Card Display (VDCD). The cardholder clicks on the first deep link, initiating an App Clip VIAP flow. The cardholder completes an authentication protocol. The issuer backend confirms identity and sends a success message to

Visa. Visa’s App Clip presents a "Push to pay" button, and the cardholder goes through the standard provisioning flow. The card is provisioned onto the cardholder's mobile wallet.

[0045] The cardholder clicks on the second link, invoking an App Clip Digital Card Display Flow. The cardholder completes an authentication protocol. The issuer backend confirms identity and sends a success message to Visa. Visa reveals PAN information, expiry, and generates CVV2.

[0046] In another embodiment, within the mobile wallet, the cardholder clicks on three dots, accessing the card number. The Pay wallet prompts a FIDO Authentication. The cardholder completes an authentication protocol. The Pay wallet calls Visa and invokes an App Clip experience for the cardholder. The issuer backend confirms identity and sends a success message to Visa. Visa reveals PAN information, expiry, and generates CVV2.

[0047] In another embodiment, the card display is performed with in the native wallet. In this embodiment the cardholder clicks on three dots and access the card number. The Pay wallet prompts a FIDO Authentication. Based on the authentication, the Pay wallet sends success message to visa and calls VDCD API. Visa reveals PAN information, expiry, and generates CVV2. The Pay wallet exposes PAN information, expiry, and CVV2 on the front end for the cardholder.

[0048] Some of the advantages of the present disclosure are listed below:

[0049] The method of the present disclosure allows to achieve on-demand access to the digital card independently of an issuer interface.

[0050] The method of the present disclosure also involve token provisioning into the digital wallet for added security and seamless future transactions.

[0051] The outlined procedures are presented to elucidate the showcased exemplary embodiments, with the understanding that ongoing technological advancements may alter the means by which specific functions are executed. These instances are provided for illustrative purposes rather than restrictive ones. Additionally, the demarcations of the functional components have been arbitrarily defined for descriptive convenience, and alternative

demarcations can be established as long as the designated functions and relationships are appropriately maintained. Persons skilled in the relevant art(s) will recognize alternative options (including equivalents, extensions, variations, deviations, etc., of those described herein) based on the teachings provided herein. Such alternatives are encompassed within the scope of the disclosed embodiments. It is also important to note that, as used herein, the singular forms "a," "an," and "the" encompass plural references unless the context clearly indicates otherwise.

[0052] Moreover, the implementation of embodiments consistent with the present disclosure may involve one or more computer-readable storage media. A computer-readable storage medium denotes any form of physical memory capable of storing information or data that can be read by a processor. Thus, a computer-readable storage medium may contain instructions for execution by one or more processors, including instructions for prompting the processor(s) to perform steps or stages consistent with the embodiments described herein. The term "computer-readable medium" should be interpreted to encompass tangible items and exclude carrier waves and transient signals, i.e., those that 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.

[0053] Lastly, the language chosen in the specification aims primarily for readability and instructional purposes, and it may not have been specifically chosen to define or limit the inventive subject matter. Therefore, the disclosure of the embodiments of this disclosure is intended to be illustrative, without imposing limitations on the scope of the disclosure.

[0054] 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.

ON DEMAND DIGITAL CARD DISPLAY

ABSTRACT

Disclosed herein is an outline of processes for accessing account information linked to a payment card, free from dependence on an issuer application. In this process a computing device first acquires a deep link from the payment network and then receives input from the user. Subsequently, an application clip is invoked in response to the user input, prompting the user for identity verification. Upon successful verification, the account information is displayed through the application clip, deep link or with in the native application.

Fig. 1

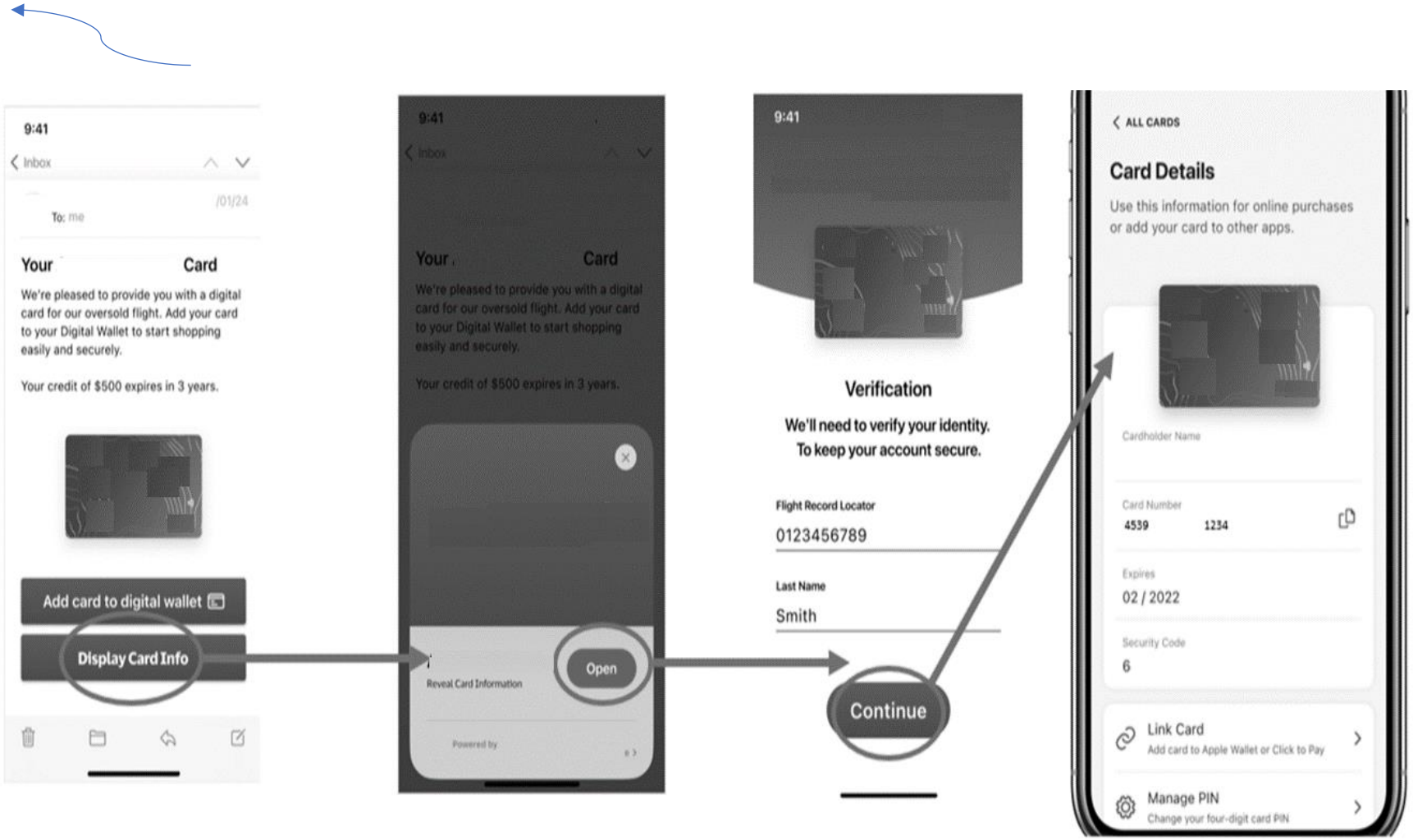
100
9:41
Inbox
To: me
Your Card
We're pleased to provide you with a digital card for our oversold flight. Add your card to your Digital Wallet to start shopping easily and securely.
Your credit of $500 expires in 3 years.
Add card to digital wallet
Display Card Info
Reveal Card Information
Open
Powered by
Verification
We'll need to verify your identity. To keep your account secure.
Flight Record Locator
0123456789
Last Name
Smith
Continue
ALL CARDS
Card Details
Use this information for online purchases or add your card to other apps.
Cardholder Name
Card Number
4539 1234
Expires
02 / 2022
Security Code
6
Link Card
Add card to Apple Wallet or Click to Pay
Manage PIN
Change your four-digit card PIN

Fig. 1

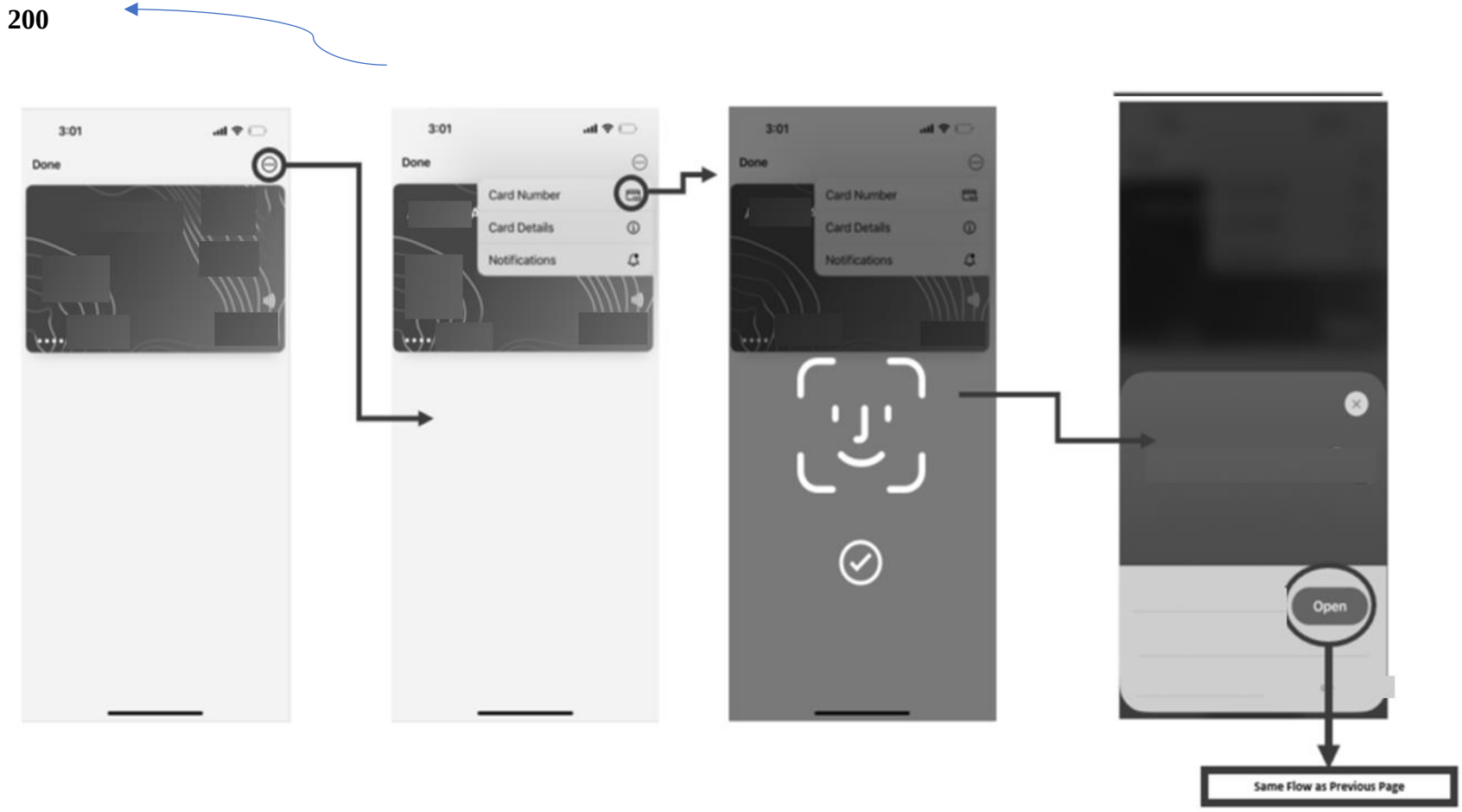
200
3:01
Done
3:01
Done
Card Number
Card Details
Notifications
3:01
Done
Card Number
Card Details
Notifications
Open
Same Flow as Previous Page

Fig. 2

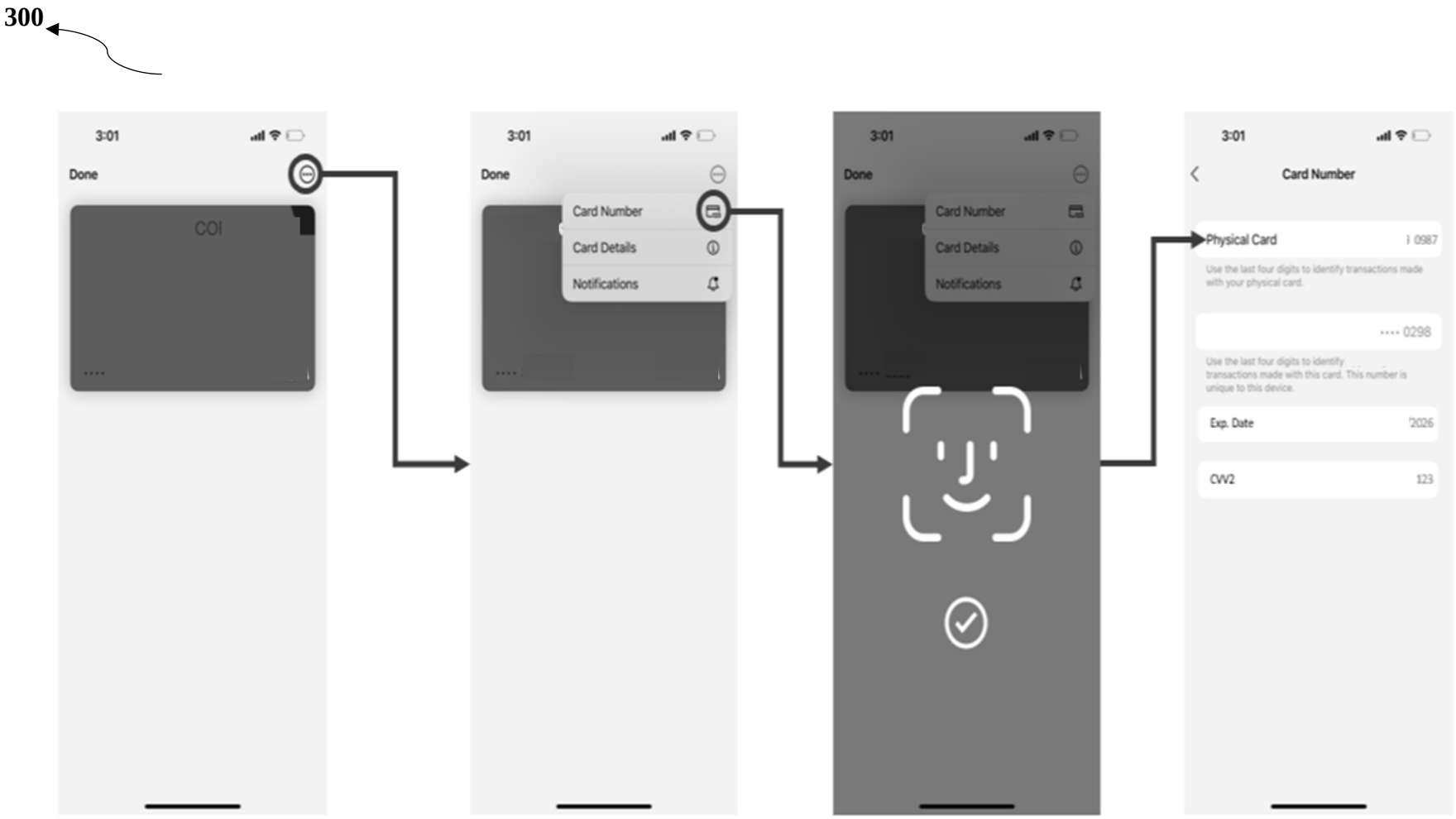
300
3:01
Done
Card Number
Card Details
Notifications
Physical Card
Use the last four digits to identify transactions made with your physical card.
Exp. Date
CVV2
123

Fig. 3

400

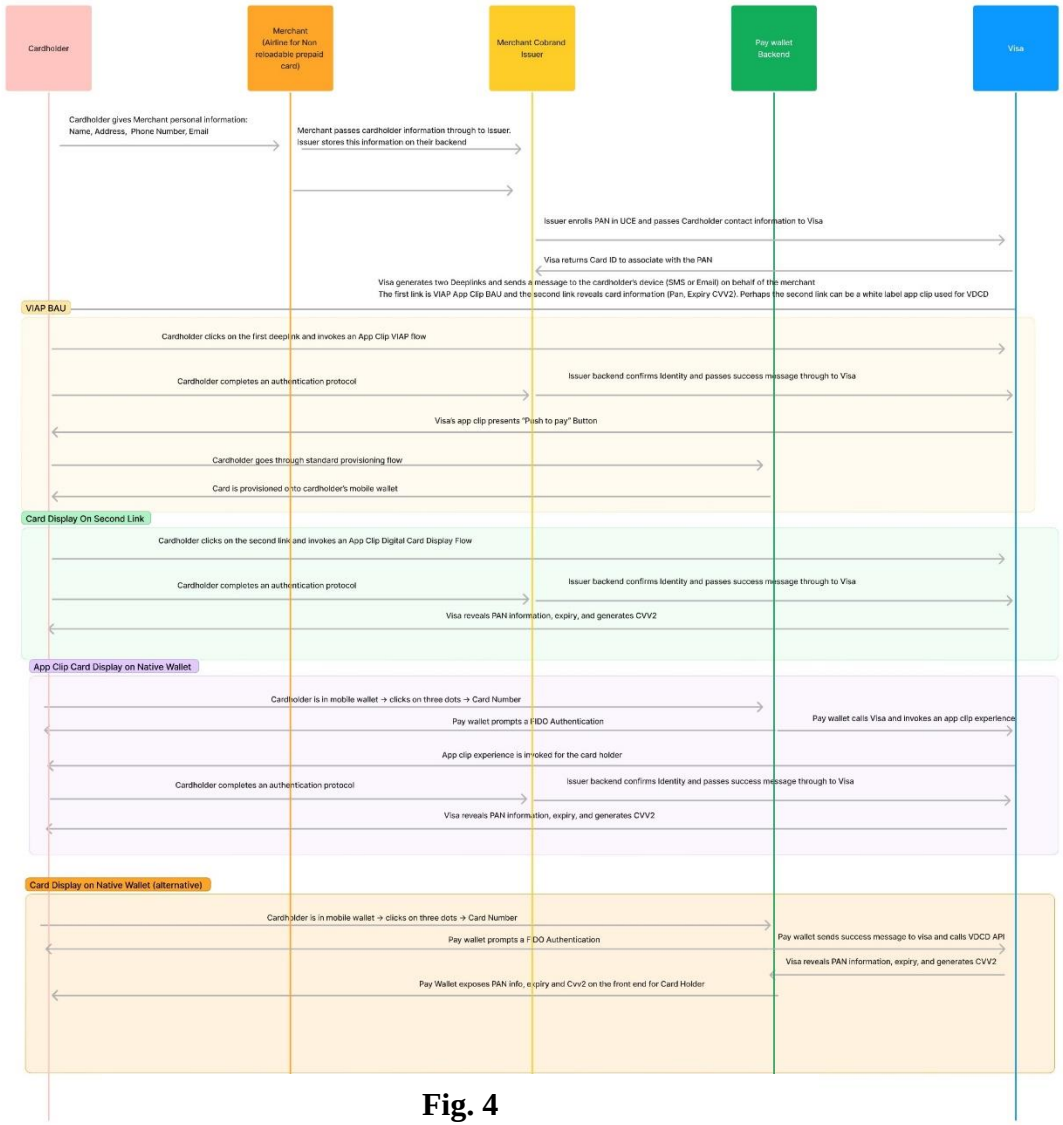
Cardholder
Merchant (Airline for Non reloadable prepaid card)
Merchant Cobrand Issuer
Pay wallet Backend
Visa
Cardholder gives Merchant personal information: Name, Address, Phone Number, Email
Merchant passes cardholder information through to Issuer. Issuer stores this information on their backend
Issuer enrolls PAN in UCE and passes Cardholder contact information to Visa
Visa returns Card ID to associate with the PAN
Visa generates two Deeplinks and sends a message to the cardholder's device (SMS or Email) on behalf of the merchant
The first link is VIAP App Clip BAU and the second link reveals card information (Pan, Expiry CVV2). Perhaps the second link can be a white label app clip used for VDCD
VIAP BAU
Cardholder clicks on the first deeplink and invokes an App Clip VIAP flow
Cardholder completes an authentication protocol
Issuer backend confirms Identity and passes success message through to Visa
Visa's app clip presents "Push to pay" Button
Cardholder goes through standard provisioning flow
Card is provisioned onto cardholder's mobile wallet
Card Display On Second Link
Cardholder clicks on the second link and invokes an App Clip Digital Card Display Flow
Cardholder completes an authentication protocol
Issuer backend confirms Identity and passes success message through to Visa
Visa reveals PAN information, expiry, and generates CVV2
App Clip Card Display on Native Wallet
Cardholder is in mobile wallet → clicks on three dots → Card Number
Pay wallet prompts a FIDO Authentication
Pay wallet calls Visa and invokes an app clip experience
App clip experience is invoked for the card holder
Cardholder completes an authentication protocol
Issuer backend confirms Identity and passes success message through to Visa
Visa reveals PAN information, expiry, and generates CVV2
Card Display on Native Wallet (alternative)
Cardholder is in mobile wallet → clicks on three dots → Card Number
Pay wallet prompts a FIDO Authentication
Pay wallet sends success message to visa and calls VDCD API
Visa reveals PAN information, expiry, and generates CVV2
Pay Wallet exposes PAN info, expiry and Cvv2 on the front end for Card Holder

Fig. 4