US 20210279993A1

(19) United States

(12) Patent Application Publication

Omojola et al.

(10) Pub. No.: US 2021/0279993 A1

(43) Pub. Date: Sep. 9, 2021

(54) **PAYMENT APPLICATION INITIATED GENERATION OF PAYMENT INSTRUMENTS**

(71) Applicant: **Square, Inc.**, San Francisco, CA (US)

(72) Inventors: **Ayokunle Omojola**, San Francisco, CA (US); **Robert Andersen**, New York, NY (US); **Daniele Perito**, San Francisco, CA (US); **Joachim Bekmann**, San Francisco (DE)

(21) Appl. No.: **17/191,646**

(22) Filed: **Mar. 3, 2021**

Related U.S. Application Data

(63) Continuation of application No. 17/065,240, filed on Oct. 7, 2020, now Pat. No. 10,991,191, which is a continuation of application No. 16/925,209, filed on Jul. 9, 2020, which is a continuation of application No. 15/721,212, filed on Sep. 29, 2017, now abandoned, which is a continuation of application No. 15/282,759, filed on Sep. 30, 2016, now Pat. No. 10,748,130.

Publication Classification

(51) **Int. Cl.**

G07F 7/08	(2006.01)
G06Q 20/34	(2006.01)
G06Q 20/32	(2006.01)
B41J 3/00	(2006.01)
B41J 2/00	(2006.01)
G06Q 20/10	(2006.01)

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

CPC ***G07F 7/082*** (2013.01); ***G06Q 20/3558*** (2013.01); ***G07F 7/086*** (2013.01); ***G06Q 20/3276*** (2013.01); ***G06Q 20/3221*** (2013.01); *G06Q 2220/00* (2013.01); ***B41J 3/00*** (2013.01); ***B41J 2/00*** (2013.01); ***G06Q 20/10*** (2013.01); ***G06Q 20/353*** (2013.01); *G06Q 20/3223* (2013.01); ***G06Q 20/354*** (2013.01)

(57) **ABSTRACT**

In some examples, a system and method for generating a payment instrument are described. The method includes receiving a unique signature that a recipient intends to associate with the payment instrument; verifying that the received feature meets an acceptability criterion; generating a representation of the received signature, wherein the representation is in a form capable of being physically associated with the payment instrument, and wherein association is established by embedding or exposing the representation on the payment instrument; and causing physical generation of the payment instrument having associated therewith the representation of the signature.

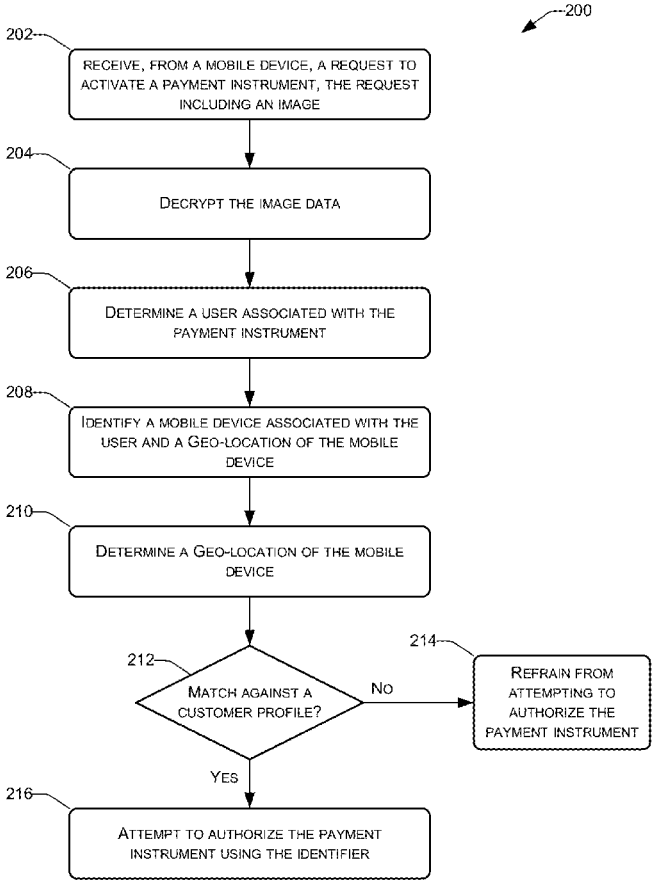

FIGURE 1

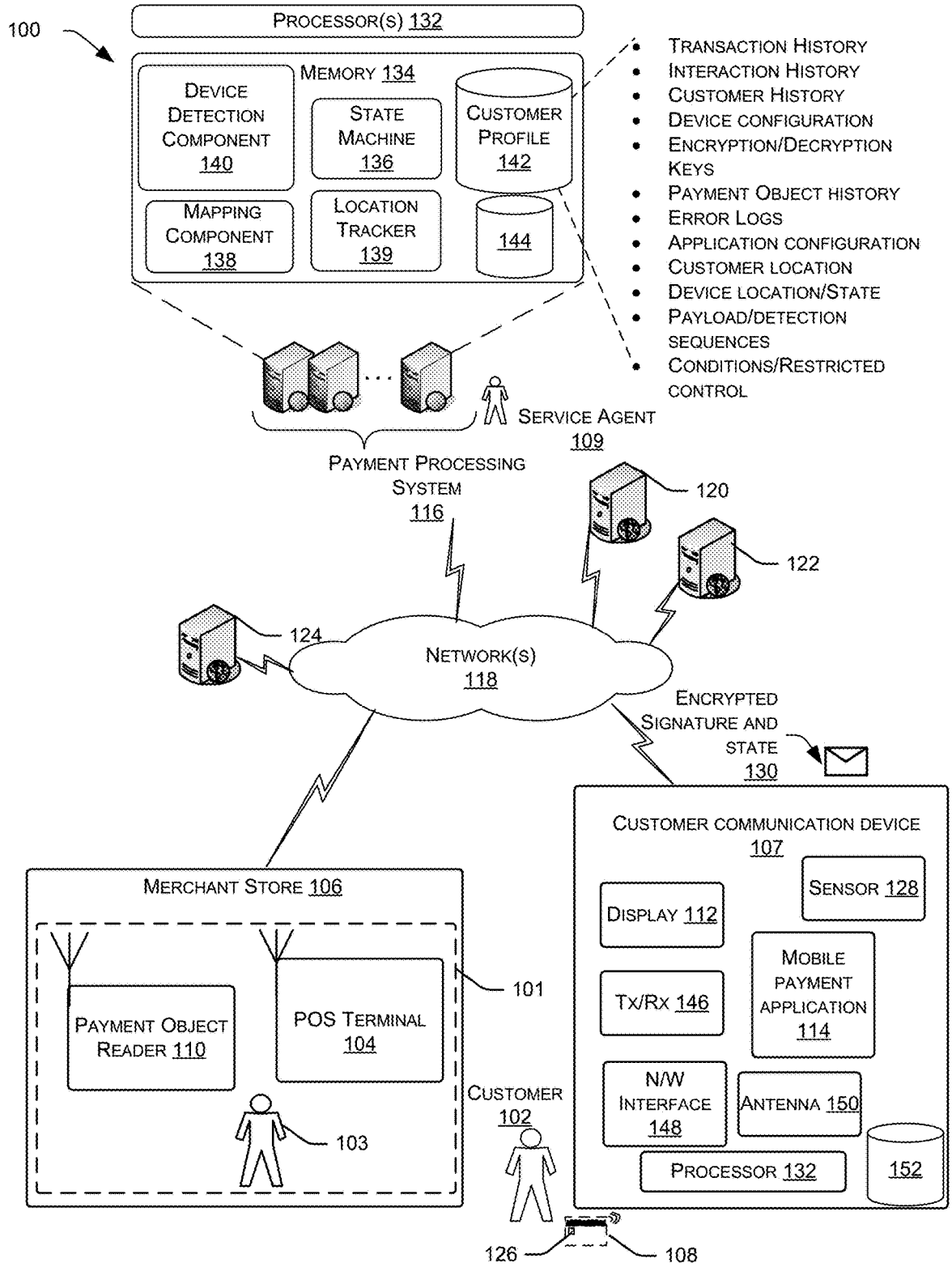
100
PROCESSOR(S) 132
MEMORY 134
DEVICE DETECTION COMPONENT 140
STATE MACHINE 136
CUSTOMER PROFILE 142
MAPPING COMPONENT 138
LOCATION TRACKER 139
144
TRANSACTION HISTORY
INTERACTION HISTORY
CUSTOMER HISTORY
DEVICE CONFIGURATION
ENCRYPTION/DECRYPTION KEYS
PAYMENT OBJECT HISTORY
ERROR LOGS
APPLICATION CONFIGURATION
CUSTOMER LOCATION
DEVICE LOCATION/STATE
PAYLOAD/DETECTION SEQUENCES
CONDITIONS/RESTRICTED CONTROL
SERVICE AGENT 109
PAYMENT PROCESSING SYSTEM 116
120
122
124
NETWORK(S) 118
ENCRYPTED SIGNATURE AND STATE 130
CUSTOMER COMMUNICATION DEVICE 107
SENSOR 128
DISPLAY 112
MOBILE PAYMENT APPLICATION 114
TX/RX 146
N/W INTERFACE 148
ANTENNA 150
PROCESSOR 132
152
MERCHANT STORE 106
PAYMENT OBJECT READER 110
POS TERMINAL 104
101
103
CUSTOMER 102
126
108

FIGURE 2

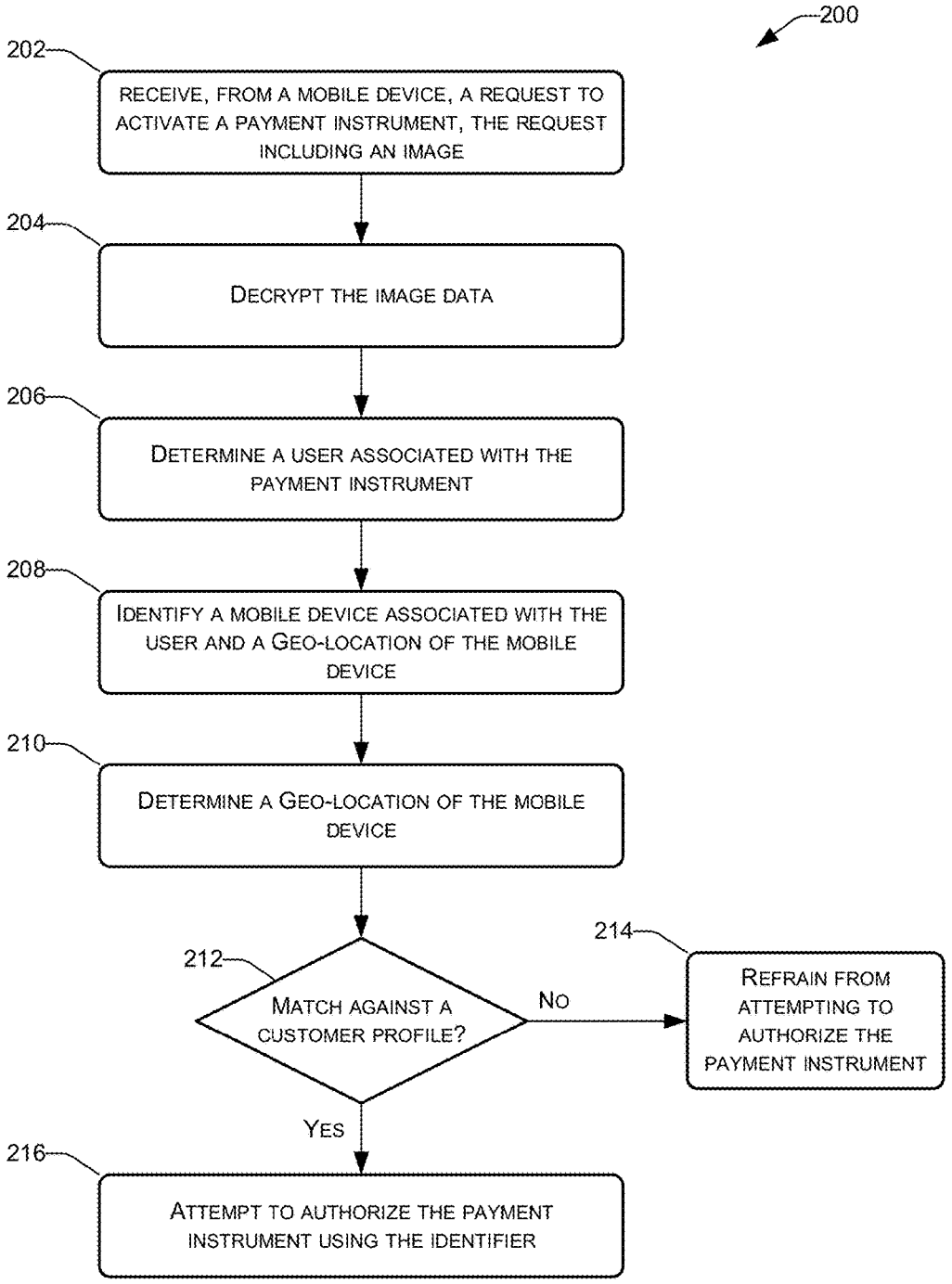
200
202
RECEIVE, FROM A MOBILE DEVICE, A REQUEST TO ACTIVATE A PAYMENT INSTRUMENT, THE REQUEST INCLUDING AN IMAGE
204
DECRYPT THE IMAGE DATA
206
DETERMINE A USER ASSOCIATED WITH THE PAYMENT INSTRUMENT
208
IDENTIFY A MOBILE DEVICE ASSOCIATED WITH THE USER AND A GEO-LOCATION OF THE MOBILE DEVICE
210
DETERMINE A GEO-LOCATION OF THE MOBILE DEVICE
212
MATCH AGAINST A CUSTOMER PROFILE?
NO
214
REFRAIN FROM ATTEMPTING TO AUTHORIZE THE PAYMENT INSTRUMENT
YES
216
ATTEMPT TO AUTHORIZE THE PAYMENT INSTRUMENT USING THE IDENTIFIER

FIGURE 3

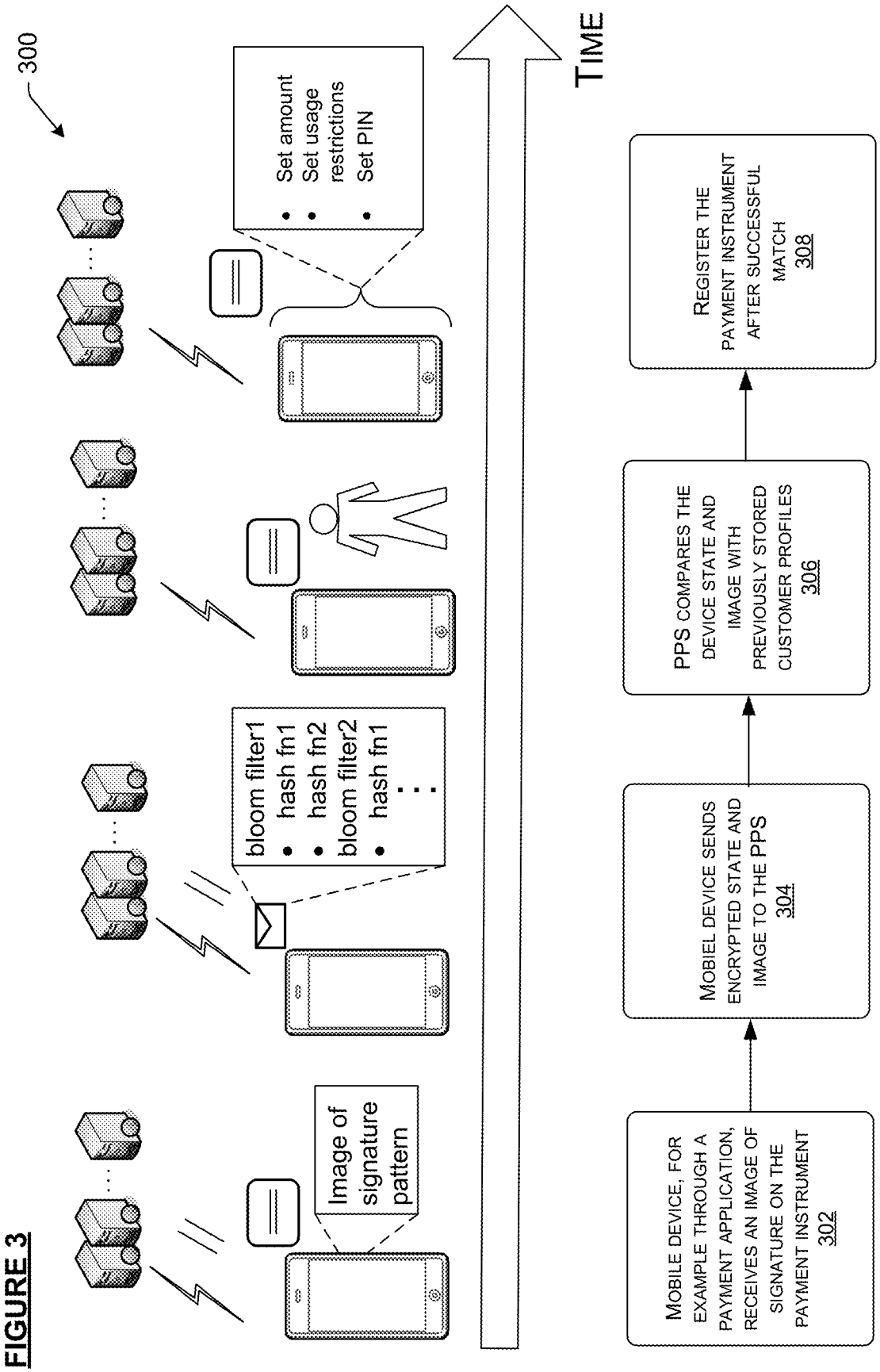
300
Image of signature pattern
bloom filter1
• hash fn1
• hash fn2
bloom filter2
• hash fn1
• . . .
Set amount
Set usage restrictions
Set PIN
TIME
MOBIEL DEVICE, FOR EXAMPLE THROUGH A PAYMENT APPLICATION, RECEIVES AN IMAGE OF SIGNATURE ON THE PAYMENT INSTRUMENT 302
MOBIEL DEVICE SENDS ENCRYPTED STATE AND IMAGE TO THE PPS 304
PPS COMPARES THE DEVICE STATE AND IMAGE WITH PREVIOUSLY STORED CUSTOMER PROFILES 306
REGISTER THE PAYMENT INSTRUMENT AFTER SUCCESSFUL MATCH 308

FIGURE 4

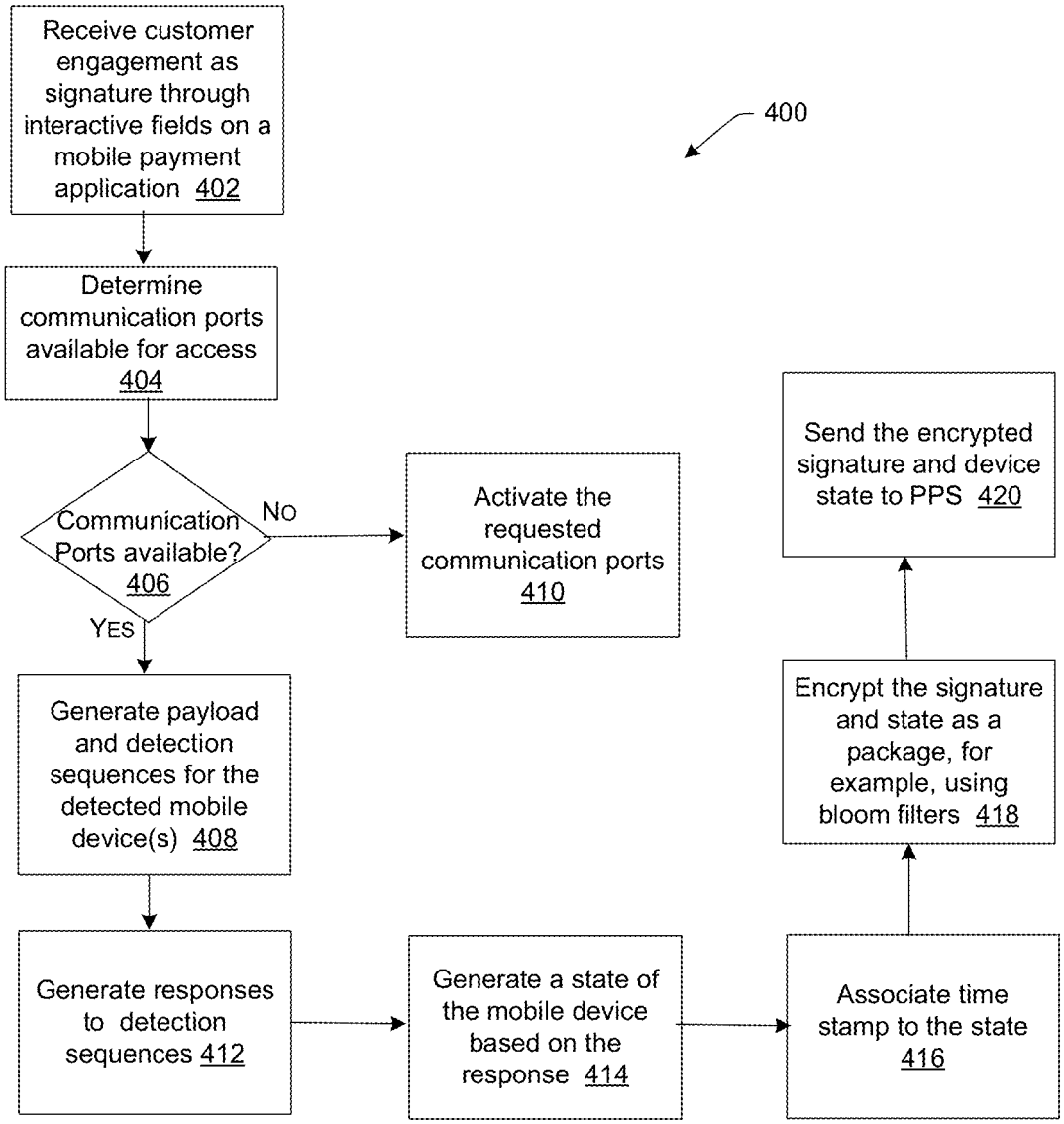
400
Receive customer engagement as signature through interactive fields on a mobile payment application 402
Determine communication ports available for access 404
Communication Ports available? 406
No
Activate the requested communication ports 410
Yes
Generate payload and detection sequences for the detected mobile device(s) 408
Generate responses to detection sequences 412
Generate a state of the mobile device based on the response 414
Associate time stamp to the state 416
Encrypt the signature and state as a package, for example, using bloom filters 418
Send the encrypted signature and device state to PPS 420

FIGURE 5

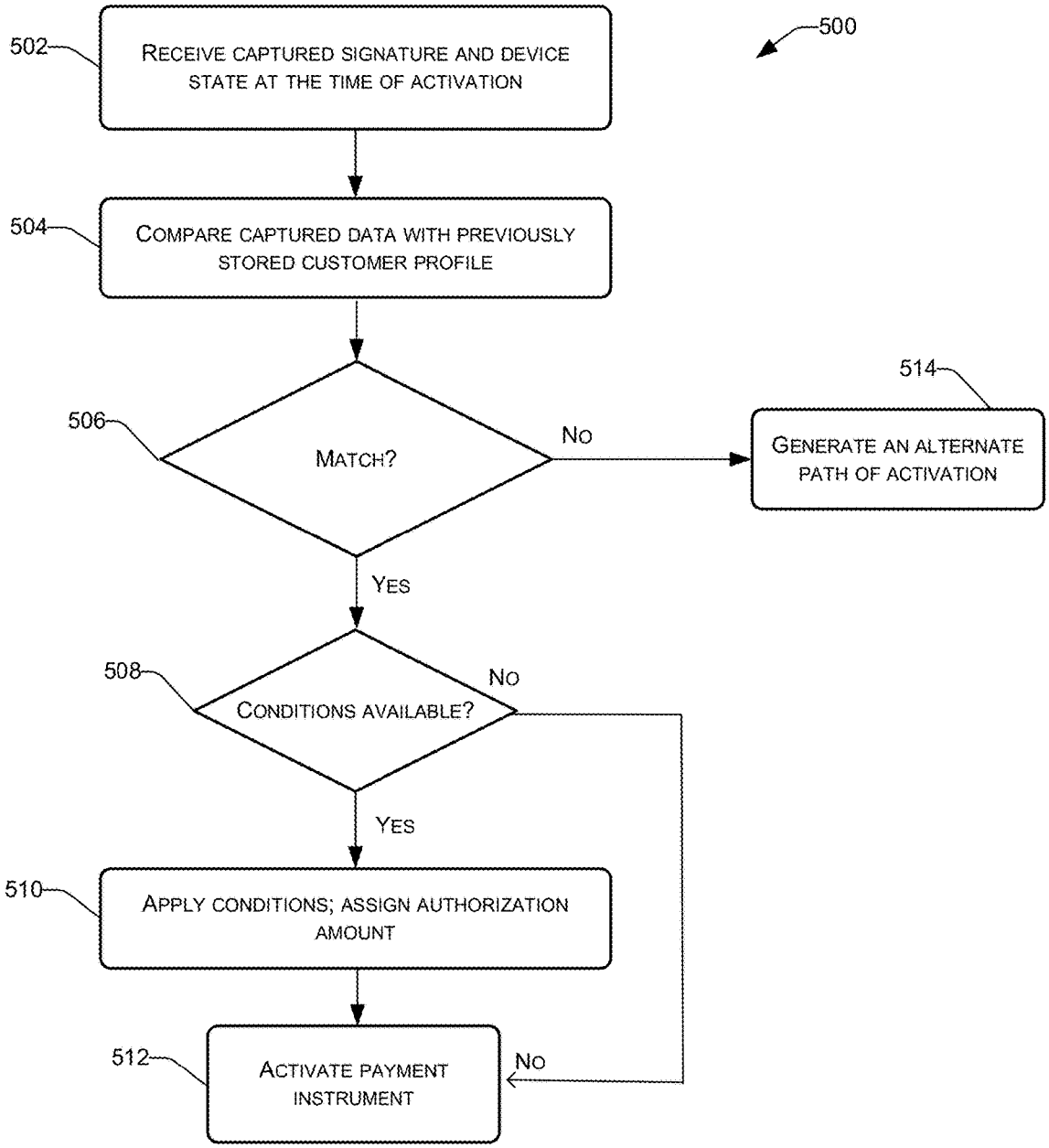
500
502
RECEIVE CAPTURED SIGNATURE AND DEVICE STATE AT THE TIME OF ACTIVATION
504
COMPARE CAPTURED DATA WITH PREVIOUSLY STORED CUSTOMER PROFILE
506
MATCH?
NO
514
GENERATE AN ALTERNATE PATH OF ACTIVATION
YES
508
CONDITIONS AVAILABLE?
NO
YES
510
APPLY CONDITIONS; ASSIGN AUTHORIZATION AMOUNT
512
ACTIVATE PAYMENT INSTRUMENT
NO

FIGURE 6

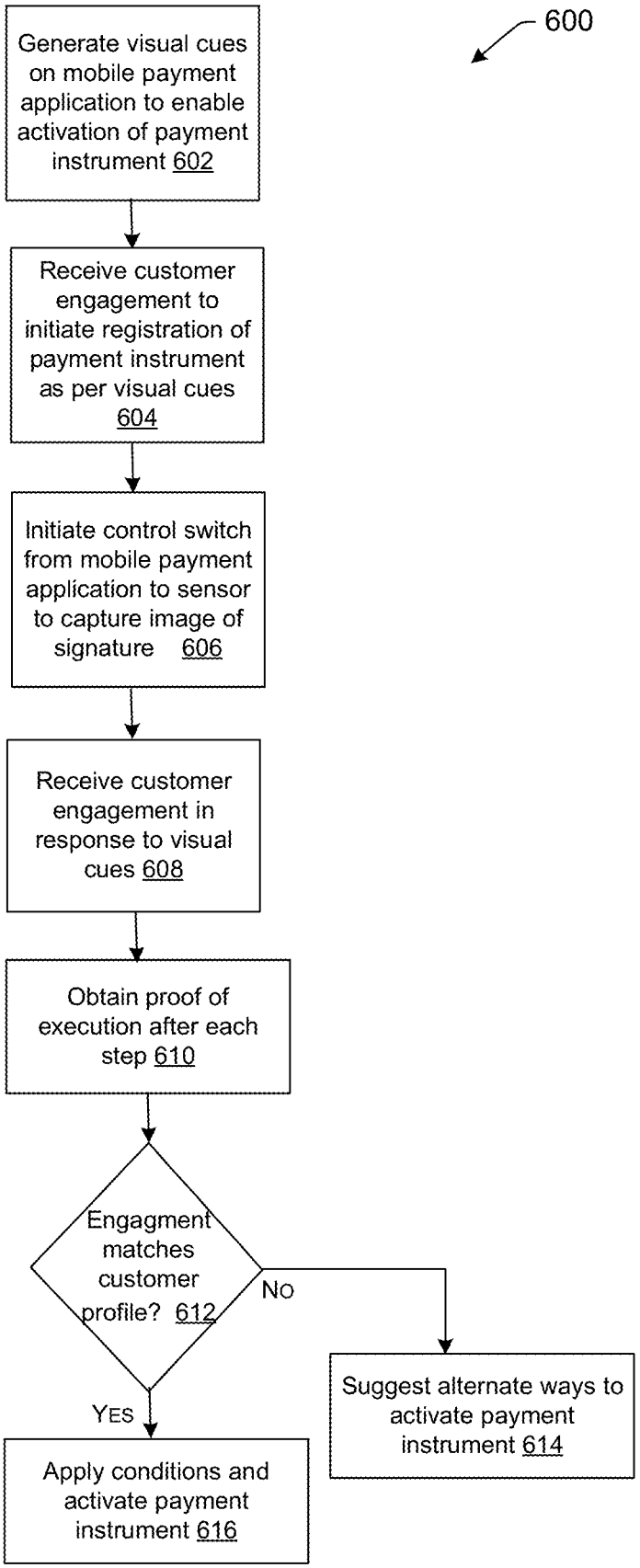
600
Generate visual cues on mobile payment application to enable activation of payment instrument 602
Receive customer engagement to initiate registration of payment instrument as per visual cues 604
Initiate control switch from mobile payment application to sensor to capture image of signature 606
Receive customer engagement in response to visual cues 608
Obtain proof of execution after each step 610
Engagment matches customer profile? 612
No
Suggest alternate ways to activate payment instrument 614
Yes
Apply conditions and activate payment instrument 616

FIGURE 7A

FIGURE 7B

FIGURE 8

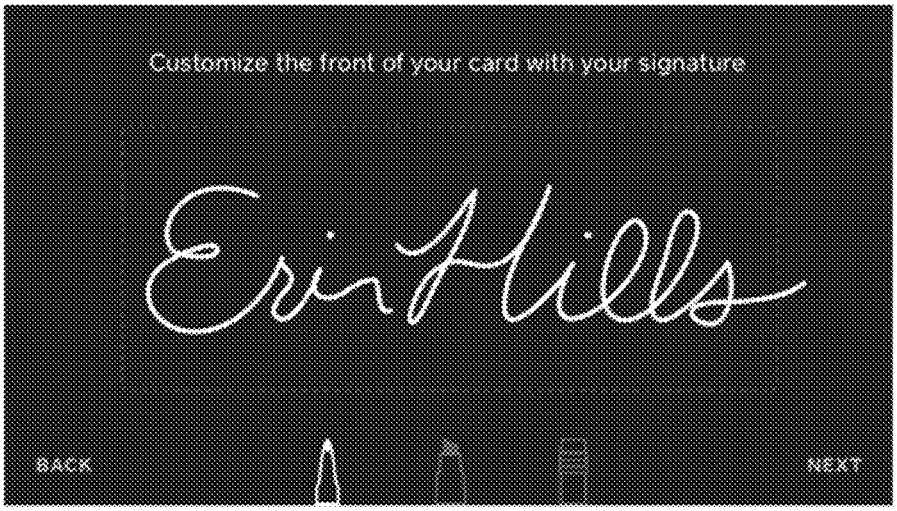
Customize the front of your card with your signature
Erin Hills
BACK
NEXT

FIGURE 9A

FIGURE 9B

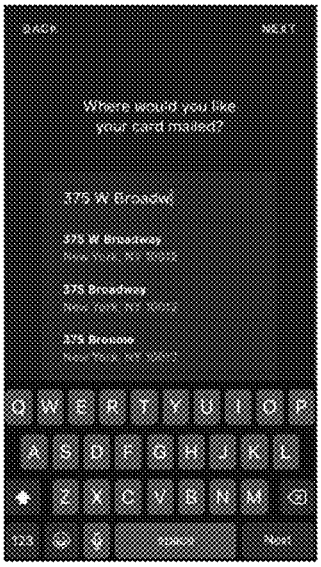

FIGURE 9C

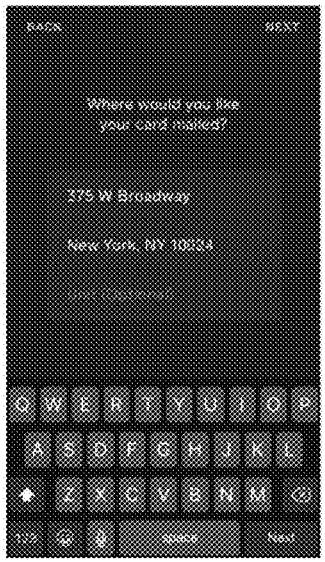

FIGURE 10B

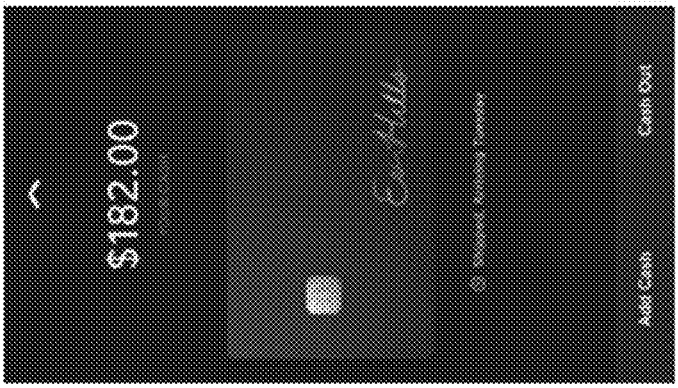

FIGURE 10A

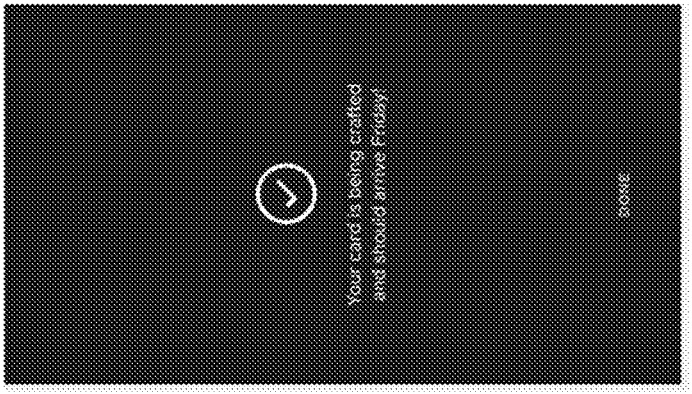

FIGURE 11A

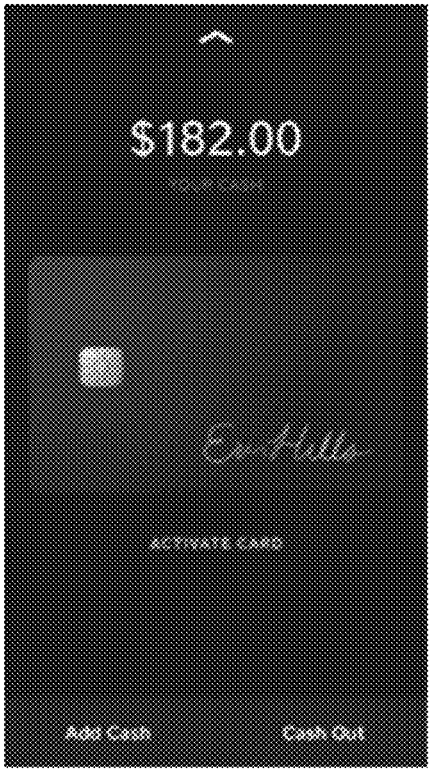

FIGURE 11B

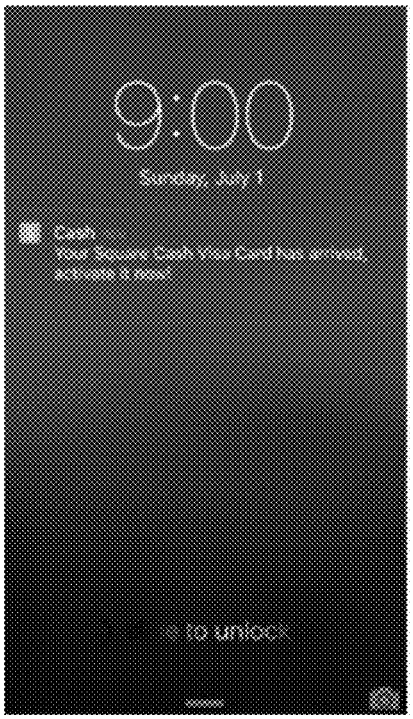

FIGURE 12

FIGURE 12A

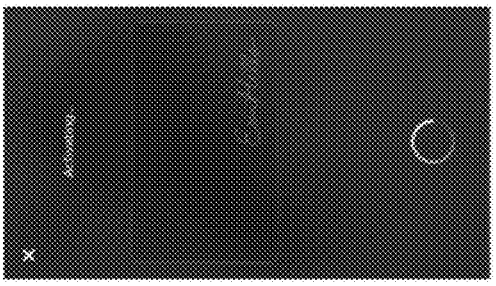

FIGURE 12C

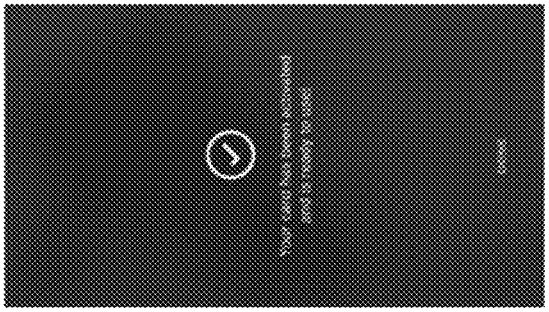

FIGURE 12E

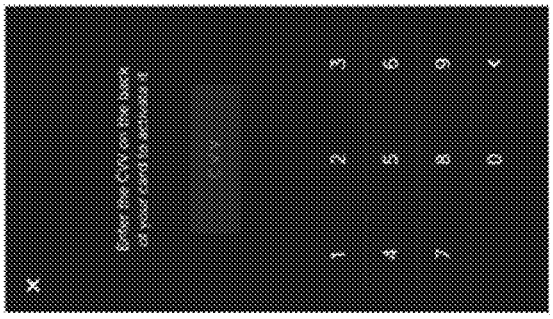

FIGURE 12B

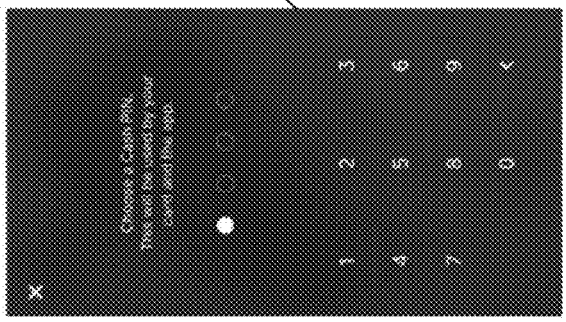

FIGURE 12D

PAYMENT APPLICATION INITIATED GENERATION OF PAYMENT INSTRUMENTS

PRIORITY

[0001] This application is a continuation of U.S. patent application Ser. No. 17/065,240 which was filed on Oct. 7, 2020, which is a continuation of U.S. patent application Ser. No. 16/925,209 which was filed on Jul. 9, 2020, which is a continuation of U.S. patent application Ser. No. 15/721,212 which was filed on Sep. 29, 2017, which is a continuation of U.S. patent application Ser. No. 15/282,759 which was filed on Sep. 30, 2016 and which granted on Aug. 18, 2020 as U.S. Pat. No. 10,748,130, and are incorporated by reference herein in their entirety.

TECHNICAL FIELD

[0002] Payment instruments are used in a wide variety of transactions. Examples of such payment instruments include credit cards, stored value cards, debit cards, loyalty cards, library cards, membership cards, and the like. The information displayed on a credit card is typically controlled by the bank issuing the card and displays information, such as the account number, a three or four digit authentication code, validity of the card, name of issuing bank, name of the interbank network, and the like. The payment instruments also include a hologram having embedded within security features and an integrated circuit to support Europay-Mastercard-Visa (EMV) payment functionalities. Despite the aforementioned options, the choices for what is to appear on a presentation are limited. When a new payment instrument is issued to a customer, that customer is told (usually via a sticker on the card) to activate the payment instrument by calling a phone number or by visiting a website where the customer registers the payment instrument by providing personally identifiable information.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] The detailed description is set forth with reference to the accompanying figures. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The use of the same reference numbers in different figures indicates similar or identical items or features. Moreover, multiple instances of the same part are designated by a common prefix separated from the instance number by a dash. The drawings are not to scale.

[0004] FIG. **1** is a block diagram illustrating an example environment for establishing a communication channel between a payment entity, e.g., a point-of-sale (POS) terminal, and a payment object reader, with a payment processing system to facilitate scheduling communication between the two for diagnosis and resolution of a technical failure, according to an embodiment of the present subject matter.

[0005] FIG. **2** illustrates a flow diagram of a method for activating a payment instrument by capturing an image of the payment instrument., according to an embodiment of the present subject matter.

[0006] FIG. **3** is a timing diagram that illustrates the timing of various steps of activation of instrument between the mobile device and the payment service, according to an example embodiment of the present subject matter.

[0007] FIG. **4** is a dataflow that illustrates the method of detecting mobile devices, and their states to use towards activating a payment instrument, according to an example embodiment of the present subject matter.

[0008] FIG. **5** depicts a sequence flow method that illustrates the method of activating a payment instrument and applying conditions, according to an example embodiment of the present subject matter.

[0009] FIG. **6** is a dataflow that illustrates the sensor-based method of activating a payment instrument, according to an example embodiment of the present subject matter.

[0010] FIGS. **7**A and **7**B illustrate example user interfaces to indicate that a payment instrument is available for physical delivery to a customer, according to an example embodiment of the present subject matter.

[0011] FIG. **8** illustrates a user interface to receive a custom signature from a customer, according to an example embodiment of the present subject matter.

[0012] FIGS. **9**A-C illustrate example user interfaces, being presented on a computing device, to receive customer engagement for the field of address where the payment instrument is to be delivered, according to an example embodiment of the present subject matter.

[0013] FIGS. **10**A and **10**B illustrate example user interfaces, being presented on the computing device, to indicate verification and information related to shipping of the physical instrument, according to an example embodiment of the present subject matter.

[0014] FIGS. **11**A and **11**B illustrate example user interfaces being presented on the computing device to notify the customer to initiate registration or activation of the payment instrument, according to an example embodiment of the present subject matter.

[0015] FIGS. **12**A-E illustrate example user interfaces, being presented on the computing device, for activating a payment instrument by using a registration feature of the payment instrument, according to an example embodiment of the present subject matter.

DETAILED DESCRIPTION

[0016] Embodiments for customizing and activating a payment object are described herein. The payment object can be customized with a signature, such as an image, pattern, alphanumeric text, or other such unique identifier that is embedded, printed or otherwise associated with the payment object. Furthermore, the signature can include not just the signature per se, but also the placement of the signature, for example with respect to the chip on the payment object and payment object number, etc. The payment object or payment instrument can be associated with a user of: a payment device (such as a point-of-sale terminal, a payment object reader, or a mobile communication device executing a payment application); or the payment application (such as an application for electronic money transfer, an application for managing inventory of items at an online storefront, an application for employee and customer management, a mobile register software application running on a mobile communication device to enable check out of purchases, and the like). The point-of-sale (POS) terminal, reader, and the payment applications allow merchant locations to accept payments for a product or a service; process the payment transaction for which the payment is made, e.g.,

by connecting to banks; and facilitate transfer of funds between accounts of payer and payee to furnish the payment transaction.

[0017] The payment instrument can be designed according to a specification corresponding to, for example, a debit card, a credit card, a smart-card (conforming to a payment instrument technical standard, such as a Europay-MasterCard-Visa ("EMV") standard), a radio frequency identification tag (i.e., near field communication enabled object), a biometric payment instrument, a virtual payment card stored on a device such as a smart phone and transmittable, for example, via near field communication (NFC), and can include personally identifiable information (PII), such as customer name, account number, and the like. The payment object can also have embedded within, or displayed on a surface, a unique pattern corresponding to or provided by the customer. The unique pattern, for example, can be a Quick Response (QR) code, a photograph, a three-dimensional image, an alphanumeric code, a text, or any other pattern.

[0018] Generally, a financial entity initiates a request for a payment instrument to be physically delivered to a user or customer. Usually, this request has to be made at a physical location of the financial entity when the user signs up for an account. When the user receives the payment instrument, the user follows set of instructions to activate the payment instrument. In the context of payment instruments, the word "activate" can mean: (a) confirming that the user in possession of the payment instrument is the intended user; (b) confirming that the payment instrument has been securely received by the intended user; (c) registering the payment instrument with the financial entity so that the intended user can use the payment instrument towards financial transactions; (d) associating the payment instrument with the identity of the user through a registration process; (e) enabling security measures and providing financial protection to the user from the time the payment instrument is activated; and/or (**0** agreeing to the terms and conditions of the financial entity or any other entity issuing the payment instrument.

[0019] Traditionally, the user activates the card either by registering the payment instrument on a web application or by calling a support number. When the user activates through such mechanisms, the user provides the account number listed on the card or personally identifiable information for verification. While registering the payment instrument, the user may encounter technical issues or errors for which the user has to reach out to a service agent. The traditional means of entering the card number or other personal information adds friction to the process of registering and is not customized according to the user.

[0020] To this end, in one implementation, the user or customer associated with a financial account at a financial entity selects or provides a signature, for example a signature that is unique to the customer during the account set-up. The payment processing system that receives the customized signature converts and/or encrypts the signature into a pattern, which is capable of being imprinted, embedded or otherwise associated with the payment instrument. Once the payment instrument is delivered to the user, the user initiates a process to activate the payment instrument. For this, a mobile device, for example customer's phone and optionally, registered with the payment processing system, executes a self-guiding tool or provides a customized flow to walk the customer through the steps of registering the payment instrument. The customer can select or provide information in response to queries that are tailored to the user. For example, one of the steps can direct the customer to take an image or a portion of the image of the pattern on the payment instrument through a sensor, such as a camera, of the mobile device. The mobile device, an application executing thereon, or the payment processing system that receives the image, then decrypts and compares the image with signatures stored at the time of registration. If a stored signature matches the captured image, the payment processing system authorizes the payment instrument to be used for purchases up to a predetermined amount or an amount requested by the customer. The predetermined amount can be determined based on the credit or debit worthiness and risk ratings associated with the customer. However, if the captured image does not match a stored signature, the payment instrument is not activated, as there is an increased likelihood that the authorization attempt is fraudulent.

[0021] Since the pattern is unique to the customer, conventional cookie-cutter flows to register payment instrument are often inaccurate and cannot best validate the user's identity. Therefore, a customized flow, as disclosed herein, generates ways to add or remove validation steps based on the user profile, such as geographical location, personalization, etc. Additionally, the signature feature automates the registration process by reducing friction associated with the user having to call an agent or having to visit a website to register the payment instrument. The registration process disclosed herein is more secure by virtue of its reliance on a customized feature. While some traditional payment instruments allow for customized features, such as image of the user or name, to be displayed on the card. it will be understood that such customizations are static in the sense that the customized features cannot be used to trigger other process flows, specifically trigger auto-registration of a payment instrument as disclosed herein. Accordingly, examples described herein provide specific technical improvements over conventional methods with streamlined automation and enhanced security functionality in registering a payment instrument.

[0022] For at least the processes described above, the payment processing system also facilitates generation and display of notifications, alerts, and selectable fields for the customer on a graphical user interface associated with their communication devices. For example, the user's communication device can include within the mobile application an option to request support by establishing connection with a service agent, for example by tapping a software or hardware button on the device or within the mobile application. In another example, the selectable icon generates an interface for the customer to provide a signature. On interaction with the selectable icon, the payment processing system (hereinafter referred to as PPS) also obtains primary or secondary contextual information from the environment of the customer. The contextual information includes:

[0023] the device information, including the type of device on which the signature is provided or the payment application is running, the hardware and software settings, the communication ports open for communication like Bluetooth, Wi-Fi, the device configuration, and so on;

[0024] the software application information, including the version of application, software application con-

figuration, other applications executing on the device; any indication of virus or malware, software settings, and so on;

[0025] the customer's information, including their phone number (which is associated with their account), any other devices associated with the user, the customer's PAN, customer's transaction history over a period of time, trends in transaction history, location, geographical location of stores, history of software downloads, and so on;

[0026] contextual information about the customer's interaction with the application, e.g. what version of the application is running, what screen is being viewed, which area of the screen is contacted as the signature is provided;

[0027] the customer's selection of call options, e.g. use an alternate phone number, call back in a certain time window offered by the server, or other such contact preferences.

[0028] The graphical user interface can also present push notifications or messages to the user; "system is ready to accept your signature. Do you want a select an image as a signature or provide your own?" with attached actions (e.g., "Yes, provide me options" to show pre-selection options for the user to select, or "Provide my own" for providing a custom signature which can be an image or text or a combination of both, and so on.

[0029] The present subject matter proposes the integration of at least the aforementioned features into a seamless and convenient mechanism for registration of a payment instrument. With relation to the problems identified previously with conventional systems and methods, the software application itself becomes an active and cooperative component of the registration process, rather than the subject of it. The description hereinafter describes the devices and applications to be related to payment technology. However, it will be understood, that the technology can be extended to any device and application that would otherwise require another entity like a service agent to help with registration of an object or product. For example, the process can easily be extended to registration and/or set-up of an electronic product, like a speaker, smart television or headphones.

[0030] In one implementation, payment object readers and/or POS terminals, mobile payment applications, hereinafter referred to as payment devices or payment entities, which implement the present techniques, include a state machine to detect state of payment device and payment application, in terms of power signal values, device or application characteristics, hardware and software configuration, and the like, and transfer such states to a PPS. In another implementation, the PPS includes the state machine to query the payment devices at various time instants, or in response to user engagement, for example with a "registration" icon. This meta-data can be saved and appended into the signature at the time of pattern creation. Later on, at the time of registration, the pattern based off the signature and the meta-data is compared with the meta-data collected from the mobile application and the mobile device. The meta-data helps provide another layer of security. In some implementations, transmitted instead of received power levels are used. In yet another implementations, other forms of signal measurements or identifiers, for example, in other frequency bands, to identify a mobile device and application for registration purposes.

[0031] The customized and automated registration technology can also be configured to operate irrespective of the kind of payment object reader, POS terminal, web applications, mobile applications, POS topologies, payment cards, computer networks, and environments. The customized and automated registration technology described herein can be configured to operate in both real-time/online and offline modes. Furthermore, even though Bluetooth or Bluetooth Low Energy has been used to describe certain embodiments, other wired or wireless protocols, such as NFC, Wi-Fi, etc., can be used with little or no modifications.

[0032] The implementations herein provide a system and method to generate a payment instrument through a mobile payment application, which in one implementation, is associated to the entity that holds the card holder's funds, whereas in another implementation, the payment application may be associated to several financial entities, which are holding separate funds for the customer. Typically, the process of ordering a physical payment instrument involves paperwork or a visit to a website, however, as described herein the payment instrument can be ordered through the payment application in a frictionless and easy manner. Furthermore, the payment instrument can be customized, for example with a unique signature, using customer's mobile device as opposed to a banking system. The signature can be printed or otherwise attached to the card, for example after confirming that the signature conforms to a set of rules. The application of rules may vary from one customer to another. For example, customers holding a higher amount of funds in their account may have a specific set of rules in comparison to customers having a greater number of miles or usage rate. The payment processor for transactions made through the payment instrument is privy to nature of such transactions and accordingly, can create rules specific to each of the customers. The technology field described herein improves the generation of payment instrument instantiation.

[0033] The following description provides specific details for a thorough understanding and enabling description of these embodiments. One skilled in the relevant art will understand, however, that the embodiments discussed herein may be practiced without many of these details. Likewise, one skilled in the relevant art will also understand that the embodiments can include many other features not described in detail herein. Additionally, some well-known structures or functions may not be shown or described in detail below, so as to avoid unnecessarily obscuring the relevant description. Some of the recurring terms are now defined.

[0034] The terms "connected" or "coupled" and related terms used throughout the description are used in an operational sense and are not necessarily limited to a direct physical connection or coupling. Thus, for example, two devices may be coupled directly, or via one or more intermediary media or devices. As another example, devices may be coupled in such a way that information can be passed there-between, while not sharing any physical connection with one another. Based on the disclosure provided herein, one of ordinary skill in the art will appreciate a variety of ways in which connection or coupling exists in accordance with the aforementioned definition.

[0035] The phrases "in some embodiments," "according to some embodiments," "in the embodiments shown," "in other embodiments," and the like generally mean the particular feature, structure, or characteristic following the phrase is included in at least one implementation of the disclosed

technology, and may be included in more than one implementation. In addition, such phrases do not necessarily refer to the same embodiments or different embodiments.

[0036] The term "component" or "engine" refers broadly to general or specific-purpose hardware, software, or firmware (or any combination thereof) components. Components and engines are typically functional components that can generate useful data or other output using specified input(s). A component or engine may or may not be self-contained. Depending upon implementation-specific or other considerations, the components or engines may be centralized or functionally distributed. An application program (also called an "application") may include one or more components and/or engines, or a component and/or engine can include one or more application programs.

[0037] The term "cause" and variations thereof, as used throughout this description, refers to either direct causation or indirect causation. For example, a computer system can "cause" an action by sending a message to a second computer system that commands, requests or prompts the second computer system to perform the action. Any number of intermediary devices may examine and/or relay the message during this process. In this regard, a device can "cause" an action even though it may not be known to the device whether the action will ultimately be executed or completed.

[0038] The term "substantially" or "approximately", as used herein, means approximately or actually equal (e.g., within ten percent of equal).

[0039] The term "communication network" may be any type of network known in the art, such as a local area network or a wide area network, such as the Internet, and may include a wireless network, such as a cellular network, a cloud network, a local wireless network, such as Wi-Fi and/or close-range wireless communications, such as Bluetooth and Bluetooth low energy, near field communications (NFC), a wired network, or any other such network, or any combination thereof. Accordingly, the network may include both wired and/or wireless communication technologies, including Bluetooth, Bluetooth low energy, Wi-Fi and cellular communication technologies like worldwide interoperability for microwave access (Wi-MAX), 3G, 4G, CDMA, digital subscriber line (DSL), etc., cloud computing technologies, as well as wired or fiber optic technologies. Additionally or alternatively, the communication network may be a mesh network. For example, in a wireless local area network (WLAN), network devices may be configured to receive and forward communications, which are ultimately destined for a different device. These types of networks are generically referred to as "mesh" networks, where network nodes may form a "mesh" of paths for which communications may travel to reach their destination. Wireless networks may use beacon transmissions to advertise the network's existence, as well as provide information about the network and capabilities associated with the network. Different kinds of beaconing mechanisms may be used, for example, one for infrastructure mode networks (also called basic service set (BSS) networks) and one for ad-hoc mode networks (also called independent basic service set (IBSS) networks). In infrastructure networks, access points (APs) are the entities responsible for generating beacons whereas in ad hoc networks, all network nodes (including user stations) participate in the generation of beacons. The ad hoc network beacons (referred to as IBSS beacons) are used to advertise the network (which consists of all the nodes) as a whole while the infrastructure network beacons (referred to as BSS beacons) are generated by an AP and meant to advertise the existence of only that individual AP. Components used for such communications can depend at least in part upon the type of network, the environment selected, or both. Protocols for communicating over such networks are well known and are not discussed herein in detail.

[0040] As used herein, the term "signature" is a unique identifier that can either be provided by a customer by keying in their preferred signature on a user interface, such as touch screen or keypad or by selecting from amongst a list of options generated by a server. In another example, the server can automatically and/or randomly assign a signature to the customer at the time of account creation. The signature can be an actual signature, alphanumeric text, a unique pattern of shapes, an image, a barcode, Quick Response (QR) codes, or a radio frequency identifier (RFID) tag. The signature is referenced as being associated or printed on the payment card, however, the signature can be provided with the payment card, for example in an accompanying letter. The signature can also be embedded, such that it is hidden to naked eye. The signature once encrypted and printed or associated to the payment card can be mentioned as pattern in the specification. The signature can also be an analog of digital file that comprises a picture or a drawing that is in a JPEG or other file format.

[0041] A variety of materials can be used to craft the payment instruments. For example, the payment instruments may be crafted stock materials, such as plastics, paper, laminates, and the like. According to the stock material used to construct the payment instrument, a number of techniques can be used to associate the signature with the payment instrument. For instance, the signature may be printed on the stock material (such as by using a laser or ink jet printer). Other examples include silk screening, use of stickers or labels, embossing, painting and the like. In some cases, the stock material may have some information already included, such as the a company logo, legal notices, and the like, or this information may be placed onto the stock material at the time the signature information is placed onto the stock material.

[0042] In addition to providing the signature on the presentation instrument, some or all of the signature may be placed in portions, for example a first portion on one side and the second portion on the other side of the payment instrument. The activation then involves reading the image in two parts and in a specific order. The signature can also be printed onto other materials as well. For example, the signature may be provided on any inserts mailed with the payment instrument, the envelope or mailer, and the like.

[0043] A wide variety of techniques may be used to deliver the payment instruments to recipients after they have been created. For example, they could be attached to a card carrier and placed into a mailer along with any other inserts. This may then be mailed to the recipient. Other techniques include personal delivery, by a courier services, by in-store pick-up and the like. The payment instruments may also be produced at the purchase location.

[0044] As described herein, the payment instrument may be in an inactive state until activated by the recipient. In this way, if the payment instrument is intercepted or stolen before reaching the recipient, it may not be used. One way to activate the presentation instrument is to require certain information to be supplied by the recipient. This information

may be input by the purchaser and then transmitted to the recipient, such as by e-mail, by a phone call, by a separate mailing, or the like. Instead of expecting the recipient to provide his or her phone number to activate the account and then calling, the payment instrument described herein includes the signature having activation capabilities. The signature triggers the activation process without the customer having to reach out to a customer representative. As such, the process of activation is not just automated but also initiated by a feature on the payment instrument that is otherwise inactive and merely ornamental and design related.

[0045] As used here, the term "pairing" or "associating" refers to a process in which the POS terminal and the payment object reader establish a communication channel with each other using wireless communication protocols, for example, Bluetooth®, Bluetooth Low Energy®, Wi-Fi®, etc. The POS terminal and the payment object reader each includes a transceiver capable of transmitting data between them once "paired."

[0046] As used herein, RSSI, or "Received Signal Strength Indicator", is a measurement of how well the payment device can hear a signal from an access point or router, such as Wi-Fi card of the payment object reader. RSSI is a term used to measure the relative quality of a received signal to the POS terminal, but has no absolute value.

[0047] Additionally, as used herein, the term "payment card," "payment object," or "payment instrument" refers to a payment mechanism that includes a debit card, a credit card, a prepaid gift card, or the like, a smartcard that has an embedded integrated circuit chip (e.g., Europay-MasterCard-Visa (EMV) card), a proxy card, or any card that functions as a combination of any of these mechanisms. The term "proxy object" as used herein refers to a card that may or may not bear a card number/account number that appears to be that of a real credit or debit card account (i.e., it is in the correct format), but where that card/account number is actually only a proxy for the customer's real card/account number. Another type of payment object is a biometrically identifiable instrument, which may be initialized using a person's finger (e.g., for fingerprint recognition), face, iris or retina, heartbeat, etc.

[0048] Alternatively, the payment object can be a software instrument or virtual instrument, such as a virtual wallet configured to initiate contactless payment transactions, e.g., a key fob, a mobile device having an RFID tag, etc. Other examples of payment object may also include a prepaid card, a gift card, a rewards card, a loyalty points card, a frequent flyer miles card, checks, cash, or in general, any kind of financial instrument that holds financial value or provides a promise to pay at a later time. Thus, a payment object transaction (also referred to as payment card transaction) may be any be a transaction where a merchant or a user swipes the user's credit card through a payment object reader in exchange for a product or service offered by the merchant.

[0049] The term "swipe" here refers to any manner of triggering a payment object reader to read data from a payment object, such as by dipping into, tapping, hovering, bringing in close contact or passing the payment object into or through a payment obj ect reader.

[0050] The term "broadcasting" refers to the modes of operation of the Bluetooth enabled device to enable connection with neighboring devices and can be either discoverable mode or advertising mode. Discoverable mode is a state within Bluetooth technology integrated devices that enables Bluetooth devices to search, connect and transfer data with each other. Discoverable mode is used to propagate the availability of a Bluetooth device and to establish a connection with another device. In some cases, the device can also be in the "non-discoverable" mode, which prevents devices from being listed during a Bluetooth device search process. However, a non-discoverable Bluetooth device is visible to devices that know its address or can discover its address.

[0051] The term "advertising" is meant to refer to another mode of operation of the Bluetooth enabled device. Both broadcasting and advertising help initiate, establish, and manage the connection with other devices. If the device just needs to communicate the status of a few parameters or alarms and does not absolutely require acknowledgement from other side, the BLE advertising mode may do the job with just a few commands sent to the BLE controller. When advertising mode is enabled, the BLE device will start to transmit special packets carrying advertising information as Payload Data Units (PDU) on the RF channels dedicated for this purpose. BLE is utilizing a common structure of over the air packets for advertising and data channels. An advertising channel PDU has a header and actual payload. The header contains information about the size of the payload and its type: advertising channels are used for exchanging information before making a connection between devices. Hence, different payload types are supported to broadcast information about the device's ability (on inability) to support a connection, to request more information or to respond with additional device information and to request the initiation of a data connection with another device.

[0052] Reference to an "embodiment" in this document does not limit the described elements to a single embodiment; all described elements may be combined in any embodiment in any number of ways. Furthermore, for the purposes of interpreting this specification, the use of "or" herein means "and/or" unless stated otherwise. The use of "a" or "an" herein means "one or more" unless stated otherwise. The use of "comprise," "comprises," "comprising," "include," "includes," and "including" are interchangeable and not intended to be limiting. Also, unless otherwise stated, the use of the terms such as "first," "second," "third," "upper," "lower," and the like do not denote any spatial, sequential, or hierarchical order or importance, but are used to distinguish one element from another. It is to be appreciated that the use of the terms "and/or" and "at least one of", for example, in the cases of "A and/or B" and "at least one of A and B", is intended to encompass the selection of the first listed option (A) only, or the selection of the second listed option (B) only, or the selection of both options (A and B). As a further example, in the cases of "A, B, and/or C" and "at least one of A, B, and C", such phrasing is intended to encompass the selection of the first listed option (A) only, or the selection of the second listed option (B) only, or the selection of the third listed option (C) only, or the selection of the first and the second listed options (A and B) only, or the selection of the first and third listed options (A and C) only, or the selection of the second and third listed options (B and C) only, or the selection of all three options (A and B and C). This may be

extended, as readily apparent by one of ordinary skill in this and related arts, for as many items listed.

[0053] It will also be appreciated by those skilled in the art that the words during, while, and when as used herein are not exact terms that mean an action takes place instantly upon an initiating action but that there may be some small but reasonable delay, such as a propagation delay, between the initial action and the reaction that is initiated by the initial action. As used in this specification and any claims of this application, the terms "computer", "server", "processor", and "memory" all refer to electronic or other technological devices. These terms exclude people or groups of people. For the purposes of the specification, the terms display or displaying means displaying on an electronic device. As used in this specification and any claims of this application, the terms "computer readable medium" and "computer readable media" are entirely restricted to non-transitory tangible, physical objects that store information in a form that is readable by a computer. These terms exclude any transitory wireless signals, wired download signals, and any other ephemeral signals. The computing system can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other. In some embodiments, a server transmits data (e.g., an HTML page) to a client device (e.g., for purposes of displaying data to and receiving user input from a user interacting with the client device). Data generated at the client device (e.g., a result of the user interaction) can be received from the client device at the server.

[0054] It should also be appreciated by those skilled in the art that any block diagrams, steps, or sub-processes herein represent conceptual views of illustrative systems embodying the principles of the present subject matter. Similarly, it will be appreciated that any flow charts, flow diagrams, state transition diagrams, pseudo code, and the like represent various processes which may be substantially represented in computer readable medium and so executed by a computer or processor, whether or not such computer or processor is explicitly shown. The order in which the methods are described are not intended to be construed as a limitation, and any number of the described method blocks can be deleted, moved, added, subdivided, combined, and/or modified in any order to implement the methods, or an alternative combination or sub-combinations. Also, while steps, sub-processes or blocks are at times shown as being performed in series, some steps, sub-processes or blocks can instead be performed in parallel, or can be performed at different times as will be recognized by a person of ordinary skill in the art. Further any specific numbers noted herein are only examples; alternative implementations can employ differing values or ranges. Furthermore, the methods can be implemented in any suitable hardware, software, firmware, or combination thereof.

[0055] While certain devices, e.g., the payment object readers and POS terminals are shown as including distinct components, this is merely for ease of illustration and not intended as limiting. In various implementations, the payment object readers and POS terminals may be identical, similar or distinct. Moreover, the components shown and described for the payment object readers and POS terminals may be implemented as more components or as fewer components and functions described for the components may be redistributed depending on the details of the implementation. Additionally, in some implementation, there may be several, hundreds, thousands, hundreds of thousands, or more, of the payment object readers and the POS terminals. Further, in some implementations, configuration, structure, and operational characteristics of the payment object readers and/or POS terminals may vary from device to device. In general, payment object readers and the POS terminals can each be any appropriate device operable to send and receive data, requests, messages, electronic messages, text messages, alerts, notifications, pop-up messages, push notifications, or other types of information over the one or more networks or directly to each other.

[0056] The registration or verification technology introduced here can be embodied as special-purpose hardware (e.g., circuitry), as programmable circuitry appropriately programmed with software and/or firmware, or as a combination of special-purpose and programmable circuitry. Hence, embodiments may include a machine-readable medium having stored thereon instructions that may be used to cause one or more processors to perform the methods, variations of the methods, and other operations described here. The machine-readable medium may include, but is not limited to, floppy diskettes, optical discs, compact disc read-only memories (CD-ROMs), magneto-optical discs, read-only memories (ROMs), random access memories (RAMs), erasable programmable read-only memories (EPROMs), electrically erasable programmable read-only memories (EEPROMs), application-specific integrated circuits (ASICs), magnetic or optical cards, flash memory, or other type of media/machine-readable medium suitable for storing electronic instructions. Various embodiments will now be described in further detail with the help of one or more figures.

[0057] Turning now to the Figures, FIG. **1** is a network environment **100** that illustrates a point-of-sale (POS) system(s) **101**, comprising of payment devices, such as a POS terminal **104** and a payment object reader **110**, which may be manned by a merchant at a merchant store **106**. The POS system **101** can communicate with another communication device, hereinafter referred to as a merchant communication device (not shown) or a customer communication device **107**, such as mobile phone or tablet of a customer **102**. For example, the customer **102** initiates communication with the POS system **101** to initiate payments, such as contactless payments, through registered communication devices, such as the customer communication devices **107**. For this, the customer **102** taps the mobile device **107** on a surface of the payment object reader **110**. In another example, the customer **102** can also initiate payments through payment instruments (also referred to as payment object), such as registered credit cards or debit cards authorized with a predefined amount. Besides payment related tasks, the customer **102** can also initiate communication with a service agent **109** of a payment processing system (PPS) **116** for technical support related to the activation of the payment instrument **108** or any of the applications on the customer communication device **107**. For example, the customer **102** contacts the service agent **109** to register a communication device **107** or a new and/or deactivated payment instrument **108** for payments. In another implementation, the customer **102** initiates communication to register a payment instrument **108** through a mobile payment application **114** execut-

ing on the customer communication device **107**, or by contacting the service agent **109** by phone, electronic mail or other means of communication. The payment instrument can be a card with magnetic stripe or smart chip or both and may work with EMV, magstripe, and other payment technologies.

[0058] The customer communication device **107** is communicatively coupled to the PPS **116**. Some of the advantages of this association are that data can be stored remotely on the PPS **116**, especially sensitive payment data. Furthermore, the remote server can provide scalability, failover management, centralized and automated backup services, and faster access to data.

[0059] The customer communication device **107** can be a mobile device or a desktop device. Mobile devices include smart phones, tablet computers, laptops, mobile wearable devices like Apple® watch or a Fitbit®, or other mobile data processing apparatus. Additionally or optionally, the customer communication device **107** may also include a sensor **128**, such as a camera, or antenna **150** or transmitter/receiver **146**, to receive and process environment characteristics, for example, location of the device, and the like. The device **107** then saves such environment characteristics either locally or sends to the payment processing system **116**, which then connects the data to a customer's identity or signature. The device **107** also has characteristics that can be tracked, detected and monitored either through another application on the device **107** or by engagement with a button, such as a start button and the like. The device characteristics include registration number associated with the device, the type of signals emitted by the device **107**, whether communication ports are enabled, whether Bluetooth is enabled, and so on. The customer communication device **107** also includes an image-capturing sensor **128**, such as a camera, or a scanner, to obtain a representation of a signature or other pattern printed on a payment instrument.

[0060] The customer communication device **107** also includes a network interface **148** to allow communication with other devices using a variety of communication protocols. For example, multiple network interfaces may be employed to allow for the communication over broadcast, multicast, and/or unicast networks. Through a communications network **118**, the customer communication device **107** is accessible through remote clients (e.g., computers with web browsers). Network interfaces **148**may employ connection protocols such as, but not limited to: direct connect, Ethernet (thick, thin, twisted pair 10/100/1000 Base T, and/or the like), Token Ring, wireless connection such as IEEE 802.11a-x, and/or the like. Should processing requirements dictate a greater amount speed and/or capacity, distributed network controllers (e.g., Distributed PPS architectures may similarly be employed to pool, load balance, and/or otherwise increase the communicative bandwidth required by the device **107**.

[0061] In some implementations, the network interfaces **148** may be communicatively coupled to hardware components, which facilitate detection of payment cards. For example, the network interfaces may couple to a payment card slot or rail designed to accept payment cards through swipe or insertion or any other action. In another example, the network interfaces may couple to one or more sensors included to detect or read the registration feature, such as the signature or any such pattern.

[0062] In various embodiments, the network interface **148** may also support wireless data transfers between the device **107** and external sources, such as clients and cameras, or the like. Wireless protocols may include Wi-Fi (e.g. IEEE 802.11a/b/g/n, WiMax), Bluetooth or Bluetooth low energy (BLE); infrared, and the like, through BLE interface, WiFi interface, QR interface, NFC interface, EMV interface, cellular technology interface, and other interface(s).

[0063] The customer communication device **107** may also comprise any sort of mobile or non-mobile device that includes an instance of a payment application **114** that executes on the respective device. In some instances, the payment application **114** can execute on a device separate from the customer communication device **107**, for example another customer communication device **107** associated with the customer **102**. The payment application **114** may provide POS functionality to the device **107** to enable the customer **102** (e.g., a buyer, an individual user, etc.) to accept and send payments after registering or otherwise associating assigned payment instruments (such as payment objects and/or communication devices **107**). The customer communication device **107** can include a display for displaying notifications, visual cues, and interactive fields to interact with the PPS **116**.

[0064] The interactive fields can also be accessible via the payment application **114** to allow the buyer to register a payment instrument. For example, the interactive fields, when selected or pressed or otherwise engaged, can generate a set of instructions for the customer **102** to follow to register the payment instrument **108**. For example, one of the instructions define the manner in which the customer **102** should obtain an image of at least a portion of the payment instrument **108**, say the portion where the custom signature is visible. In another example, the interactive fields or selectable icons when selected establish a communication channel between the customer **102** and a service agent **109**. The communication can be in the form of text, electronic mail, phone call, or any other kind of notification. The payment application **114**, too, has application characteristics or profiles associated thereto. The payment application characteristics and profiles, include for example, application version history, status of APIs or handlers executing on the application, error log, transaction log, and so on. The states of the payment application **114** can also be sent to the PPS **116** from time to time, and the instructions of how to collect state can be dictated by the state machine **136**. Analysis of states helps determine the unique profile of the customer **102**. While payment application characteristics and device characteristics are distinct from each other, most applications execute on devices. Therefore, for the purpose of this application, person skilled in the art can assume device characteristics or profiles and device states to include payment application characteristics or profiles. Also, the characteristics and profiles are assumed to be environment metadata, which is encrypted along with the signature provided by the customer. The environment metadata, as described later, provides another layer of security or verification at the time of registration. In one implementation, the metadata includes the characteristics, state of the devices, applications and other entities in the environment of the communication device **107**. Such metadata may also be embedded in the payment card. In another implementation, metadata includes a pattern obtained as a combination of the

signature, the chip, and embedded metadata, and the placement or pattern generated as a combination.

[0065] The term "mobile payment application" or "mobile payment portal" as used here, refers to any registration application that enables communication between users (e.g., sender and recipient of a message) over a wired or wireless communications network. The registration application can be employed by a service provider that delivers a communication service to users, e.g., chat capability or capability to request customer support through ticket creation The registration application may include one or more components and/or engines, or a component and/or engine can include one or more applications. The registration application can include, for example, a mobile payment application, a text messaging application for communication between phones (e.g., conventional mobile telephones or smartphones), or a cross-platform instant messaging application for smartphones and phones that use the Internet for communication.

[0066] The registration application can also include, for example, a web browser application installed on the payment entity, such as a device **107** or a POS terminal **104**, accessible via a uniform resource locator (URL). In some embodiments, the URL is identified by a graphical user interface (GUI) of a mobile payment application installed on the payment entity.

[0067] In one implementation, the POS terminal **104** can be a POS terminal operated and managed by a merchant(s). Furthermore, the POS terminal **104** can be of a varied hardware and/or software configuration, such that POS terminal **104** may be an Android device or an iOS device. In another example, POS terminal **104** can be a cellphone or a tablet computer. The POS terminal **104** can be an electronic point-of-sale system that is connected to a payment object reader **110** capable of accepting a variety of payment instruments, such as credit cards, debit card, gift cards, near-field communication (NFC) based payment instruments, and the like. In one implementation, the payment object reader **110** can accept a payment instrument that is capable of being registered through a signature associated with it. Such a payment instrument with an active-passive registration element, e.g., a customized signature, provided by the user is discussed herein.

[0068] The POS terminal **104** can be connected to a central processing server, hereinafter referred to as the payment processing system (PPS) **116**, to obtain inventory of available products and services and risk parameters. The POS terminal **104** can work in both online and offline modes to allow the merchant to both access the inventory and provisionally process payments whether or not the communication network between the PPS **116** is established or not.

[0069] In some types of businesses, the POS device **104** may correspond to a store or other place of business of the merchant, and thus, may be a fixed location that typically does not change on a day-to-day basis. In other types of businesses, however, the POS system **101** may change physical location from time to time, such as in the case that the merchant operates a food truck, is a street vendor, a cab driver, etc., or has an otherwise mobile business, e.g., in the case of merchants who sell items at buyer's homes, places of business, and so forth. As mentioned before, the POS terminal **104** is connected to a payment object reader **110** that receives the payment object. The payment object reader **110** may be a magnetic stripe card reader, optical scanner, smartcard (card with an embedded IC chip) reader (e.g., an EMV-compliant card reader or NFC enabled reader), radio frequency identification (RFID) reader, or the like, configured to detect and obtain data off any payment object. Accordingly, the payment object reader **110** may include hardware implementation, such as slots, magnetic tracks, and rails with one or more sensors or electrical contacts to facilitate detection and acceptance of a payment object.

[0070] In the figure, the PPS or the device **107** is shown to include certain components. The components may be distributed between the device **107** and the payment processing system **206**. The payment processing system **116** may have limited memory and may only receive cached data when analyzing but otherwise the cached data and components may be stored in the device **107**.

[0071] In one implementation, the payment processing system (PPS) **116** includes one or more components configured specifically to allow the PPS **116** to activate a payment instrument through registration features, such as signatures on payment instrument, through device or applications, such as device **107** and application **114**, and its corresponding device characteristics, profiles, signatures, or fingerprints and store as state along with timestamp at which state status is obtained.

[0072] The components of the device **116** include, for example, a device detection component **140**, a mapping component **138**, a state machine **136**, a location tracker **139**, a customer profile data-structure within a database **144**. The customer profile data-structure includes tables related to transaction history, interaction of the customer with the devices, including PPS, the customer account history, the device configuration, the encryption/decryption keys, payload or detection sequences, the payment instrument history, error logs, mobile payment application configuration, customer location history, device location or states, any conditions or restricted controls to be applied to the customer's account and so on. As mentioned before, in one implementation, these components can be part of a POS terminal, such as POS terminal **104**, connected to the payment processing system **116**. The PPS is communicatively connected to an entity that can be a payment application (not shown), or a device **107**. The payment entity has device characteristics that include but are not limited to: timing parameters, radiated performance, wireless performance, quality of communication links, radio frequency response, transmission measurements, receiver measurements, and engineering tolerances. The communication interface **148** includes ports that can be hardware or software implementations, and can allow the payment entity to communicate with other entities, such as PPS **116**, for example the service agent **109** can communicate with the customer **102** through communication established via communication interface **148**. The payment entity also includes a display **112** where visual cues may be represented to the customer **102**, for example, instructions of how to collect and send data related to state of the device **107**.

[0073] In one implementation, the device detection component **140** is configured to detect devices through physical device characteristics, such as mechanical and operational differences, associated with a device accompanying a merchant. The communication protocol network interface **148** includes various communication protocol interfaces available to the payment processing system **116** with which it can interact with other wireless devices, e.g., customer associated devices. The device detection component **140** is also

configured to generate a state, such as a profile of the communication device in response to a received device characteristic, and to determine unique attributes of the payment entity, that can then act as secondary authentication to the signature at the time of activation of the payment instrument.

[0074] The device detection component **140** may also accompany request for information with specific sequences or payload, which it generates or modifies based on the available communication ports. The payload may either be common between all devices being registered or unique for each payment entity. The payload can be a data signal or a series of instructions that trigger the payment entity or certain components, like the transmitter or sensors, to respond. The nature of responses from the payment entity or the content therein can be unique based on the device. The responses from the selected devices can also be in the form of affirmative or negative answers to queries from the payment entity. The responses, whether binary or textual information, can be conditioned.

[0075] The state machine **136** performs at least the tasks performed by the device detection component **140** and also tracks the state of the device. For example, each time an activation request is made, or a device is queried, a new state may be obtained by the state machine **136**. The states are stored, with a timestamp, in state data structure. In one implementation, the state machine **136** is configured to query the device **107** for state information at periodic or predetermined time intervals. In another implementation, the state machine **136** can query the device **107** at random time intervals to determine or when an activation request is made or account is set up with the payment service. The state machine tracks data related to location of the device, and monitors activity (such as transaction activity, movement activity for example movement from one location to another) to determine unique trends and data associated with the customer and device, and stores such trends and environmental data in customer profile.

[0076] The PPS **116** also includes a location tracker **139** tracks the user's mobile device and the merchant point of sale device to push information based on proximity through for example, short-range communication networks, such as Bluetooth, BLE, and NFC technologies. The location tracker **139** allows and enables the PPS to create APIs for functionalities such as determining which protocols or ports are available in proximate devices, which devices are proximate, for creating receipts, associating rewards, recording loyalty points, etc. global positioning system (GPS) thereby allowing PPS to determine a device location, for example. a separate GPS unit (also referred to as the location component) may be used to determine the location of a buyer registering or activating a payment transaction using a feature on the payment card. Alternatively, the GPS unit by communicating with a chip on the payment instrument, can determine when the instrument reaches a specific location. The GPS or WPS (Wi-Fi positioning system) unit may work on any of the protocols mentioned above. The location information may be used to advertise location specific information to the user. WPS uses surrounding wireless networks to triangulate the location where the photo was taken, unlike GPS, which uses satellites. According to related aspects of the present subject matter, triangulation of data may be by "direct" triangulation, e.g., as where the identity of the buyer device is determined from the point of intersection (or the point of least squares fit) of multiple device profiles or fingerprints (from multiple fingerprints corresponding to detection sequences). Alternatively, or in addition, triangulation may be "indirect," as where the identity of the buyer device is determined not only from the device fingerprints, but also from relative fingerprints originating from other devices in the proximity or historical purchases. The present subject matter also includes implementations where images that are taken by the customer are geo-tagged and the compared to the delivery location of file to determine whether or not a fraudulent attempt is being made to activate the card.

[0077] The present subject matter includes method and systems to generate a payment instrument **108** that may be customized for the customer **102**, for example based on a user input or a system input which is based on past user interactions analyzed using machine learning models. To this end, in one implementation, the customer **102** is presented with an option to provide or even select a system input, for example, on the device **107**'s display **112** or on an interface within the mobile payment application **114**. The customer **102** can provide input in the form of selection where the payment processing system **116** presents to the user one or more options to select from. The options may be templated based on signatures provided by other customers, signatures provided by customers at POS terminals, or can be static images or text. In another example, the customer **102** may provide an input by for example drawing a signature on the user interface, or writing a text.

[0078] In one implementation, the payment processing system, for example through the state machine **136**, determines a set of rules that can be applied to the customer **102**'s signature. The rules can be set according to the customer **102** or can be the same for all the customers **102**. If the rules are configured according to the customer, the state machine **136** uses the state of the customer, and the customer's device to create user specific rules. The state machine **136** may also leverage past transactions or customer signatures provided against payment transactions at one or more POS terminals. The customized rules may also include restrictions dictating the number of times a customer **102** can provide an unacceptable signature before which the customer is barred, for example for a certain time period, from providing any more signatures. The rules can also be specific to the financial entity or location associated with the payment instrument. The rules can also dictate inclusions or exclusions of certain kinds of signatures, for example, offensive signatures may not be acceptable. The signatures may be analyzed on an acceptability criteria and optionally using an acceptability scale to determine whether or not the signature can be allowed. While one signature may be allowed for one customer, the other customer may not be able to use the same or similar signature, for example based on how similar the signatures are or based on the acceptability criteria set up for different customers. The rules may be further modified based on successful or unsuccessful attempts by the customer.

[0079] In one implementation, the payment processing system **116** may verify the conformance of the signature against the rules after the customer **102** has submitted the signature. In another implementation, the payment processing system **116** verifies the conformance of the signature with the rules as the customer is providing the signature. For example, the payment processing system **116** implements

machine learning to determine the course that the customer is likely to take with the drawing and either recommend a different course or reject the signature in advance in adherence with the rules. Such recommendations may be made in real-time or near real-time so that the process is more efficient and there is less back and forth between the user and system input.

[0080] After the payment processing system **116** approves the signature, the payment processing system **116** generates a representation, such as an image object, to apply on the payment instrument. In some cases, the signature can directly be associated to the payment instrument without the need of a representation. In some cases, the association includes an actual embedding, printing, or logical associating of the signature or representation to the payment instrument. Additionally, or alternatively, the signature before being printed on the payment instrument can be used to either look up an account or create an account for the customer. The data structure of the account can then include the newly created signature.

[0081] In one implementation, the representation can include all the content that gets printed on the payment instrument including the signature, account number, and other information, such as customer name, debit card expiration, financial entity, etc. The representation can then be sent to the card manufacturers for association.

[0082] The present subject matter includes methods and systems to register or activate a payment instrument **108** with the payment processing system **116** by leveraging one or more registration features **126** of the payment instrument **108**. In one implementation, the customer **102** or the payment processing system **116** assigns a unique signature **126** to the customer **102**, where the signature or a representation of the signature (also called as pattern herein) may be embedded, printed or otherwise associated with the payment instrument **108**. The customer **102** after receiving the payment instrument **108** accesses the mobile payment application **114** to register the payment instrument **108**. The mobile payment application **114** generates customized flows including actions to scan, photograph or read the signature of the payment instrument **108**. The mobile payment application **114** then sends the scanned image to the payment processing system **116**, which compares the scanned image to the encrypted signature as provided by the customer before the payment instrument was dispatched. In one implementation, the mapping component **138** compares a pattern (obtained when the user captures an image of the payment instrument) and a stored signature (obtained when the user finally connects with the server).

[0083] If the comparison yields a positive match (that is the states are within predetermined threshold value or if the deviation from provided signature to image captured at the time of activation is within a threshold), that is, if the scanned image matches the signature corresponding to the customer and/or associated mobile communication device **107**, the payment instrument **108** is activated. Additionally, the payment processing system **116** applies conditions, such as usage conditions or credit limit, etc., to the payment instrument **108** at this time. However, if the scanned image does not match any of the signatures in the database of the payment processing system **116**, the payment processing system **116** does not activate the payment instrument **108** and generates a notification for the customer **102** to contact a service agent **109** or visit a website instead.

[0084] After the payment instrument is activated, the payment instrument can be used at any payment entities including POS terminal **104** or reader **110**. For the sake of completeness, when using the instrument at the locations, the data is sent to the PPS **116** for further processing. On receiving authorization or contemporaneous to the authorization step, the POS terminal **104** or the payment processing system **116** on behalf of the merchant, generates a fund transfer request for the amount of product or service requested by the merchant **103**. The PPS **116** can be a cloud computing environment, a virtualized computing environment, a computer cluster, or any combination thereof. The PPS **116** can analyze the fund transfer request based on a plurality of rules stored in a knowledge database (not shown) before sending the fund transfer request to a computer system **120** of the PPS' acquirer or merchant's acquirer (hereinafter "acquirer **120**"). For example, one of the rules in the knowledge base may be determining whether the request was authorized based on device fingerprinting as authentication in the offline mode. In one implementation, the acquirer **120** is a bank or financial institution that processes payments (e.g., credit or debit card payments) and may assume risk on behalf of a merchant **103** or a plurality of merchants **103** aggregated by and represented under PPS **116**. The acquirer **120** sends the fund transfer request to the computer system **122** of a card payment network (e.g., Visa, MasterCard, Discover or American Express) (hereinafter "card payment network **122**") to determine whether the transaction is authorized or deficient in any other way. In some implementations, PPS **116** may serve as an acquirer and connect directly with the card payment network **122**. The card payment network **122** forwards the data to the computer system of an issuing bank **124**. The issuer **124** is a bank or financial institution that offered a financial account (e.g., credit or debit card account) to the buyer **102** or **102**A. The issuer makes a determination as to whether the buyer **102**A has the capacity to absorb the relevant charge associated with the payment transaction.

[0085] Each of the aforementioned computer systems can include one or more distinct physical computers and/or other processing devices which, in the case of multiple devices, can be connected to each other through one or more wired and/or wireless networks. All of the aforementioned devices are coupled to each other through the communications network **118**, including the Internet, intranet, a cellular network, a local area network, a wide area network, or any other such network, or combination thereof. Protocols and components for communicating over such a network are well known and are not discussed herein. Furthermore, PPS **116**, the POS terminal **104**, and the mobile device **107** can also communicate over the communications network **118** using wired or wireless connections, and combinations thereof. The payment transaction is either approved or rejected by the issuer **124** and/or the card payment network **122**, a payment authorization message is communicated from the issuer to the merchant computing device **104** via a path opposite of that described above.

[0086] When the transfer of the funds is successful, the transaction is assumed to be processed or completed. Accordingly, a receipt is generated for the user to indicate completion of transaction and details of transaction as proof of purchase. The PPS **116** can also update the inventory and

manage employee information related to employee that performed the purchase, for example assign tips, or hourly rate, etc.

[0087] FIG. **2** illustrates a flow diagram of a method **200** for activating a payment instrument by capturing an image of the payment instrument. At **202**, the process **200** receives, from a mobile device, a request to register or activate a payment instrument, with the request including a representation of a portion of the payment instrument, for example a customized signature displayed on the payment instrument, the signature is interchangeably referred to as a registration feature. The representation can be in the form of an image, scan, or a manual entry of the alphanumeric text or identification of a feature from amongst a list of features displayed on an interface of the device. At **204**, the process **200** analyzes the representation and decrypts if need be. Some implementations perform optical character recognition (OCR) on the image or the signature. In various implementations, text recognition can use classifiers such as support vector machines or neural networks or more classical OCR algorithms such as a stretch and warp analysis. In some implementations, additional versions of the text recognition results, such as a set number of the remaining versions of the text recognition results with the highest confidence scores, can also be transmitted to the financial institution for attempted verification. Additional information can also be transmitted to the financial institution such as portions of an address, a name, a card expiration, a CVV, a phone number, an email, etc. In some implementations, the verification occurs by a user performing an inspection of the best guess and verifying that it is correct. In some implementations where individual character confidence scores are conditional on selections at other character positions, versions of the text recognition results can be updated by modifying the individual character confidence scores. For example, where a version of the text recognition results had a 51% confidence score for an "8" character in position 3, and had a 46% confidence score for a "0" character in position 3, and due to the selected character for position 1, "0" is no longer an option for position 3 due to application of the Luhn algorithm, the confidence score for an "8" at position 3 can be recomputed as 97%. In some implementations where individual character confidence scores are not conditional on other character positions, but a total confidence score for a version of text recognition results is conditional on individual character confidence scores for that version, the combined confidence score for a particular version of the text recognition results can be recomputed based on the selected character being attributed a high confidence score. Taking a simplified example where the account data comprises only four numbers, and one of the versions of the text recognition results with corresponding individual character position confidence scores, denoted "character": score, of: {"2":38%, "5":98%; "4":76%, "8": 60%}, the initial total confidence score can be the average: 68%. If the selected character is "2" for position 1, this version of the text recognition results can be updated to have the corresponding confidence scores: {"2":100%, "5":98%; "4":78%, "8":60%}, thus the total confidence score can be updated to be the new average: 84%.

[0088] At **206**, the process **200** may determine a user associated with the payment instrument, for example based on the customer profile. For instance, where the user (e.g., the customer in the transaction) maintains a user account at the entity performing the process **200**, the user account and, hence, the user, may be identified by mapping the determined information of the payment instrument with the user's account. After identifying the user and user account, a user device associated with the user may be determined at **208**, along with a current geo-location of the user device, such as a phone, tablet computing device, etc. That is, in instances where the user has allowed the sharing of the geo-location of the user's device with the entity (e.g., payment service), the entity may determine a current geo-location of the device. At **210**, the process **200** may also determine a current geographical location of the customer device at which the transaction is being conducted, again with (e.g., advanced) consent of the customer.

[0089] At **212**, the process **200** compares the analyzed data and current location of customer and device and other device state to previously stored customer profiles to determine whether or not the holder of the payment instrument is authorized to activate the payment instrument. The payment service can request additional information, such as an identifier of the payment instrument, an expiration date of the payment instrument, a card network of the payment instrument, a CVV of the payment instrument, or the like, as secondary tool of activation of instrument. If the image matches a saved profile, it is more likely that the image provided by the customer device is in fact a current image of the user's payment instrument rather than a fraudulently obtained image. If the proximity is not within a threshold distance, then at **214** the process **200** may refrain from attempting to activate the payment instrument. In other instances, the process **200** may additionally or alternatively contact the user associated with the payment instrument to receive secure and explicit approval to activate the payment instrument.

[0090] FIG. **3** illustrates a process **300** for an example scenario showing interaction between a customer and a mobile payment application after the customer receives a payment instrument and wishes to register the payment instrument through the mobile payment application, according to an embodiment of the present subject matter.

[0091] FIG. **3** illustrates, at **302**, a customer, after receiving a payment instrument configured as per signature provided at the time of sign-up, captures an image of the signature displayed on the payment instrument. In some implementations, the signature may be embedded or otherwise not visible to the naked eye. In such cases, the mobile payment instrument indicates to the customer the portion of the payment instrument that is to be scanned. In yet other implementations, the customer captures a pattern, including the signature, the metadata embedded in the payment instrument, the placement of the chip and card number, and optionally, other ornamental features such as the color, et. The metadata includes environmental data such as data corresponding to the mobile device of the customer, the mobile payment application executing on the mobile device, and other environmental data that the PPS collects at the time of registration of the payment instrument. The definition of pattern also includes the unique placement of the pattern on the payment instrument.

[0092] At **304**, a customer communication device encrypts the obtained signature and additionally or optionally sends encrypted data associated with customer communication device to a payment service such as PPS. For example, the customer communication device has installed thereon a

mobile payment application or is of a certain model or is located at a certain geographic location The PPS may save the encrypted data in a customer profile. In some embodiments, a customer may modify the respective customer profile, and may select a set of criteria to be included in the encrypted data. The set of criteria may include, but is not limited to, information regarding prior payment instrument approval (i.e., designating the customer as trusted), customer information, the time of issue, merchant location and so on. The PPS too requests for data such as error logs and other information in the form of state of device at time T**1**. In some embodiments, the encrypted data may include information regarding device and application configuration.

[0093] As depicted at **304**, the data may be encrypted using bloom filters with hash functions. Each bloom filter may be sized based upon the customer profile of the particular merchant. In various embodiments, the size of a bloom filter (i.e., size of the array and number of hash functions) may be determined based upon a false positive tolerance. In such embodiments, the false positive tolerance may be a factor of the importance of each criterion. Thus, the more important the criterion, the lower the tolerance for a false positive.

[0094] At **306**, the PPS may determine, based on the state extracted from the encrypted data, including the signature, whether the payment instrument can be registered and authorized to the customer for future use. For example, the PPS determines, based on the state and the signature (decrypted from the encrypted data) matching a previously stored signature corresponding to the customer or mobile payment application of the customer, that the payment instrument is activated. If no match is obtained, the PPS can block the payment instrument and assume for it to be in the hands of a fraudulent user. In another implementations, the PPS can send instructions for the customer to connect with a service agent or access a website where personally identifiable information can be provided for registration.

[0095] At **308**, the PPS can authorize the payment instrument as a registered instrument and allocate conditions and amount for enabling use. Thus, a signature that is otherwise a passive element is used to activate a payment instrument.

[0096] FIG. **4** is a sequence flow method that depicts detecting a device registered to a customer at the time of a first interaction between the customer and the PPS for account set-up prior to or contemporaneous to registration of a payment instrument, according to an embodiment of the present subject matter. The process **400** can be performed by one or more components, devices, or modules such as, but not limited to, the mobile device, the payment processing system, merchant device or POS terminal, or payment beacon or other components or devices. For the sake of explanation, the description hereinafter is described with reference to components described in FIG. **1**, such as POS terminal **104** or payment object reader **110**. As illustrated in FIG. **4**, the process **400** includes a set of operations from step **402** to step **420**.

[0097] In one implementation, the detection of device and creation of a device profile is performed prior to the registration of the payment instrument. In some implementations, the creation of the device profile may happen on a device separate from the device used at the time of registration. In such cases, the customer may create several device profiles or associate several profiles with a single device.

[0098] The process **400** starts with the operation at step **402**. A customer **102** indicates through interaction with a software interactive field on the payment application or a physical button on the communicative device **107** that the customer **102** wishes to provide a signature. The signature can be in the form of an alphanumeric text, image, pattern, or a combination thereof. For this, the mobile payment application or PPS can generate an interface, for example a touch screen or key interface, where the customer **102** can manually key in information. In other examples, the mobile payment application or PPS provides pre-set options, which the customer **102** can choose as signature. For example, the pre-set options may include stock images randomly selected for the customer **102**. In other instances, the pre-set options may be configured for the customer **102** based on device profile, environmental data, or other data obtained from the customer like personal identifiable information.

[0099] Once the signature is provided, the PPS **116** collects environmental data corresponding to the customer interaction including, but not limited to, device profile. Thus, the PPS may store the location coordinates of the device **107**. The PPS proceeds to detecting location of the POS system **101** through location detection techniques, such as techniques based on triangulation, trilateration, multilaterations, geo-fence, global or local positioning systems, and the like. This step may be performed contemporaneous to the steps of scanning the device described below. The payment processing system **116** scans device **107** and applications, including the mobile payment applications, executing on the device for environmental data. The PPS **116** obtains authorization from the customer.

[0100] The PPS then determines how it can interact with the recognized buyer device or devices. For this, the PPS sends preliminary signals or data to explore communication ports in the device **107**, which are available for access and communication (step **404**). If there is at least one communication port available as determined in step **406**, the flow control moves to step **408**. In some cases, the PPS may detect a number of communication ports that are available or can be made available on request. In such cases, the customer selects a communication port. In other cases, the selection process can be automated such that ports that meet certain conditions are enabled or used. For example, only power-saving or time-saving communication channels are set up.

[0101] If no ports are available for access, the flow transitions to step **410** where the customer is notified to activate certain ports to allow communication. Such notifications may be sent through text or push notifications. After activation, the flow either moves to **406** for confirmation or directly to **408**.

[0102] At step **408**, the device detection component **140** of the PPS generates payload and/or detection sequences adapted based on the available communication ports and in accordance with the communication protocols on which the ports operate. The payload and detection sequences can be configured based on type of the POS system **101** (such as the type of terminal—Android based, iOS based and so on). In some implementations, a unique payload is generated every time. The detection sequences can be in the form of specific signals requesting the device to respond in a certain way or to release certain information, such as version number of the device, software version, operating system, error logs, and the like.

[0103] The targeted device **107** processes the payload and detection sequences via the appropriate communication ports and protocols (step **412**) and responds accordingly. Thus, based on the detection sequences and payload, the device responds in a certain manner and generates state of the device, time-stamped at T**1** (or environmental data), which is captured by the sequences or payload or some other signal and stored, for example, in the device itself or sent to the POS terminal via the same or a different communication channel, as shown in step **414**. The device state is stored as state value at first time, T**1**, i.e., the first time customer established communication with the PPS for account set-up. The detection sequences can also be information-gathering requests configured to obtain state, for example in the form of digital device fingerprints, from the devices. Device state also includes radio, mechanical or operational fingerprints—such as radiated performance, device defects, sensor performance, communication speed or lags, spectrum data, the location and time of the transaction or buyer, or the card information, open communication ports, settings of applications, the number of applications running on the devices, memory usage, virus identification, and the like (step **416**).

[0104] At step **418**, the device state at T**1** and the signature provided by the customer at step **402** may be encoded at the device level. The payment device can also apply tokenized pseudo-random numbers (also referred to as hash keys) to the feature vectors to generate the digital device fingerprint. A National Institute of Standard and Technology (NIST) compliant True Random Number Generator (TRNG) can generate the pseudo-random numbers. The encoding can also be done based on keys generated by a cryptographic unit (not shown). Examples of keys include authentication keys, which include SCP03 master keys (Message Authentication Code Key: MAC, Encryption Key: ENC and Key Encryption Key: KEK, which are 256-bit Advanced Encryption Standard (AES) symmetric keys with associated key derivation data) or Key Agreement Keys (e.g., user server signature verification public key, user server static public key, user static key pair with both public and private key). The encrypted state can also be created using other schemes, such as fuzzy vault algorithm, a cancelable fuzzy vault scheme based on irreversible hash functions, such as MD, RIPEMD, and SHA.

[0105] In some implementations, the device state and signature may be encrypted using bloom filters with hash functions. The bloom filter may use the hash functions to store information about a customer without the risk of the customer's payment information or signature being stolen or otherwise used in a nefarious manner (e.g., through reconstruction). In various embodiments, the hash functions hash or map the customer's signature and device state (i.e., an element) to designated array positions of a bloom filter array to test whether the criterion is met (i.e., a positive match occurs when all of the mapped-to array positions have a value of one "1"; no match occurs, and the criterion is not met, if any of the array positions contain a zero ("0")). In some embodiments, the device state may be truncated to a number less than the standard **16** or 17-digit identifier number. For example, the hash functions may truncate a payment instrument identifier to a **10**-digit number, and map the 10-digit number to the bloom filter array. Though bloom filters with hash functions are described herein, it is imagined that the other encryption techniques may be used to maintain the security of state, such as hash tables, simple arrays, and the like. In various embodiments, the device **107** may incorporate a plurality of bloom filters, each designated to determine if the ticket meets one or more criteria of a particular merchant. The criteria may be based on issue level, number of tickets sent over a period of time, interaction history, customer data, customer device information, and/or merchant history. For example, a bloom filter and/or hash function may be designated to determine that a customer has multiple devices at one location (e.g., a laptop, phone, etc.). In some embodiments, the device **107** may incorporate one bloom filter (for a particular merchant) with one or more hash functions, each hash function configured to determine if the customer profile including the device state and/or signature satisfies one or more criteria. Each bloom filter may be sized based upon the merchant profile of the particular customer.

[0106] In various embodiments, the size of a bloom filter (i.e., size of the array and number of hash functions) may be determined based upon a false positive tolerance. In such embodiments, the false positive tolerance may be a factor of the importance of each criterion. Thus, the more important the criterion, the lower the tolerance for a false positive.

[0107] In various embodiments, the customer and/or PPS may designate a tolerance by inputting a probability percentage for false positives (i.e., a merchant will tolerate a 1% chance of a false positive). The tolerance may be set for all bloom filters in a customer profile, or it may be set per criterion. For example, a bloom filter designated to determine whether a customer profile may be sized such that the probability of a false positive is relatively high (i.e., >1%). Whereas a bloom filter designated to determine if a customer profile is associated with a fraudulent attempt to register may be sized for a low probability of false positives (i.e., <1%).

[0108] In various embodiments, the device may comprise at least a payment application for processing transactions. The payment application may receive and store data from the customer profile. In some embodiments, the payment application may process and save data locally on the device.

[0109] While in other implementations, the device state obtained at T**1**, which are to be used for device identification and testing at a later time for payment instrument registration, are then sent to the PPS, as a customer profile, as shown in step **420**.

[0110] FIG. **5** is a sequence flow method that depicts a method **500** for registering a payment instrument using a device associated with a customer or s payment application associated with the payment service where the payment instrument includes a registration feature as previously provided by the customer, according to an embodiment of the present subject matter. The process **500** can be performed by one or more components, devices, or modules such as, but not limited to, the mobile device, the payment processing system, merchant device or POS terminal, or payment beacon or other components or devices. For the sake of explanation, the description hereinafter is described with reference to components described in FIG. **1**, such as customer communication device **107**. As illustrated in FIG. **5**, the process **500** includes a set of operations from step **502** to step **514**.

[0111] The process **500** starts with the operation at step **502**. On receiving a physical payment instrument with the custom signature, the customer **102** accesses the mobile payment application or a landing page of a website to initiate

registration of the payment instrument for use. At step **502**, the customer scans or captures an image of the payment instrument or a portion of the payment instrument displaying the signature. The mobile payment application displays to the customer the method of capturing the pattern, which may or may not be visible to the naked eye. For example, the mobile payment application may indicate the customer to place the payment instrument in a certain orientation or fit within a preset shape, to capture image. The device **107** on which the mobile payment application is executing encrypts the signature and optionally, the device state, such as data related to the device **107**, mobile payment application **114**, location of the device, etc. The PPS **116** receives the encrypted information from the device **107** at step **502**.

[0112] In response, the PPS **116** retrieves a customer profile packet including device state and signature from the device associated with the customer as obtained at a previous time instant, say at the time of account set-up. The customer profile may be encrypted. In such case, the packet having device state and signature is first decrypted using technologies known in the art (step **504**).

[0113] The PPS **116** then compares the customer profile packet with newly obtained pattern and other information to authorized activation of the payment instrument (step **506**). If the match operation (step **506**) as a result of the comparison at step **504** yields a "Yes," the flow transitions to step **508**. The PPS **116** confirms to check whether there are any rules (e.g., as defined below) associated with the device or customer, which restrict activation of the payment instrument, or if the credit line is to be computed or adjusted. (step **508**). In case there are any conditions, the conditions are applied at step **510** and then the card is activated at step **512**. If conditions are not available, the payment instrument is activated with default conditions at step **512**. .

[0114] If the match operation (step **506**) as a result of the comparison at step **504** yields a "No," the PPS **116** generates an alternate path for the customer to follow to activate the payment instrument (step **514**). For example, the alternate path may involve communicating with a service agent. For this, the PPS **116** can generate notifications to alert the customer indicating various options for example, "call customer care," or "provide SSN to proceed."

[0115] FIG. **6** is a sequence flow method that depicts a method **600** for activating a payment instrument on a device or application associated with the customer, according to an embodiment of the present subject matter. The process **600** can be performed by one or more components, devices, or modules such as, but not limited to, the customer mobile device, the payment processing system, merchant device or POS terminal, or payment beacon or other components or devices. For the sake of explanation, the description hereinafter is described with reference to components described in FIG. **1**, such as customer communication device **107**. As illustrated in FIG. **6**, the process **600** includes a set of operations from step **602** to step **616**.

[0116] The process **600** starts with the operation at step **602**. The PPS **116** or the mobile payment application **114** receives a ticket indicating a request from the customer to activate the payment instrument. In response, the mobile payment application **114** generates visual cues such as instructions to activate the payment instrument. At this time, the device **107**, through its communication interfaces, obtains device state and other environmental data as secondary authentication. The visual cues can be in the form of notifications, such as push notifications. The push notifications are sent to the payment device or the device associated with the customer. For example, the mobile payment application **114** presents on the interface of the payment device real-time and customized instructions, such as, "press a button located at the bottom of the reader," "turn the device off for five seconds", "register your instrument at this time". "move the device an inch closer to the terminal", "do you need additional assistance?", "connecting to a support representative", "your bank has approved registration", and so on. To this end, the customer submits user engagement input in response to each of the activation instructions while the PPS or the mobile payment application **114** waits. Other examples of user engagement input include providing authentication or security keys as a visual, audio or haptic input.

[0117] At step **604**, the customer engages with the device or the notifications or both to start the process. In response to customer engagement for the first time or at the time of engagement with visual cues, the PPS initiates a mode switch. The modes are switched from merchant control to at least view, edit, or collect mode. In collect mode, PPS can collect information related to customer engagement, for example in the form of environmental data or screenshots as proof of engagement (step **606**).

[0118] At step **608**, PPS receives customer engagement in response to activation path. In some cases, the PPS can request control from the customer and automatically execute certain or all steps described in the activation path. For example, the PPS can automatically push certain updates or delete data from the devices to assist in activation. In one implementation, the mobile payment application **114** switches control from the mobile payment application **114** interface to the sensor, such as camera, to facilitate capturing of an image of the signature on the payment instrument.

[0119] At step **610**, PPS obtains image, scans or otherwise information indicating engagement with a signature on the payment instrument and device's state after each step of the activation step. At step **612**, PPS matches the engagement data as reflected in the obtained images and device state with previously stored customer profiles. If there is a match, that is, "yes" branch of the step **612**, PPS continues to allow activation of the payment instrument and applies any conditions or restricted control on the payment instrument. For example, the credit line can be determined and assigned to the customer at this time.

[0120] At step **616**, however, if the PPS determines that the engagement does not match with any of the customer profiles, either the PPS takes control, for example, for automatic execution of an activation path or under authority of a service agent. In another case, the PPS can generate notifications to alert the customer on an authorized device or an authorized phone number or email address that an attempt is being made to activate an issued payment instrument and the attempt may be fraudulent. In yet another case, the mobile payment application **114** or PPS generates alternate ways to activate the card in step **614**, for example, by providing secondary information, like an SSN, PIN, etc.

[0121] FIGS. **7**A and **7**B illustrate example user interfaces to indicate that a payment instrument is available for physical delivery to a customer, according to an example embodiment of the present subject matter. In FIG. **7**A, the interface on a mobile payment application provides an option to the customer to request a physical delivery of the payment

instrument. As shown in FIG. **7**B, the customer can also see the instrument information, such as number, expiration date, CVV, etc., to enable the customer to use the payment instrument without a physical instrument as well. However, if the customer chooses to request a delivery of the physical instrument, for example in a metal or plastic form, the selectable option such as " mail me a card" gives the customer that flexibility.

[0122] FIG. **8** illustrates a user interface to receive a custom signature from a customer, according to an example embodiment of the present subject matter. As shown in FIG. **8**, the customer can customize the payment instrument with a signature for which the interface provides a writing tool. In other implementations, the customer can select from pre-set options, such as an image, an alphanumeric value, etc., as the signature. The customer can also select the location on the payment instrument where the signature should be featured and whether or not it should be visible. For example, in some cases, the signature can be encrypted and embedded in the card such that only certain scanners can read the signature.

[0123] In one implementation, the system and method generates a physical payment card which is customized for a user via a payment processing system. To this end, in one implementation, the user may request, through a payment application executing on a user device such as a phone or computer, generation of a physical payment card for an account associated with the user. Optionally, the payment application may notify the user to approve generation of a card for their account. In cases where the payment application has digital wallets corresponding to several user accounts, each of the accounts may be connected to a card generation functionality. In another example, all the accounts may be connected to a single payment instrument.

[0124] Through the application, the user may provide a signature to be printed on the payment card. For this, the PPS may cause activation of a user interface on the customer device to enable receipt of the signature. The PPS may generate a set of rules either specific to the user or applicable to all users. As the user is providing the signature, the PPS may ensure that the user is conforming to the rules, for example in real-time or near real-time, or after the signature is complete. The advantage of PPS checking the conformance of the signature as the user is drawing is that the changes can be made at that time instant.

[0125] The present subject matter includes method and systems to generate a payment instrument **108** that may be customized for the customer **102**, for example based on a user input or a system input which is based on past user interactions analyzed using machine learning models. To this end, in one implementation, the customer **102** is presented with an option to provide or even select a system input, for example, on the device **107**'s display **112** or on an interface within the mobile payment application **114**. The customer **102** can provide input in the form of selection where the payment processing system **116** presents to the user one or more options to select from. The options may be templated based on signatures provided by other customers, signatures provided by customers at POS terminals, or can be static images or text. In another example, the customer **102** may provide an input by for example drawing a signature on the user interface, or writing a text.

[0126] In one implementation, the payment processing system, for example through the state machine **136**, determines a set of rules that can be applied to the customer **102**'s signature. The rules can be set according to the customer **102** or can be the same for all the customers **102**. If the rules are configured according to the customer, the state machine **136** uses the state of the customer, and the customer's device to create user specific rules. The state machine **136** may also leverage past transactions or customer signatures provided against payment transactions at one or more POS terminals. The customized rules may also include restrictions dictating the number of times a customer **102** can provide an unacceptable signature before which the customer is barred, for example for a certain time period, from providing any more signatures. The rules can also be specific to the financial entity or location associated with the payment instrument. The rules can also dictate inclusions or exclusions of certain kinds of signatures, for example, offensive signatures may not be acceptable. The signatures may be analyzed on an acceptability criteria and optionally using an acceptability scale to determine whether or not the signature can be allowed. While one signature may be allowed for one customer, the other customer may not be able to use the same or similar signature, for example based on how similar the signatures are or based on the acceptability criteria set up for different customers. The rules may be further modified based on successful or unsuccessful attempts by the customer, and other context such as geographical location of the customer, etc.

[0127] In one implementation, the payment processing system **116** may verify the conformance of the signature against the rules after the customer **102** has submitted the signature. In another implementation, the payment processing system **116** verifies the conformance of the signature with the rules as the customer is providing the signature. For example, the payment processing system **116** implements machine learning to determine the course that the customer is likely to take with the drawing and either recommend a different course or reject the signature in advance in adherence with the rules. Such recommendations may be made in real-time or near real-time so that the process is more efficient and there is less back and forth between the user and system input.

[0128] After the payment processing system **116** approves the signature, the payment processing system **116** generates a representation, such as an image object, to apply on the payment instrument. In some cases, the signature can directly be associated to the payment instrument without the need of a representation. In some cases, the association includes an actual embedding, exposing, printing, or logical associating of the signature or representation to the payment instrument. Additionally, or alternatively, the signature before being printed on the payment instrument can be used to either look up an account or create an account for the customer. The data structure of the account can then include the newly created signature and a position indicating where the various content goes. For example, the signature may go in the lower right corner of the card, while the card number may be printed in the center of the back of the card.

[0129] In one implementation, the representation can include all the content that gets printed on the payment instrument including the signature, account number, and other information, such as customer name, debit card expiration, financial entity, etc. The representation can then be sent to the card manufacturers for association. After generation of the card, the PPS causes delivery of the card to the

users. Accordingly, a notification may be sent to the user when the card is being prepared and when it is ready to be sent. In some cases, the notification may also be sent prior to printing of th card to confirm whether the signature and design of the overall card is acceptable to the user.

[0130] FIGS. **9**A-C illustrate example user interfaces, presented on a computing device, to receive customer engagement for the field of address where the payment instrument is to be delivered, according to an example embodiment of the present subject matter. The customer can select the addresses from a list of addresses provided by the customer at the time of account set up. Alternatively, the customer can use the pre-fill or suggestion feature facilitated by the mobile payment application thus as the customer enters the address, the mobile payment application can suggest possible entries.

[0131] FIGS. **10**A and **10**B illustrate example user interfaces, being presented on the computing device, to indicate verification and information related to shipping of the physical instrument, according to an example embodiment of the present subject matter. After the customer provides the address information for delivery, the request to generate and deliver the payment instrument is sent by the mobile payment application to the PPS through the computing device. The PPS then facilitates generation of the payment instrument with the customized signature and at a customized location. If the location and signature are not customized, the PPS may randomly generate a signature to be associated with the customer. The signature is embedded, printed, or otherwise associated with the payment instrument. After the payment instrument is crafted, the payment instrument is delivered to the customer. In some instances, a tracking chip within the payment instrument indicates when the payment instrument has reached the customer or whether or not it has reached the location where the customer requested delivery or if the customer is attempting to activate the payment instrument from a location different than the delivery location.

[0132] FIGS. **11**A and **11**B illustrate example user interfaces being presented on the computing device to notify the customer to initiate registration or activation of the payment instrument, according to an example embodiment of the present subject matter. Once the customer receives the physical payment instrument, the method starts at FIG. **11**A where the customer is notified through visual cues to activate the payment instrument. This notification can be within the mobile payment application as shown in FIG. **11**A or as part of a text notification on home page as shown in FIG. **11**B.

[0133] FIGS. **12**A-E illustrate example user interfaces, being presented on the computing device, for activating a payment instrument by using a registration feature of the payment instrument, according to an example embodiment of the present subject matter.

[0134] FIG. **12**A shows example visual cues on the mobile payment application that the mobile payment application or PPS generates to enable the customer to activate the payment instrument. As shown, the mobile payment application sends cues to snap a picture of the payment instrument for example by placing or fitting the payment instrument within a preset shape on the user interface of the mobile device. In other instances, the payment application can send visual cues to scan the payment instrument. By placing the payment instrument in a prescribed shape or orientation, the mobile payment application or PPS is able to read the signature by extracting relevant data from certain coordinates. Along with the signature, the mobile payment application can also ask the customer to key-in the CVV printed at the back of the payment instrument as shown in FIG. **12**B. During this time, the mobile payment application can also collect environmental data, such as data on the location, the device, the application, etc., as secondary authentication of the customer. The confirmation process is shown in FIG. **12**C where the mobile payment application compares the obtained data and signature image with previously stored profiles. This step can be performed in both online or offline modes.

[0135] Once a match is obtained and identity of the customer is verified against the instrument holder, the payment instrument is activated as shown in FIG. **12**E. In some implementations, a PIN number can be assigned as shown in FIG. **12**D. It will be understood that the interfaces are shown as examples only and any layout, orientation, color scheme, and arrangements are possible.

[0136] Unless contrary to physical possibility, it is envisioned that (i) the methods/steps described above may be performed in any sequence and/or in any combination, and that (ii) the components of respective embodiments may be combined in any manner. Note that any and all of the embodiments described above can be combined with each other, except to the extent that it may be stated otherwise above or to the extent that any such embodiments might be mutually exclusive in function and/or structure.

[0137] Although the present subject matter has been described with reference to specific example embodiments, it will be recognized that the subject matter is not limited to the embodiments described, but can be practiced with modification and alteration within the spirit and scope of the appended claims. Accordingly, the specification and drawings are to be regarded in an illustrative sense rather than a restrictive sense. It will thus be appreciated that those skilled in the art will be able to devise various arrangements that, although not explicitly described or shown herein, embody the principles of the present subject matter. Furthermore, all examples recited herein are intended to be for illustrative purposes only to aid the reader in understanding the principles of the present subject matter, and are to be construed as being without limitation to such specifically recited examples and conditions. Moreover, all statements herein reciting principles, aspects, and embodiments of the present subject matter, as well as specific examples thereof, are intended to encompass equivalents thereof.

[0138] A sensor-implemented method for activating a payment instrument associated with a user through a mobile payment application associated with a payment processing system (PPS), the method comprising providing an engagement option on a user interface of the mobile payment application executing on a mobile device of the user; detecting, by a processor of the mobile device and in response to an interaction of the user with the engagement option, an indication that the user has submitted a signature to be associated with the payment instrument; generating a request, from the mobile payment application and for the payment processing system, to cause a physical delivery of the payment instrument to a user location, wherein the payment instrument includes a pattern that substantially corresponds to the signature submitted by the user; receiving, by the processor of the mobile device, an indication that the user intends to activate the delivered payment instrument

having the pattern; generating, on the interface of the mobile payment application, a set of instructions for the user instructing the user to capture an image of the pattern; obtaining, by at least one sensor of the mobile device and as a sensor input, the image of the pattern; transmitting, by the processor of the mobile device, the image of the pattern to the payment processing system; comparing, by a processor of the payment processing system, the image of the pattern with one or more previously submitted signatures including the signature submitted by the user; if the image of the pattern matches a previously submitted signature provided by the user, activating, by the payment processing system, the payment instrument, wherein activating further includes granting the user, by the payment processing system, access to a predetermined amount of funds through the activated payment instrument; and if the image of the pattern does not match a previously submitted signature provided by the user, generating instructions for the user to provide secondary authentication.

What is claimed is:

1. A method comprising:

generating, by a payment service system (PSS) and in a data store maintained by the PSS, an account for a user, wherein the account is generated based on an account request received from the user via a payment application associated with the PSS and executing on a device associated with the user, and wherein the PSS is configured to process payment transactions for the user using the account based on interactions by the user with the payment application;

receiving, by the PSS and from the payment application, a payment card request from the user to associate a payment card with the account, wherein the payment card request is made via an interaction by the user with the payment application;

based on the payment card request, facilitating, by the PSS:

transmission of instructions to cause the payment card to be printed for physical delivery to the user; and

generation of a virtual card account associated with the payment card and the account, wherein the virtual card account is usable for payment transactions by the user prior to delivery of the payment card; and

upon receiving an indication of physical receipt of the payment card via the payment application, activating, by the PSS, the payment card for use in payment transactions.

2. The method as claim **1** recites, further comprising:

presenting, by the payment application interfacing with the PSS, a handwriting interface for capturing handwritten input from the user, wherein the handwritten input is associated with a card customization feature for printing on the physical payment card.

3. The method as claim **2** recites, further comprising, upon receiving a confirmation of the card customization feature:

mapping, by the PSS and in the data store, card information associated with the payment card to the account of the user.

4. The method as claim **2** recites, wherein instructions to cause the payment card to be printed for physical delivery include instructions to print the card customization feature on the payment card.

5. The method as claim **4** recites, wherein the instructions to print the card customization feature on the payment card comprise instructions to print the card customization feature at a predetermined location on the payment card.

6. The method as claim **1** recites, wherein, based on receiving the payment card request, presenting, by the PPS, a representation of a virtual payment object associated with the virtual card account.

7. The method as claim **6** recites, wherein the virtual payment object includes content printed on the payment card, including one or more of an account identifier, a name, an expiration date, a financial entity associated with the account, or a card customization feature.

8. The method as claim **6** recites, further comprising:

causing presentation of, by the PSS and on an interface of the device associated with the user, the virtual payment object.

9. The method as claim **1** recites, further comprising:

configuring the virtual card account for inclusion in a virtual wallet associated with the user and the mobile device.

10. The method as claim **1** recites, wherein the virtual card account remains usable after activation of the payment card.

11. A system comprising:

one or more processors;

one or more non-transitory computer-readable media storing instructions executable by the one or more processors, wherein the instructions program the one or more processors to perform actions comprising:

generating, by a payment service system (PSS) and in a data store maintained by the PSS, an account for a user, wherein the account is generated based on an account request received from the user via a payment application associated with the PSS and executing on a device associated with the user, and wherein the PSS is configured to process financial transactions for the user using the account based on interactions by the user with the payment application;

receiving, by the PSS and from the payment application, a payment card request from the user to associate a payment card with the account, wherein the payment card request is made via an interaction by the user with the payment application;

based on the payment card request, facilitating, by the PSS:

transmission of instructions to cause the payment card to be printed for physical delivery to the user; and

generation of a virtual card account associated with the payment card and the account, wherein the virtual card account is usable for payment transactions by the user prior to delivery of the payment card; and

upon receiving an indication of physical receipt of the payment card via the payment application, activating, by the PSS, the payment card for use in payment transactions.

12. The system as claim **11** recites, the actions further comprising:

presenting, by the payment application interfacing with the PSS, a handwriting interface for capturing handwritten input from the user, wherein the handwritten input is associated with a card customization feature for printing on the physical payment card.

13. The system as claim **12** recites, wherein instructions to cause the payment card to be printed for physical delivery include instructions to print the card customization feature on the payment card.

14. The system as claim **11** recites, wherein, based on receiving the payment card request, presenting, by the PPS, a representation of a virtual payment object associated with the virtual card account.

15. The system as claim **14** recites, wherein the virtual payment object includes content printed on the payment card, including one or more of an account identifier, a name, an expiration date, a financial entity associated with the account, or a card customization feature.

16. The system as claim **14** recites, the actions further comprising:

causing presentation of, by the PSS and on an interface of the device associated with the user, the virtual payment object.

17. The system as claim **11** recites, the actions further comprising:

configuring the virtual card account for inclusion in a virtual wallet associated with the user and the mobile device.

18. The system as claim **11** recites, wherein the virtual card account remains usable after activation of the payment card.

19. A method comprising:

generating, by a payment service system (PSS) and in a data store maintained by the PSS, an account for a user, wherein the account is generated based on an account request received from the user via a payment application associated with the PSS and executing on a mobile device associated with the user, and wherein the PSS is configured to process financial transactions for the user using the account based on interactions by the user with the payment application;

receiving, by the PSS and from the payment application, a payment card request from the user to associate a payment card with the account, wherein the payment card request is made via an interaction by the user with the payment application;

based on the payment card request, facilitating, by the PSS:

transmission of instructions to cause the payment card to be printed for physical delivery to the user; and

generation of a virtual card account associated with the payment card and the account, wherein the virtual card account is usable for payment transactions by the user prior to delivery of the payment card;

configuring the virtual card account for inclusion in a virtual wallet associated with the user and the mobile device; and

upon receiving an indication of physical receipt of the payment card via the payment application, activating, by the PSS, the payment card for use in payment transactions.

20. The method as claim **19** recites, further comprising:

causing presentation of, by the PSS and on an interface of the device associated with the user, a representation of a virtual payment object associated with the virtual card account.

* * * * *