

(12) **United States Patent**
Rinehart et al.

(10) **Patent No.:** **US 12,483,555 B1**
(45) **Date of Patent:** **Nov. 25, 2025**

(54) **MUTUAL AUTHENTICATION SYSTEM**

(56) **References Cited**

(71) Applicant: **United Services Automobile Association (USAA)**, San Antonio, TX (US)

U.S. PATENT DOCUMENTS

6,711,400 B1 3/2004 Aura
8,424,057 B2 * 4/2013 Mardikar H04W 12/128
713/168

(72) Inventors: **Casey Roberto Rinehart**, San Antonio, TX (US); **Justin Royell Nash**, Little Elm, TX (US); **Navaid Hussain**, Dallas, TX (US); **Soon Fatt Hoo**, Tahlequah, OK (US); **Subhalakshmi Selvam**, Allen, TX (US); **Steven Michael Anzaldua**, Goliad, TX (US)

(Continued)

FOREIGN PATENT DOCUMENTS

WO WO-2012055829 A1 * 5/2012 G06F 21/34

OTHER PUBLICATIONS

(73) Assignee: **United States Automobile Association (USAA)**, San Antonio, TX (US)

Alexandre Alapetite, "Dynamic 2D-barcode for multi-device Web session migration including mobile phones", Technical University of Denmark, Department of Management Engineering Produktionstorvet 426-A, DK-2800 Kongens Lyngby, Denmark, doi: 10.1007/ s00779-009-0228-5. (Year: 2010).

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 883 days.

Primary Examiner — Piotr Poltorak

(21) Appl. No.: **17/712,647**

(74) *Attorney, Agent, or Firm* — Potomac Law Group, PLLC; Dannon G. Allbee

(22) Filed: **Apr. 4, 2022**

Related U.S. Application Data

(63) Continuation-in-part of application No. 16/837,921, filed on Apr. 1, 2020, now Pat. No. 11,316,849.
(Continued)

(51) **Int. Cl.**
H04L 29/06 (2006.01)
G06Q 30/016 (2023.01)
H04L 9/40 (2022.01)

(52) **U.S. Cl.**
CPC **H04L 63/0869** (2013.01); **G06Q 30/016** (2013.01)

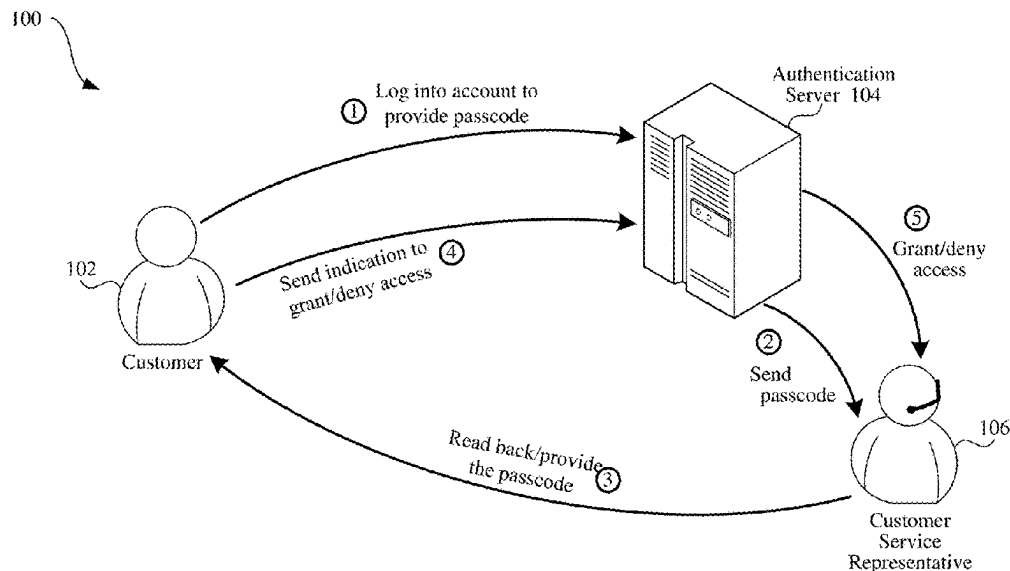
(58) **Field of Classification Search**
None

See application file for complete search history.

(57) **ABSTRACT**

Mutual authentication and CSR verification techniques are described in this patent document. When a first person calls a second person, neither of them know that the other person is who he or she says he or she is. After a second person receives the call, the second person can log into a provider portal using a user device. After the second person logs in, the second person can see a verification of the call, can input on the user device a time passcode, or can receive such as passcode from a central system to authenticate the first person. The first person can provide the passcode to the second person. Upon receiving the inputted passcode, the second person can use his or her user device to indicate that the time passcode is correct so that the second person can be authenticated to access the first person's account.

20 Claims, 11 Drawing Sheets



Page 2

* cited by examiner

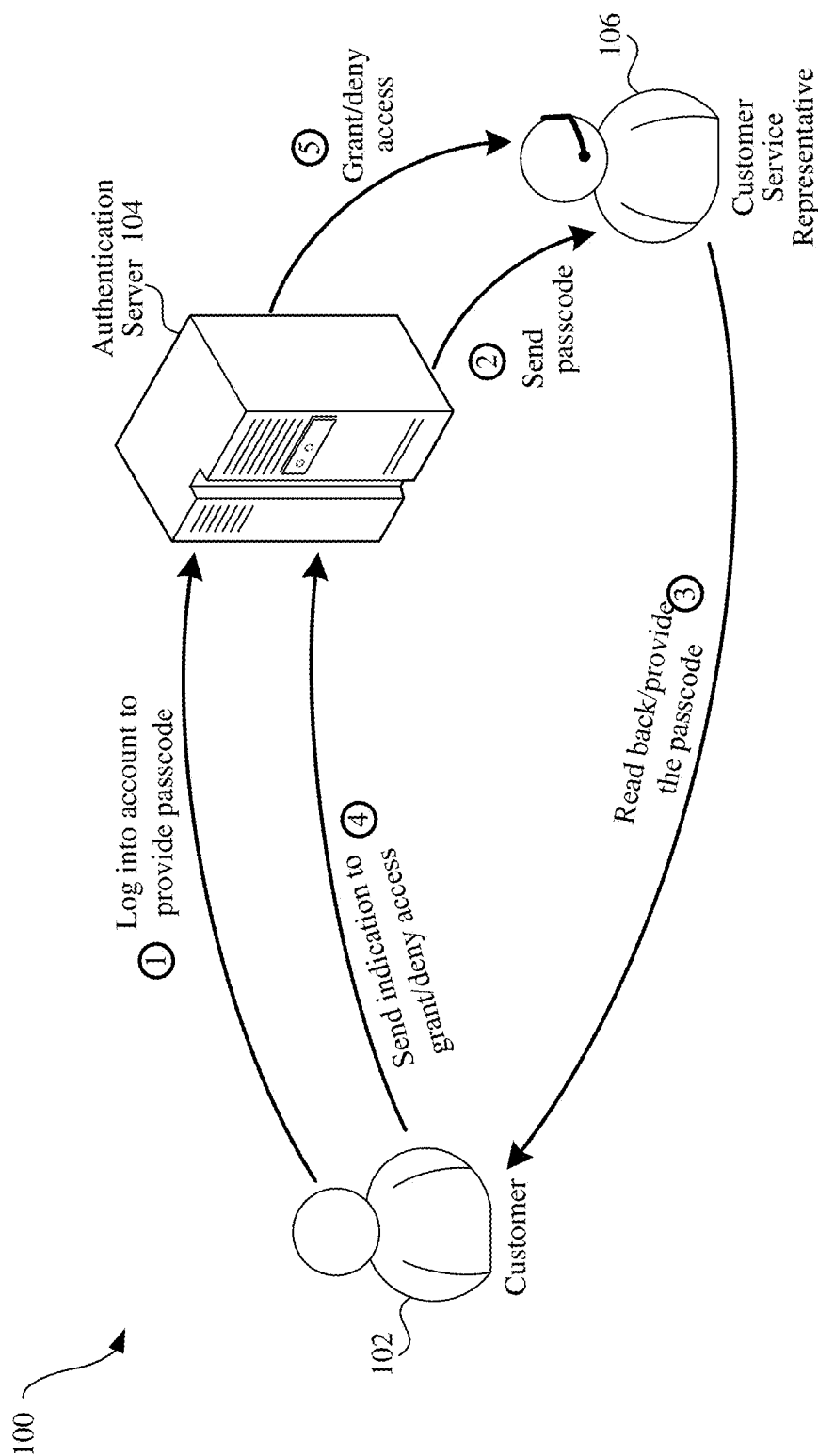


FIG. 1A

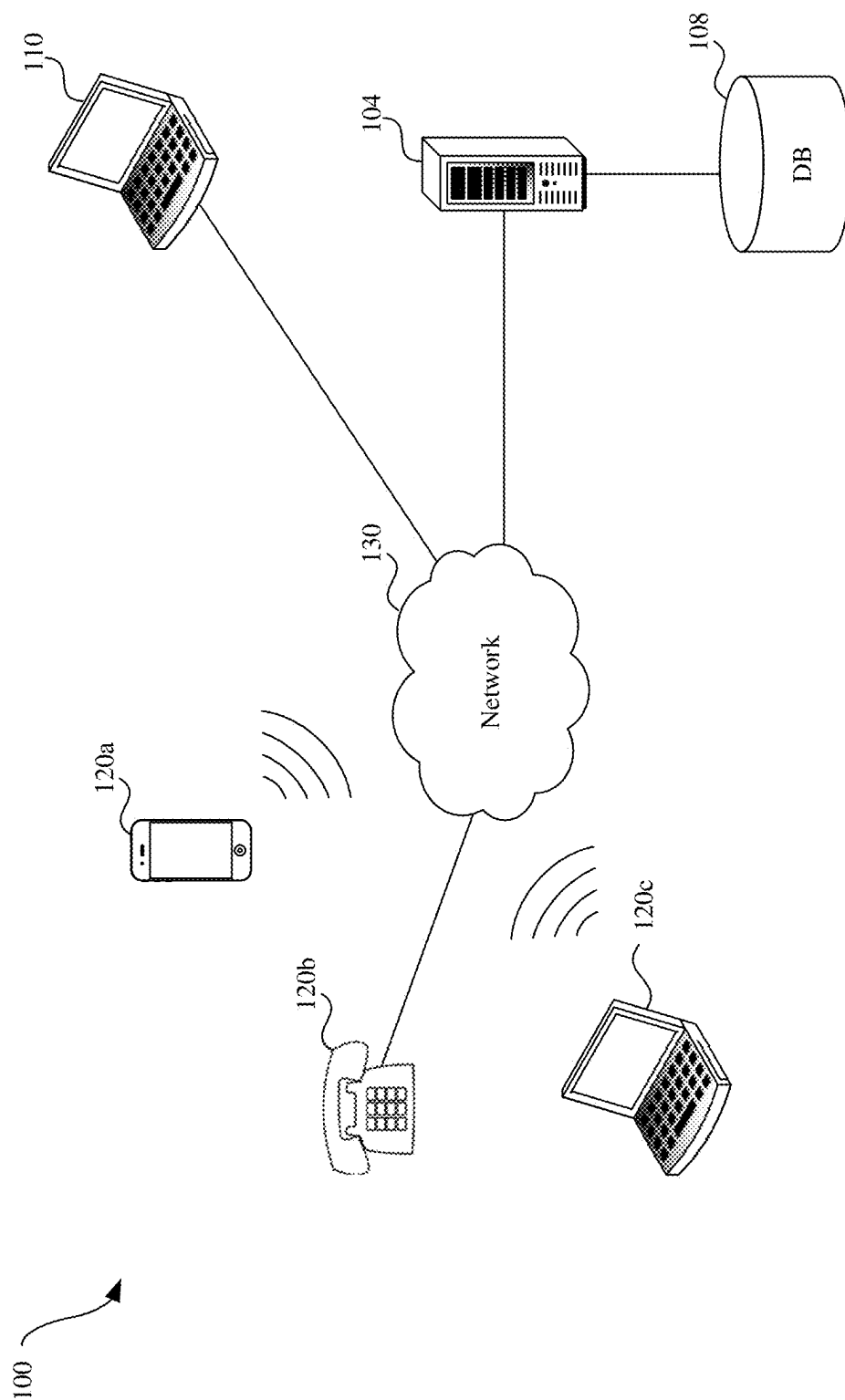


FIG. 1B

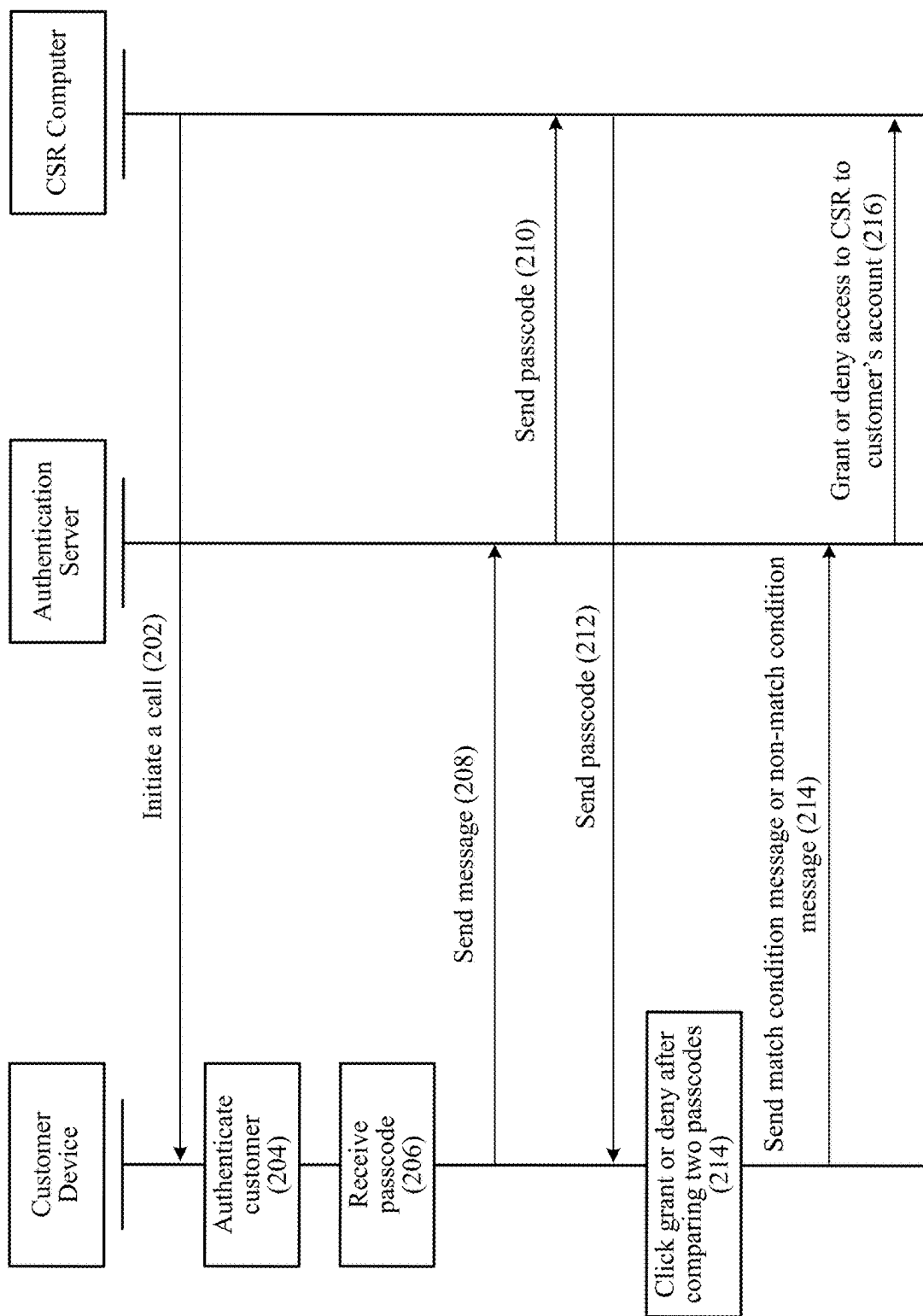
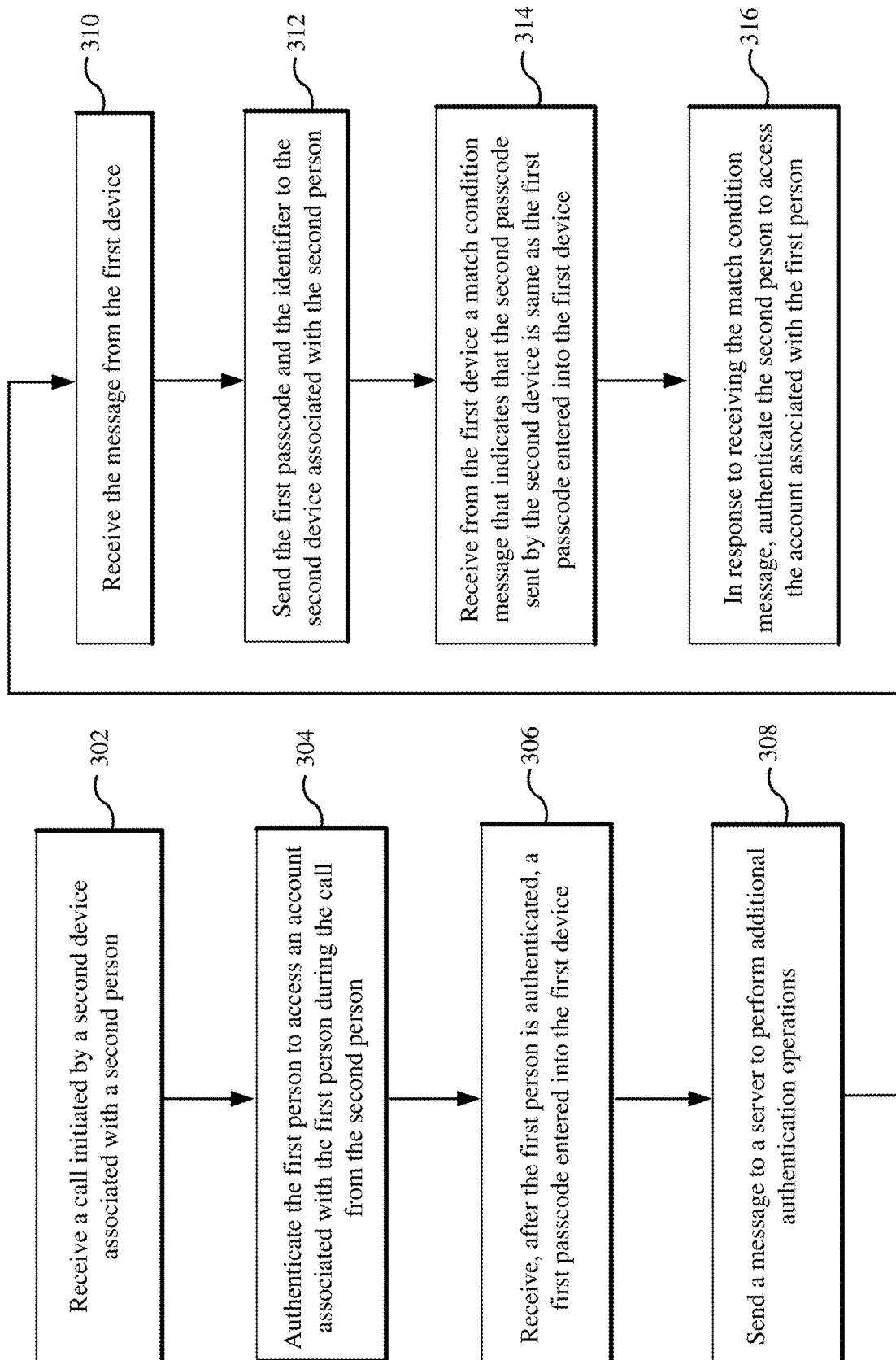


FIG. 2

**FIG. 3**

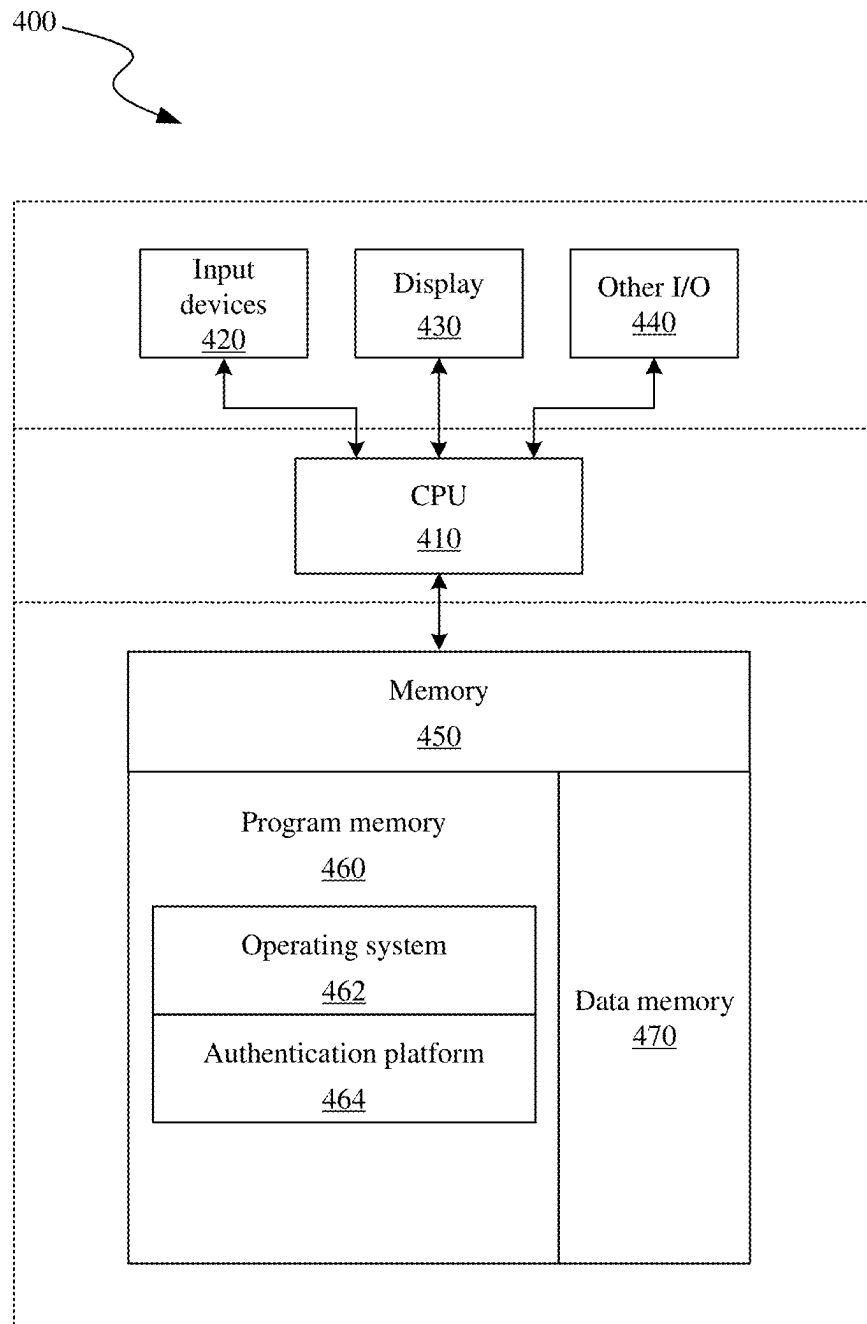


FIG. 4

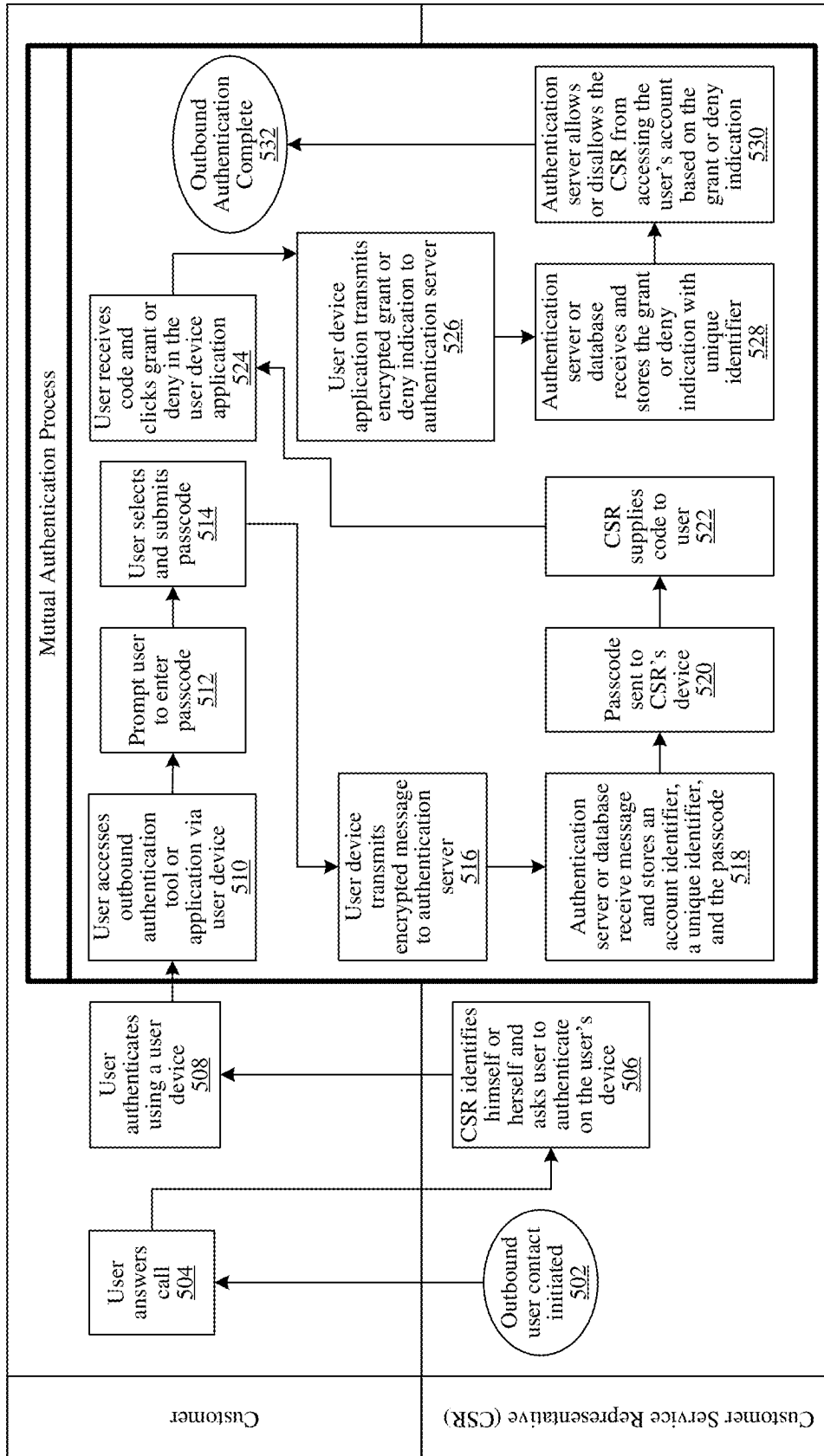


FIG. 5

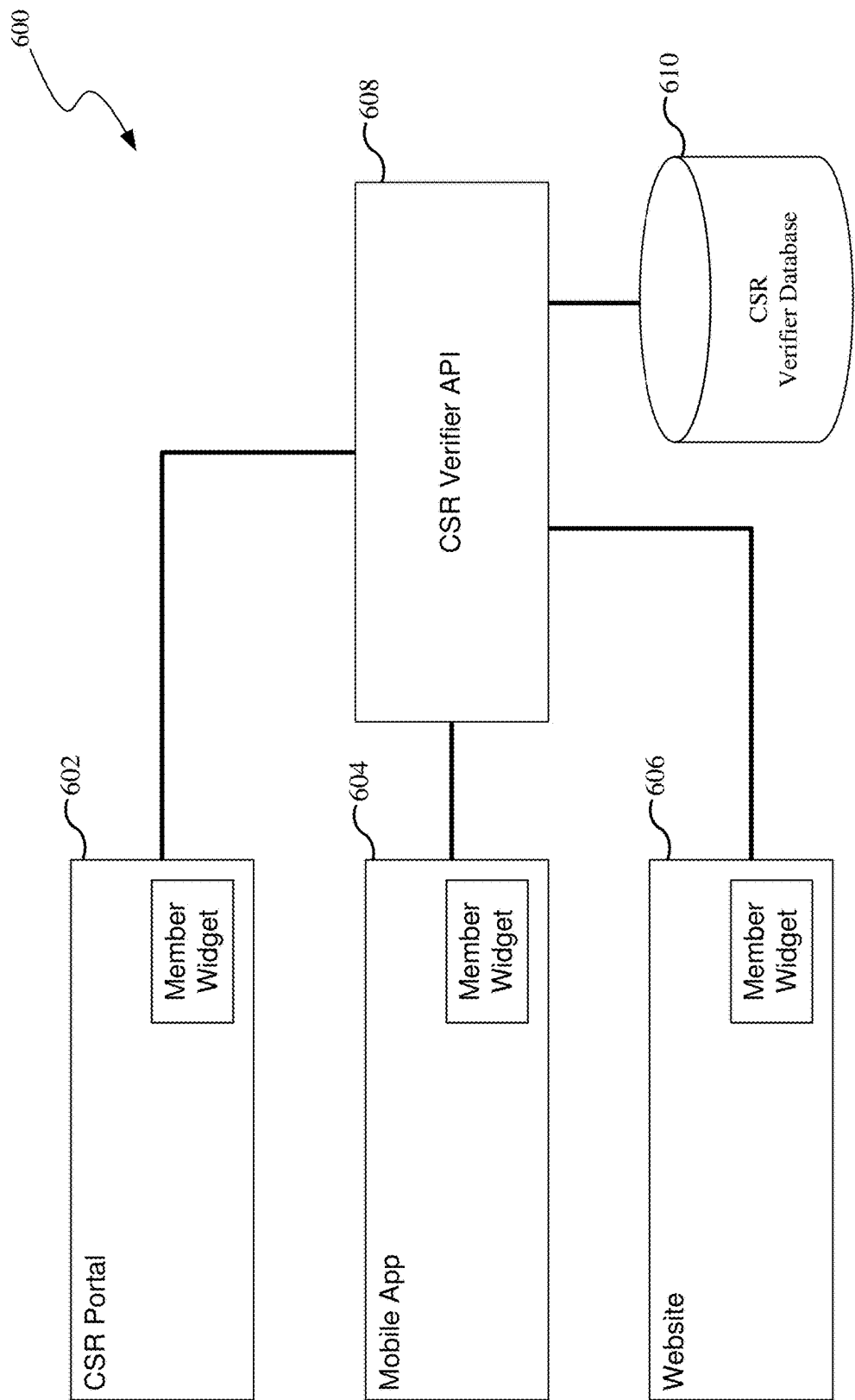


FIG. 6

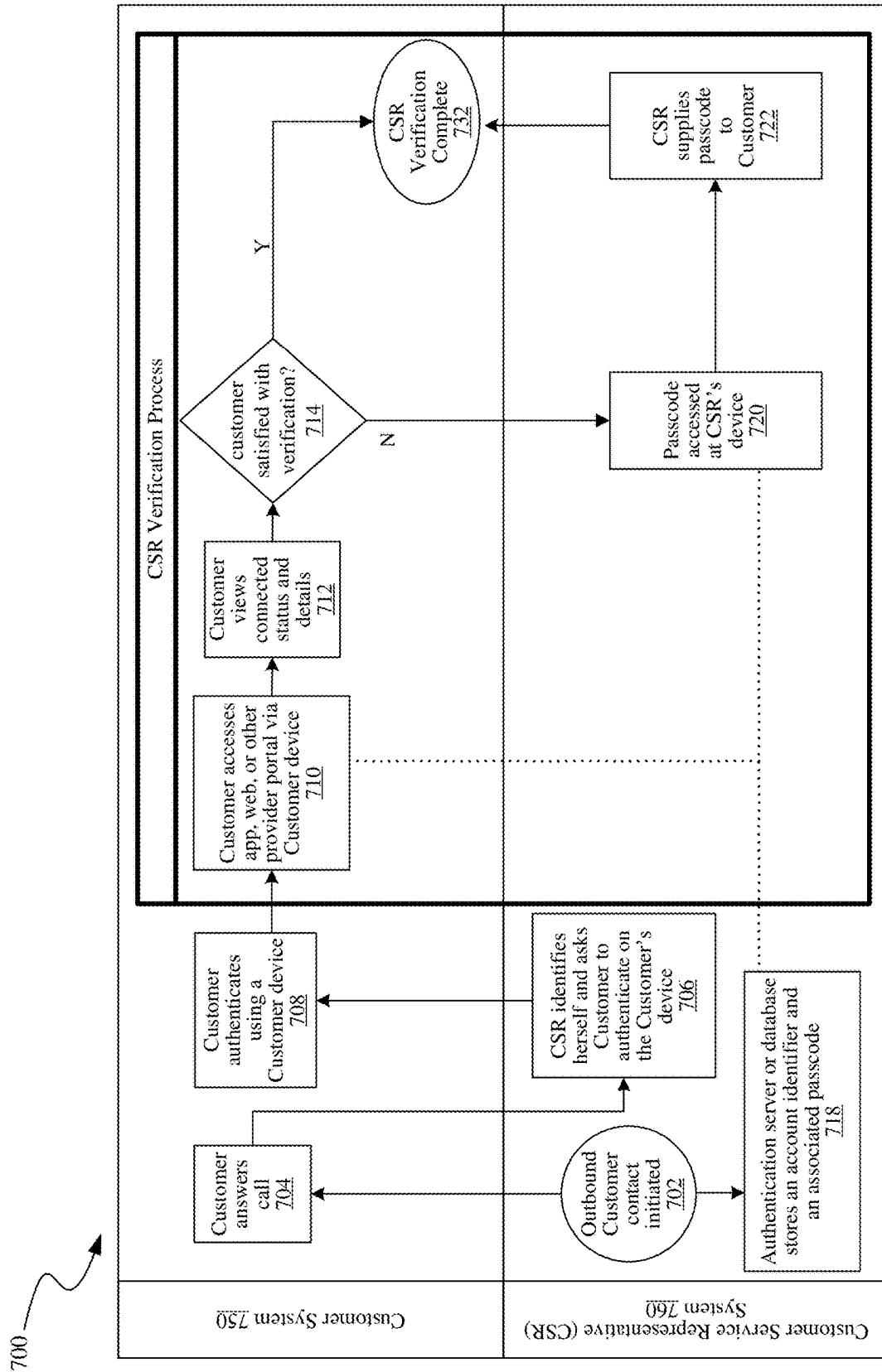


FIG. 7

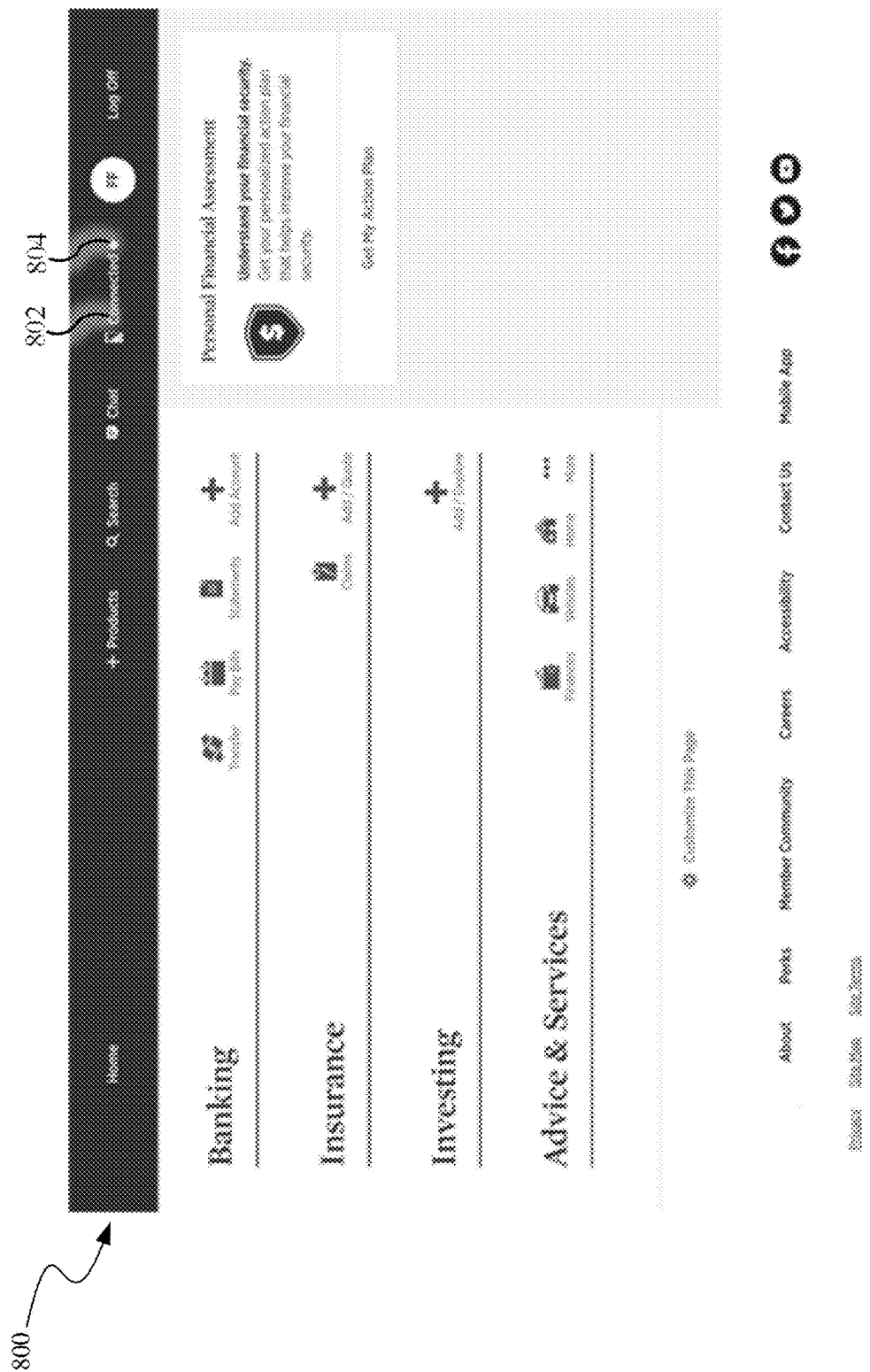


FIG. 8A

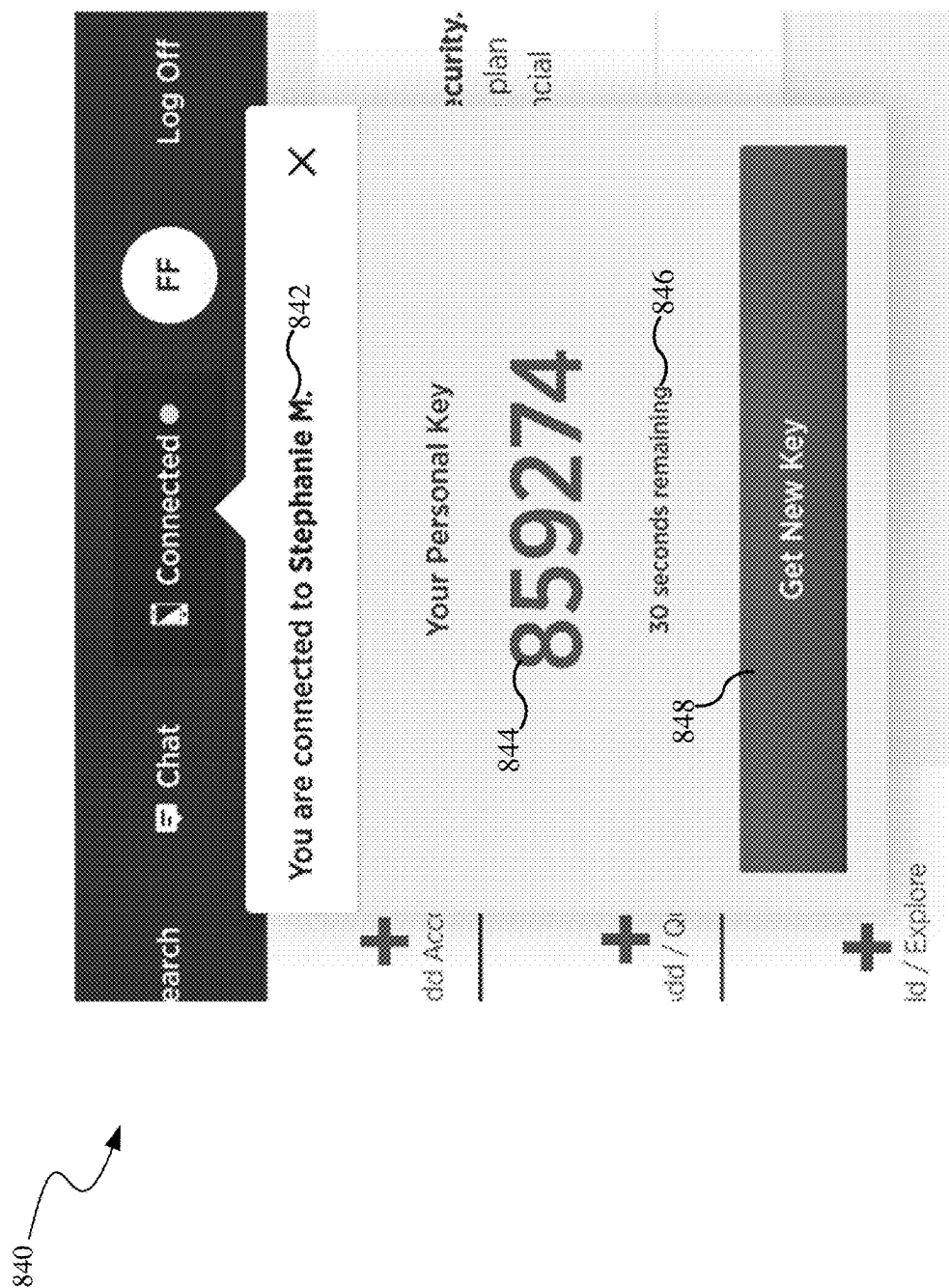


FIG. 8B

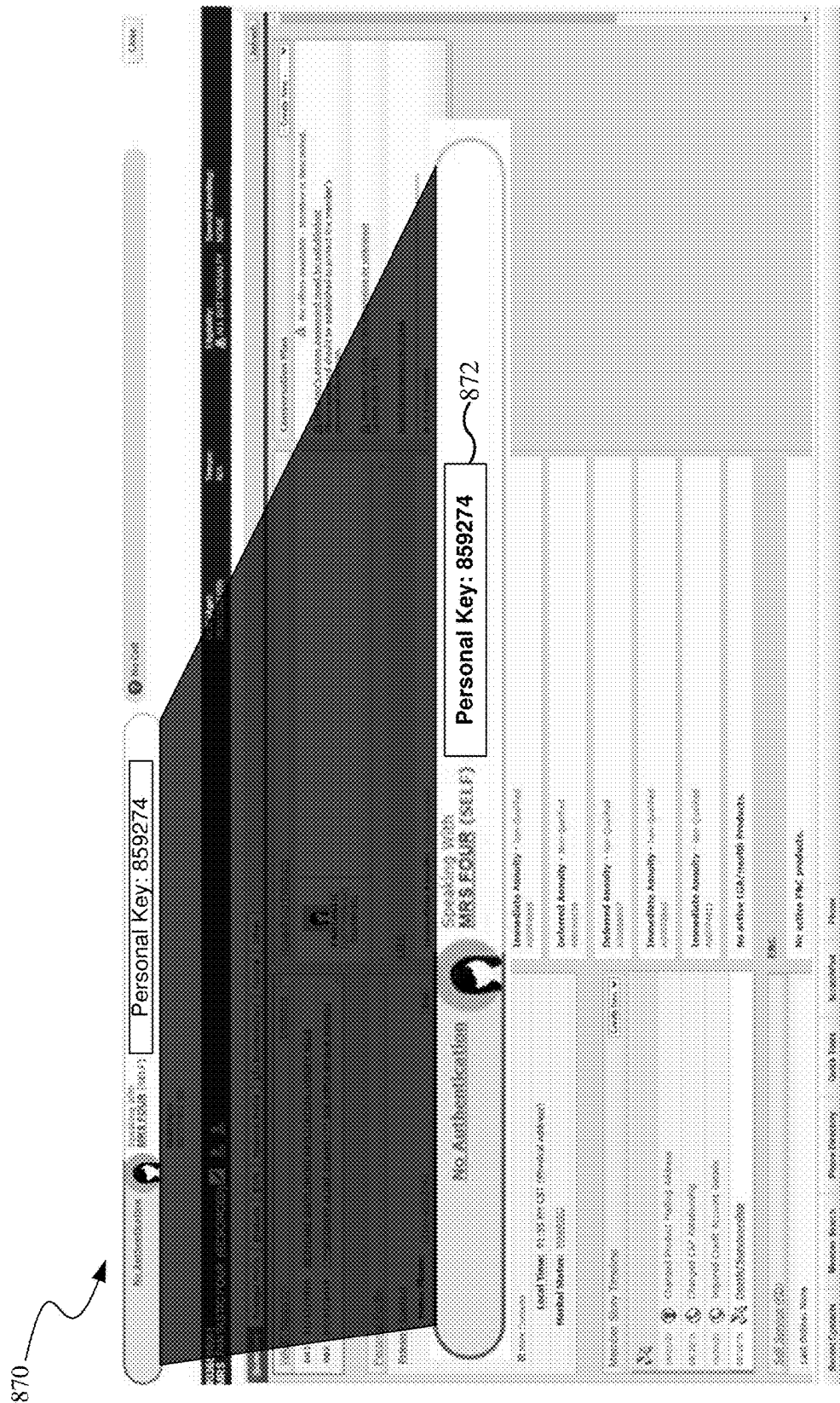


FIG. 8C

1

MUTUAL AUTHENTICATION SYSTEM**CROSS-REFERENCE TO RELATED APPLICATIONS**

This application claims priority to U.S. Provisional Patent Application No. 62/829,569, entitled “MUTUAL AUTHENTICATION SYSTEM”, which was filed on Apr. 4, 2019, and is a Continuation-in-Part of U.S. patent application Ser. No. 16/837,921, entitled “MUTUAL AUTHENTICATION SYSTEM”, which was filed on Apr. 1, 2020, the contents of each of which are incorporated by reference in their entirety herein.

TECHNICAL FIELD

This disclosure is directed generally to systems, methods, and apparatus for performing authentication.

BACKGROUND

When a customer calls an organization’s customer service phone number, he or she is asked to provide certain personal information about him or her so that a customer service representative can determine that the customer is who he or she says. In this way, a customer service representative can authenticate the identity of the customer calling. In some cases, customer service representatives call customers for marketing purposes (e.g., to sell additional products or finalize transaction), for notification purposes (e.g., to notify a customer of a suspected credit card fraud) or to collect information for a service or product they are providing. Customers who receive such calls may implicitly trust the customer service representative at least because the customer service representative’s claim that he or she belongs to a trustworthy organization (e.g., the customer’s bank) or because of the reason for the customer service perspective’s call (e.g., to notify of a credit card fraud). Fraudsters know about this phenomenon and call the customers pretending to be affiliated with the organization that the customer trusts. Thus, customers who receive such calls are susceptible to having their personal sensitive information stolen by the fraudsters.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1A shows an example overview of operations performed in a mutual authentication system.

FIG. 1B shows an example block diagram of a mutual authentication system.

FIG. 2 shows an example sequence diagram of the operations performed by devices in the mutual authentication system.

FIG. 3 is an example flow diagram of a mutual authentication process.

FIG. 4 is a block diagram illustrating an overview of devices on which some implementations of the authentication server or customer device (or user device) can operate.

FIG. 5 is an example implementation of a flow diagram of a mutual authentication process.

FIG. 6 is a block diagram illustrating an overview of entities in a CSR verification system.

FIG. 7 is an example implementation of a flow diagram of a CSR verification process.

FIG. 8A is an example user interface for a provider portal for a CSR verification system showing a connected status.

2

FIG. 8B is an example user interface for provider portal for a CSR verification system showing a CSR identifier and personal key.

FIG. 8C is an example user interface for a MSR portal for a CSR verification system.

The techniques introduced here may be better understood by referring to the following Detailed Description in conjunction with the accompanying drawings, in which like reference numerals indicate identical or functionally similar elements. Moreover, while the technology is amenable to various modifications and alternative forms, specific embodiments have been shown by way of example in the drawings and are described in detail below. The intention, however, is not to limit the technology to the particular embodiments described. On the contrary, the technology is intended to cover all modifications, equivalents, and alternatives falling within the scope of the technology as defined by the appended claims.

DETAILED DESCRIPTION

When a customer receives a call from a customer service representative (CSR) of a trustworthy organization (e.g., the customer’s bank) the customer is unable to verify that the CSR is who he or she says. In some cases, fraudsters have been known to steal personal information and use it for nefarious purposes (e.g., taking out loans, filing fake tax returns, having a credit card sent to the fraudster’s address). In a specific example, a fraudster can steal account login and password information that belongs to a customer, log into the customer’s account, initiate a transaction that triggers a one-time code (OTC) being sent to the customer’s mobile device, and then call the customer pretending to be the CSR to obtain the OTC. The fraudster can then use the OTC for authentication and proceed with a transaction.

To address at least this problem, this patent document describes technology that can allow two persons to perform mutual authentication when a first person (e.g., a CSR) calls a second person (e.g., a customer). For example, after a second person receives the call, the second person is asked to authenticate himself or herself using a user device (e.g., via a mobile device application or via a web browser). After the second person logs into his or her account, the second person can input on the user device a one-time passcode to authenticate the first person. The user device sends the passcode to a server that allows the first person to read back the inputted one-time passcode to the second person. Upon receiving the inputted one-time passcode, the second person can use his or her user device to indicate that the one-time passcode is correct so that the second person can be authenticated to access the first person’s account. In this way, the second person is authenticated as well because the first person verifies that the second person accessed (e.g., in some cases provided authentication information to obtain access) to the mobile application or web portal to input the one-time passcode.

To further address at least this problem, this patent document describes technology that can allow a CSR verification process when a first person (e.g., a CSR) calls a second person (e.g., a customer). The CSR Verification System helps customers feel secure that the person they are talking to is an agent of the provider the CSR indicates. This is done by 1) adding an indicator (such as a “connected” button and a green pulsating “Online Now” indicator) to the customer’s UI and 2) when a customer selects the indicator, it can reveal the name of the CSR and a time sensitive personal key (which is visible to the CSR in a CSR portal),

3

allowing the CSR to read the number back to the customer for further security. For example, when the call is initiated, a CSR Verification System logs details of the call including an identification of the CSR making the call (e.g., her name) and a link between the call and a profile of the customer. When the customer receives the call and the CSR introduces herself, the customer can access a provider portal associated with the CSR (e.g., a mobile app or website) which is generated, based on the call detail log linking the customer's profile to the call, to include a UI showing that someone from that provider is on a call with the customer and the CSR's identifier. If the customer wants a further verification, the customer can access a personal key via the provider portal (e.g., a unique key that is regenerated and provided to the UI every 30 seconds). The CSR can also be provided the current version of the personal key via a CSR portal and can read the personal key to the customer-verifying that the CSR is associated with the provider and thus verifying the CSR to the customer.

In this patent document, the terms "customer service representative" ("CSR") and "customer" are used to simplify the description of the example mutual authentication techniques. However, these terms are not meant to be exclusive or limiting. The mutual authentication and CSR verification techniques described in this patent document can be applied in many other contexts where a caller calls a user of an organization. For example, a person can verify that it is indeed a governmental agency calling to verify benefits or obtain information when a governmental agency calls the person.

FIG. 1A shows an example overview of operations performed in a mutual authentication system and/or a CSR Verification System 100. In an example scenario, a CSR 106 can initiate a call to speak to a customer 102. In some implementations, the CSR Verification System 100 can record an indication of the call in a profile of the customer 102, indicating that the CSR 106 is on a call with the customer and an identifier for the CSR 106. On the call, the CSR 106 can identify himself or herself as belonging to an organization or company. The CSR 106 can ask the customer 102 to authenticate himself or herself on a device associated with the customer 102. At operation 1, the customer 120 logs into his or her account to provide a passcode to an authentication server 104. The passcode can include numbers, letter, symbols, or any combination thereof. For example, the passcode may be 123456 or Bird.

At operation 1, the customer 102 can log into a provider portal for his or her account in a variety of ways. For example, the customer can log into his or her account on a web browser operating on the customer's computer or on the customer's mobile device (e.g., smartphone). In another example, the customer 102 can log into his or her account on an application operating on the customer's mobile device. By logging into the customer's account, the customer can authenticate himself or herself. Once the customer logs into his or her account, the customer's device can provide a passcode to the authentication server 104. In some implementations, instead of the customer's device providing the passcode to the authentication server 104, the authentication server 104 can have generated the passcode and provided an indication of the connected call, the CSR's identifier, and the passcode to be included in the UI of the provider portal into which the customer has logged in. When the customer logs into her account, she can immediately see that someone from this organization is on a call with her. In some cases, this may be sufficient verification and the call can proceed without further verification.

4

At operation 2, the authentication server 104 sends the passcode to the CSR's computer. At operation 3, the CSR 106 can read back the passcode to the customer 104 via the call or the CSR 106 can input the code such that it appears on the customer's mobile application, web browser, in a push notification or text message. In some cases, this may be sufficient verification and the call can proceed without further verification.

In other cases, at operation 4, the customer 102 can use his or her device to send to the authentication server 104 an indication as to whether the CSR is granted to denied access to the customer's account. For example, if the customer 102 determines that the passcode repeated or sent by the CSR matches the passcode entered by the customer 102, then the customer can press a "grant" button on a graphical user interface (GUI) displayed on the customer's device to indicate to the authentication server 104 that the CSR is granted access to the customer's account. Conversely, if the customer 102 determines that the passcode repeated by the CSR does not match the passcode entered by the customer 102, then the customer can press a "deny" button on a graphical user interface (GUI) displayed on the customer's device to indicate to the authentication server 104 that the CSR is denied access to the customer's account.

At operation 5, the authentication server 140 can either grant or deny the CSR access to the customer's account based on the indication (e.g., grant/deny) received from the customer's device.

FIG. 1B shows an example block diagram of a mutual authentication system 100 that includes a CSR's computer 110 and/or phone that can initiate a call to speak to a customer via the customer's device 120a-120c (e.g., laptop, phone, wearable, or smartphone). The call from the CSR's computer 110 or phone can be sent to the customer's device 120a-120c via a communication network 130. The communication network 130 may include the Internet, a cellular network, a public switched telephone network (PSTN), a voice over Internet Protocol (VOIP) network, or any combination thereof. This patent document describes various operations performed by an authentication server 104. In some embodiments, a single server can perform the operations described for the authentication server 104. In some other embodiments, multiple servers can perform the operations described for the authentication server 104. As further explained in this patent document, the authentication server 104 can store information to and retrieve information from the database 108.

FIG. 2 shows an example sequence diagram of the operations performed by devices in the mutual authentication system. The operations described in steps 202 to 216 are performed during the time that the CSR is on a call (or other interactions) with the customer. At step 202, a CSR's computer or phone device can initiate a call (e.g., phone call) to a customer device. At operation 204, the customer is authenticated to access his or her account via the device based on information provided by the customer. For example, the customer may authenticate himself or herself by entering his or her login information (e.g., biometric information, or personal identification number, or username and password) in a web browser or in a mobile application operating on the customer's device.

The customer may be authenticated using one of several authentication techniques. In some embodiments, the customer's device may compare the login information provided by the customer to login information previously stored on the customer device. In such embodiments, if the customer's device determines that the provided login information is the

5

same as the previously stored login information, then the customer device may authenticate the customer to access his or her account on the customer device. In some other embodiments, the customer's device may send the login information to an authentication server so that the authentication server can compare the login information provided by the customer to login information previously stored on a database associated with the authentication server. In such embodiments, if the authentication server determines that the provided login information is the same as the previously stored login information, then the authentication server can send a message to the customer device indicating that the customer is authenticated to access his or her account on the customer device. In yet some other embodiments, a customer may be authenticated by other interactions such as receiving a text message with a one-time code (OTC) and then entering that OTC in the customer device.

After the customer logs into his or her account, the customer device may show an option for the customer to authenticate the customer service representative (e.g., on a separate tab in a mobile application, in a pop-up message on a web browser, in a push notification). Upon selection of that option, at operation **206**, the customer device prompts the customer to provide a passcode. After the customer enters the passcode, the customer device can generate a message that includes the passcode and an account identifier associated with the account of the customer (e.g., account number, member number or login information). At operation **208**, the customer device sends the message to the authentication server. In some embodiments, the customer device encrypts the message prior to sending the message to the authentication server.

At operation **210**, the authentication server sends the passcode to the CSR's computer. The authentication server may send the passcode to the CSR's computer using one of several techniques. For example, once the authentication server receives the passcode, it sends the passcode to the CSR's computer without receiving any further request from the CSR's computer. In another example, after the customer mentions to the CSR that he or she has entered the passcode in the customer device, the CSR may request and obtain the passcode from the authentication server. In some embodiments, after the passcode is received by the CSR's computer, the passcode is display on the CSR's computer so that the CSR can verbally mention the passcode to the customer over the call. In some other embodiments, after the passcode is received by the CSR's computer, the passcode is sent by the CSR's computer to the mobile application operating on the customer's device.

At operation **214**, the customer device displays or audibly presents to the customer the passcode sent by the CSR or the CSR's computer. The customer can compare the password that he or she entered at operation **206** with the passcode that was sent at operation **212**. If the customer determines that the two passcodes match, the customer can select a "grant" button on a GUI operating on the customer device. After the customer clicks the "grant" button, the customer device sends a match condition message to the authentication server at operation **214**, where the match condition message indicates the two passcodes were determined to be the same. The match condition message may be another message (e.g., a data packet) that includes information to indicate that the two passcodes were determined to be the same.

Conversely, if the customer determines that the two passcodes do not match, the customer can select a "deny" button on a GUI operating on the customer device. After the customer clicks the "deny" button, the customer device

6

sends a non-match condition message to the authentication server at operation **214**, where the non-match condition message indicates the two passcodes were determined to be different. The non-match condition message may be another message (e.g., a data packet) that includes information to indicate that the two passcodes are different.

In some embodiments, instead of using "grant" and "deny" buttons, the GUI may have two buttons that state "passcodes are same" and "passcodes are different." The selection of either the "passcodes are same" or "passcodes are different" buttons by the customer can trigger to the customer device to respectively send either the match condition message or the non-match condition message to the authentication server. In some embodiments, the customer device can encrypt the match condition message or the non-match condition message prior to sending any one of them to the authentication server.

At operation **216**, the authentication server can determine either to allow the CSR access to the customer's account or to deny the CSR access to the customer's account. In response to receiving the match condition message, which is sent to the authentication server when the two passcodes are the same, the authentication server authenticates the CSR to access the account associated with the customer. In some embodiments, the authentication server can send the account identifier to the CSR's computer at step **216** after receiving the match condition message. In some other embodiments, the authentication server can send the account identifier to the CSR's computer at operation **210**, and at operation **216** allows the CSR's computer to access the account associated with the account identifier.

In response to receiving the non-match condition message, which is sent to the authentication server when the two passcodes are different, the authentication server denies the CSR access to the account associated with the customer. In some embodiments, the authentication server can send the account identifier to the CSR's computer at operation **216** after receiving the match condition message. In some other embodiments, the authentication server can send the account identifier to the CSR's computer at operation **210**, and at operation **216** allows the CSR's computer to access the account associated with the account identifier.

In some embodiments, after operation **206** and prior to operation **208**, the customer device may generate a unique identifier (e.g., randomly generate ID) that can be used to identify the call with the CSR. The unique identifier can be included in the message sent to the authentication server at operation **208**. The authentication server can store the unique identifier in a database along with either the word "grant" or the word "deny." For example, if the authentication server receives a match condition message at step **214**, the authentication server can log this event by storing the word "grant" next to the unique identifier associated with the call. In some embodiments, an employee identifier of the CSR can also be stored next to the unique identifier. In this way, a log can be generated to show the calls on which CSRs were allowed to access customer accounts, and the calls on which CSRs are denied access to customer accounts.

In some embodiments, the mutual authentication system may be designed to authenticate a CSR to access a customer account within a pre-determined duration of time after an event is triggered. For example, after the authentication server receives the message at operation **208**, the operations performed at operations **210** to **214** should be performed within 2 minutes. If, for example, a match condition message is received by the authentication server at 2 minutes and 10 seconds after the message is received at operation **208**,

the authentication server can still deny the CSR access to the customer's account. Thus, a message received at operation **208** can be stored on the authentication server or on a database associated with the authentication server for a pre-determined duration of time (e.g., 2 minutes), where the CSR can be authenticated to access a customer's account if the match condition message is received by the authentication server within the pre-determined duration of time.

In some embodiments, the operations described in FIG. **2** can be performed only if the customer device and/or a mobile application on the customer device has been previously registered with the authentication server. In such embodiments, once a customer device and/or mobile application is registered, it can be qualified to perform the type of mutual authentication described in this patent document.

FIG. **3** is an example flow diagram of a mutual authentication process. Operations **302** to **308** are performed by a first device (e.g., smartphone or laptop) associated with a first person (e.g., a customer), and operations **310** to **316** are performed by a server (e.g., an authentication server). At the receiving operation **302**, the first device receives a call initiated by a second device (e.g., a computer and/or phone) associated with a second person (e.g., a customer service representative).

At the authentication operation **304**, the first device authenticates the first person to access an account associated with the first person during the call from the second person. The first person is authenticated based on user information received via the first device. In some embodiments, the user information includes a personal identification number of the first person, or biometric information of the first person, or a user name and a password of the first person.

At the receiving operation **306**, the first device receives, after the first person is authenticated, a first passcode entered into the first device. At the sending operation **308**, the first device sends a message to a server to perform additional authentication operations, wherein the message includes an identifier associated with the account of the first person and the first passcode. In some embodiments, the message is encrypted by the first device prior to sending the message to the server.

At the receiving operation **310**, the server (e.g., authentication server) receives the message from the first device. In some embodiments, the message includes a second identifier randomly generated by the first device, where the second identifier uniquely identifies the call when the first person is authenticated. In such embodiments, the server is configured to store the second identifier and either a grant designation in response to authenticating the second person to access the account or a deny designation in response to denying the second person access to the account. In some embodiments, the grant designation or the deny designation are stored in a manner that indicates a relationship with the second identifier. For example, the words "grant" or "deny" may be stored on a database next to the second identifier.

At the sending operation **312**, the server sends the first passcode and the identifier to the second device associated with the second person, where a second passcode is sent by the second device via the call to the first device. In some embodiments, the first passcode and the second passcode include letters, numbers, or symbols.

At the receiving operation **314**, the server receives from the first device a match condition message that indicates that the second passcode sent by the second device is same as the first passcode entered into the first device. At the authenticating operation **316**, the server, in response to receiving the

match condition message, authenticates the second person to access the account associated with the first person.

In some embodiments, the server of FIG. **3** is further configured to receive from the first device a non-match condition message that indicates that the second passcode sent by the second device is different from the first passcode entered into the first device. If the server receives the non-match condition message, the server denies the second person access to the account associated with the first person. In some embodiments, the first device is configured to encrypt the match condition message or the non-match condition message prior to sending the match condition message or the non-match condition message to the server.

In some embodiments, the message is stored on the server or on a database associated with a server for a pre-determined duration of time, and the second person is authenticated in response to receiving the match condition message within the pre-determined duration of time. In some embodiments, the first person is authenticated via an application operating on the first device or via an Internet browser operating on the first device.

FIG. **4** is a block diagram illustrating an overview of devices on which some implementations of the authentication server or customer device (or user device) can operate. The devices can comprise hardware components of a device **400**, such as the authentication server or customer device, both of which can include an authentication platform **464** that determine whether a person is authenticated to access an account. For instance, one version of the authentication platform **464** operating on the authentication server can determine whether a customer service representative, as described in this patent document, is authenticated to access a customer's account. And, another version of the authentication platform **464** operating on the customer device can determine whether a customer, as described in this patent document, is authenticated to access the customer's device and to provide a passcode to the authentication servers for further authentication related operations.

Device **400** can include one or more input devices **420** that provide input to the CPU (processor) **410**, notifying it of actions. The actions are typically mediated by a hardware controller that interprets the signals received from the input device and communicates the information to the CPU **410** using a communication protocol. Input devices **420** include, for example, a mouse, a keyboard, a touchscreen, an infrared sensor, a touchpad, a wearable input device, a camera- or image-based input device, a microphone, or other user input devices.

CPU **410** can be a single processing unit or multiple processing units in a device or distributed across multiple devices. CPU **410** can be coupled to other hardware devices, for example, with the use of a bus, such as a PCI bus or SCSI bus. The CPU **410** can communicate with a hardware controller for devices, such as for a display **430**. Display **430** can be used to display text and graphics. In some examples, display **430** provides graphical and textual visual feedback to a person operating the device **400**. In some implementations, display **430** includes the input device as part of the display, such as when the input device is a touchscreen or is equipped with an eye direction monitoring system. In some implementations, the display is separate from the input device. Examples of display devices are: an LCD display screen; an LED display screen; a projected, holographic, or augmented reality display (such as a heads-up display device or a head-mounted device); and so on. Other I/O devices **440** can also be coupled to the processor, such as a network card, video card, audio card, USB, FireWire or other external

device, camera, printer, speakers, CD-ROM drive, DVD drive, disk drive, or Blu-Ray device.

In some implementations, the device **400** also includes a communication device capable of communicating wirelessly or wire-based with a network node (e.g., a server) or with a user device (e.g., a laptop, desktop, or mobile device) or with one or more computers (e.g., desktop or laptop) associated with the customer service representatives. The communication device can communicate with another device or a server through a network using, for example, TCP/IP protocols. Device **400** can utilize the communication device to distribute operations across multiple network devices.

The CPU **410** can have access to a memory **450**. A memory includes one or more of various hardware devices for volatile and non-volatile storage, and can include both read-only and writable memory. For example, a memory can comprise random access memory (RAM), CPU registers, read-only memory (ROM), and writable non-volatile memory, such as flash memory, hard drives, floppy disks, CDs, DVDs, magnetic storage devices, tape drives, device buffers, and so forth. A memory is not a propagating signal divorced from underlying hardware; a memory is thus non-transitory. Memory **450** can include program memory **460** that stores programs and software, such as an operating system **462** and authentication platform **464**. The authentication platform **464** may include modules or processes or methods or user interfaces (UIs) for authentication a person to access an account, as described in FIGS. **1**, **2**, **3**, **5**, **6**, **7** and **8** of this patent document and/or in the various embodiments in this patent document. Thus, for example, the memory **450** may store instructions that upon execution by CPU **410** configure the device **400** to perform the operations described for the authentication server in FIGS. **1**, **2**, **3**, **5**, **6**, **7** and **8** and/or in the various embodiments described in this patent document. In another example, the memory **450** may store instructions that upon execution by CPU **410** configure the device **400** to perform the operations described for the customer device (or user device) in FIGS. **1**, **2**, **3**, **5**, **6**, **7** and **8** and/or in the various embodiments described in this patent document. Memory **450** can also include data memory **470** that can include the various scores described in this patent document, which can be provided to the program memory **460** or any element of the device **400**.

Some implementations can be operational with numerous other general purpose or special purpose computing system environments or configurations. Examples of well-known computing systems, environments, and/or configurations that may be suitable for use with the technology include, but are not limited to, personal computers, server computers, handheld or laptop devices, cellular telephones, portable electronic devices such as smartphones, wearable electronics, gaming consoles, tablet devices, multiprocessor systems, microprocessor-based systems, set-top boxes, programmable consumer electronics, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, or the like.

FIG. **5** is an example implementation of a flow diagram of a mutual authentication process. The flow diagram of FIG. **5** describes a process that is designed to solve the technical problem of performing outbound authentication where a CSR calls a customer. At step **502**, a CSR calls a customer, and at step **504**, the customer answers the call. However, at step **504**, the customer may most likely not recognize the CSR or may not be able to verify that the CSR is who he or she says he or she is. At the same time, when the customer

answers the call at step **504**, the CSR may not know that the customer is who he or she says he or she is.

After the customer answers the call at step **504**, the CSR can identify himself or herself and can ask the customer to authenticate himself or herself on the customer's device. For example, the CSR may request the customer to enter his or her login information in a mobile application or a web browser operating on the customer's device.

At step **508**, the customer logs into his or her account using a customer's device, and in so doing, authenticates himself or herself. The customer may log into his or her account by providing to the customer device the customer's biometric information or by providing a username and password. The mobile application or web browser operating on the customer device may include an "outbound authentication tool" or an "outbound authentication application" link. At step **510**, the customer selects the outbound authentication tool or application link via a graphical user interface (GUI) displayed by the customer device. In response, at step **512**, the outbound authentication tool or application requests the customer to enter a passcode via the GUI. At step **514**, the user selects a passcode, which can include numbers, letter, symbols, or any combination thereof. In some embodiments, the passcode may be a four or six digit code for ease of use.

At step **516**, after the user selects and enters his or her passcode, the customer device sends an encrypted message to an authentication server. The encrypted message can include the user's account identifier, the user selected passcode, and a unique identifier that can be used to identify the ongoing call between the CSR and the customer.

At step **518**, the authentication server receives and can store in a database the account identifier, the unique identifier, and the passcode. At step **520**, the authentication server sends the passcode to a computer or device associated with the CSR. At step **522**, the CSR can read back the passcode to the customer via the call.

At step **524**, the customer device can receive the code and can visually or audibly present the code to the customer. If the customer determines that the passcode provided by the CSR matches or is the same as the passcode that the customer entered, then the customer may select a "grant" button on the GUI displayed on the customer's device. If, however, the customer determines that the passcode provided by the CSR does not match or is different from the passcode that the customer entered, then the customer may select a "deny" button on the GUI displayed on the customer's device.

At step **526**, the user device transmits an encrypted grant or deny message to the authentication server that indicates to the authentication server whether the customer has granted or denied access to the CSR to the customer's account. At step **528**, the authentication server receives the encrypted grant or deny message and stores either the word "grant" or the word "deny" next to the unique identifier to create a log as to whether the CSR was granted or denied access to the customer's account for the call associated with the unique identifier. At step **530**, the authentication server can either allow or deny the CSR from accessing the customer's account based on receiving either the grant message or the deny message. At step **532**, the outbound authentication process is completed.

FIG. **6** is a block diagram illustrating an overview of entities **600** in a CSR verification system. When a call is initiated, the CSR portal **602**, via the CSR Verifier API **608**, logs in the CSR Verifier Database **610** an identification of the CSR making the call (e.g., her name) and a link between the

11

call and a profile of the customer. This can be a result of a manual entry by the CSR or through an automated process where the CSR makes the call through the CSR Verification System and the CSR Verification System automatically updates the customer's profile. When the customer receives the call and the CSR introduces herself, the customer can access a provider portal associated with the CSR (e.g., a mobile app **604** or website **606**) which is generated, based on the call detail log in the customer's profile via CSR Verifier API **608**, to include a UI showing that someone from that provider is on a call with the customer from the CSR Verifier Database **610**. If the customer wants a further verification, the customer can access the CSR's identifier and a personal key via the provider portal **604** or **606** (e.g., a unique key that is regenerated and provided to the UI every 30 seconds from the CSR Verifier Database **610** via the CSR Verifier API **608**). The CSR can also be provided, in her CSR Portal **602**—updated via CSR Verifier API **608** from the CSR Verifier Database **610**, the current version of the personal key and can read the personal key to the customer. The customer can see that the personal key in her provider portal and the personal key provided by the CSR match, proving that the CSR is associated with the provider and thus verifying the CSR to the customer.

FIG. 7 is an example implementation of a flow diagram of a CSR verification process **700**. Portions of process **700** can be performed with a customer system **750** while other portions can be performed with a CSR system **760**.

At block **702**, a CSR initiates an outbound call to a customer. A link between the call and the customer is established, at block **718**, e.g., by registering the call record in a profile of the customer, the call record can indicate an identifier of the CSR (e.g., her name, ID number, or handle) and can include a passcode (such as a personal key which can be, e.g., a random number, word, phrase, etc., which can be periodically re-generated such as every 30 seconds). In various implementations, this link can be generated in response to the CSR entering an indication of the customer she is calling in her CSR portal or by virtue of the CSR making the call through the CSR portal which can automatically create the link with the customer's profile.

At block **704** the customer can answer the call and at block **706** the CSR can identify herself and can ask the customer to authenticate on the Customer's device, e.g., by logging into a provider portal, which the customer can do at block **710** (e.g., providing authentication credentials). The UI presented by the provider portal when the customer logs in at block **710** can include an indicator that a CSR from the provider is on a call with the customer (e.g., a "connected" button and a green pulsating "Online Now" indicator). As indicated by the dotted line, these indicators can be set by virtue of the link stored at block **718**.

At block **712**, the customer can view the connected status (and may also view call details such as the CSR's name) and, at block **714** can determine whether she is satisfied with the verification. If so, CSR verification is complete, and the call can continue at block **732**. If not, the customer can ask the CSR for further verification and the CSR verification process can continue at block **720**.

At block **720**, the CSR can access a CSR portal which can show the current version of the passcode for the call as stored at block **718** (as indicated by the dotted line). At block **722**, the CSR can supply the passcode to the customer, e.g., by reading it or causing it to be sent to the customer, e.g., via text message, email, push notification, etc. The customer can verify that this passcode matches one shown in the UI of the provider portal the customer accessed at block **710**. This

12

passcode can be regenerated upon the customer's command (e.g., pressing a button in the UI) or periodically (e.g., every 30 seconds) and updated to the customer's provider portal and the CSR portal. Once the customer verifies that the provided passcode matches the one shown in her provider portal, CSR verification is complete, and the call can continue at block **732**.

FIG. 8A is an example user interface **800** for a provider portal for a CSR verification system showing a connected status. Example user interface **800** can be an interface that a customer sees when they log into a provider portal when they receive a call from a CSR. If a legitimate CSR from the provider is on a call with the customer, the user interface **800** can include "connected" status indicator **802** and icon indicator **804** indicating the provider has logged an active call with the customer. FIG. 8B is an example user interface **840** for provider portal for a CSR verification system showing a CSR identifier and personal key. Example user interface **840** can be provided when the customer selects the connected status indicator **802**, which can provide an identifier **842** (e.g., name) of the CSR on the call and a personal key **844** that the CSR can read back to the customer to verify herself. The user interface **840** can also include a timer **846** indicating when the current version of the personal key **844** will expire and be regenerated and a control **848** that the customer can activate to cause the CSR Verification System to regenerate a new personal key before the timer **846** expires. FIG. 8C is an example user interface **870** for a MSR portal for a CSR verification system. For clarity purposes, the example user interface **870** illustrates a portion zoomed in, which includes the current active personal key **872**, which the CSR can read back to the customer to verify herself.

In an example embodiment, the above-described methods are embodied in the form of processor-executable code and stored in a computer-readable program medium. Thus, a non-transitory machine-readable medium having machine executable instructions stored thereon that, when executed by one or more processors, direct the one or more processors to perform a method described in FIGS. 1, 2, 3, 5, 6, 7 and 8, and/or in the various embodiments described in this patent document.

Those skilled in the art will appreciate that the components illustrated in FIG. 1-8 described above, and in each of the flow diagrams, may be altered in a variety of ways. For example, the order of the logic may be rearranged, sub-steps may be performed in parallel, illustrated logic may be omitted, other logic may be included, etc. In some implementations, one or more of the components described above can execute one or more of the processes described above.

CONCLUSION

Unless the context clearly requires otherwise, throughout the description and the claims, the words "comprise," "comprising," and the like are to be construed in an inclusive sense, as opposed to an exclusive or exhaustive sense; that is to say, in the sense of "including, but not limited to." As used herein, the terms "connected," "coupled," or any variant thereof means any connection or coupling, either direct or indirect, between two or more elements; the coupling or connection between the elements can be physical, logical, or a combination thereof. Additionally, the words "herein," "above," "below," and words of similar import, when used in this application, refer to this application as a whole and not to any particular portions of this application. Where the context permits, words in the above Detailed Description

using the singular or plural number may also include the plural or singular number respectively.

Several implementations of the disclosed technology are described above in reference to the figures. The computing devices on which the described technology may be implemented can include one or more central processing units, memory, user devices (e.g., keyboards and pointing devices), output devices (e.g., display devices), storage devices (e.g., disk drives), and network devices (e.g., network interfaces). The memory and storage devices are computer-readable storage media that can store instructions that implement at least portions of the described technology. In addition, the data structures and message structures can be stored or transmitted via a data transmission medium, such as a signal on a communications link. Various communications links can be used, such as the Internet, a local area network, a wide area network, or a point-to-point dial-up connection. Thus, computer-readable media can comprise computer-readable storage media (e.g., “non-transitory” media) and computer-readable transmission media.

As used herein, being above a threshold means that a value for an item under comparison is above a specified other value, that an item under comparison is among a certain specified number of items with the largest value, or that an item under comparison has a value within a specified top percentage value. As used herein, being below a threshold means that a value for an item under comparison is below a specified other value, that an item under comparison is among a certain specified number of items with the smallest value, or that an item under comparison has a value within a specified bottom percentage value. As used herein, being within a threshold means that a value for an item under comparison is between two specified other values, that an item under comparison is among a middle specified number of items, or that an item under comparison has a value within a middle specified percentage range.

As used herein, the word “or” refers to any possible permutation of a set of items. For example, the phrase “A, B, or C” refers to at least one of A, B, C, or any combination thereof, such as any of: A; B; C; A and B; A and C; B and C; A, B, and C; or multiple of any item, such as A and A; B, B, and C; A, A, B, C, and C; etc.

The above Detailed Description of examples of the technology is not intended to be exhaustive or to limit the technology to the precise form disclosed above. While specific examples for the technology are described above for illustrative purposes, various equivalent modifications are possible within the scope of the technology. For example, while processes or blocks are presented in a given order, alternative implementations may perform routines having steps, or employ systems having blocks, in a different order, and some processes or blocks may be deleted, moved, added, subdivided, combined, and/or modified to provide alternative or subcombinations. Each of these processes or blocks may be implemented in a variety of different ways. Also, while processes or blocks are at times shown as being performed in series, these processes or blocks may instead be performed or implemented in parallel, or may be performed at different times. Further any specific numbers noted herein are only examples: alternative implementations may employ differing values or ranges.

The teachings of the technology provided herein can be applied to other systems, not necessarily the system described above. The elements and acts of the various examples described above can be combined to provide further implementations of the technology. Some alternative implementations of the technology may include not only

additional elements to those implementations noted above, but also may include fewer elements.

These and other changes can be made to the technology in light of the above Detailed Description. While the above description describes certain examples of the technology, and describes the best mode contemplated, no matter how detailed the above appears in text, the technology can be practiced in many ways. Details of the system may vary considerably in its specific implementation, while still being encompassed by the technology disclosed herein. As noted above, particular terminology used when describing certain features or aspects of the technology should not be taken to imply that the terminology is being redefined herein to be restricted to any specific characteristics, features, or aspects of the technology with which that terminology is associated. In general, the terms used in the following claims should not be construed to limit the technology to the specific examples disclosed in the specification, unless the above Detailed Description section explicitly defines such terms. Accordingly, the actual scope of the technology encompasses not only the disclosed examples, but also all equivalent ways of practicing or implementing the technology under the claims.

To reduce the number of claims, certain aspects of the technology are presented below in certain claim forms, but the applicant contemplates the various aspects of the technology in any number of claim forms. For example, while only one aspect of the technology is recited as a computer-readable medium claim, other aspects may likewise be embodied as a computer-readable medium claim, or in other forms, such as being embodied in a means-plus-function claim. Any claims intended to be treated under 35 U.S.C. § 112 (f) will begin with the words “means for”, but use of the term “for” in any other context is not intended to invoke treatment under 35 U.S.C. § 112 (f). Accordingly, the applicant reserves the right to pursue additional claims after filing this application to pursue such additional claim forms, in either this application or in a continuing application.

We claim:

1. A method of performing customer service representative (CSR) call verification, the method comprising:
 - receiving a first indication of A) a call initiated by a CSR of a provider and B) a customer to which the call was placed;
 - recording, based on the first indication and in a profile of the customer, a second indication of the call, wherein the second indication of the call is associated with the CSR who initiated the call;
 - receiving a login request from the customer to a provider portal of the provider and, in response, serving data for a first user interface of the provider portal, wherein the data includes a call status indicator specifying that there is an ongoing call between an agent of the provider and the customer, based on the second indication of the call;
 - as a result of selection of the call status indicator via the first user interface, serving additional data for the first user interface of the provider portal, the additional data including i) the second indication of the call, ii) a third indication of the CSR who initiated the call, and iii) a generated personal key for the call; and
 - providing data for a second user interface displayed to the CSR who initiated the call, wherein the second user interface includes the generated personal key; wherein the CSR provides the generated personal key to the customer to verify the call.

15

2. The method of claim 1, wherein the second indication of the call is provided automatically by a CSR verification system when the CSR initiates the call via the CSR verification system.

3. The method of claim 1, wherein the recording is done in a CSR verification database via an API accessible by each of: a CSR portal that can present the second user interface, a mobile application that can present a first version of the first user interface, and a website that can present a second version of the first user interface.

4. The method of claim 1, wherein the first user interface includes, based on the association between the call and the CSR who initiated the call, an identifier of the CSR who initiated the call.

5. The method of claim 1, wherein the generated personal key for the call is a randomly generated number or phrase.

6. The method of claim 1, wherein the generated personal key for the call is updated after a set period and the updated version of the personal key is provided for display in the first user interface and the second user interface.

7. The method of claim 1, wherein the generated personal key for the call is updated in response to a customer command to generate a new personal key and the updated version of the personal key is provided for display in the first user interface and the second user interface.

8. A non-transitory computer-readable storage medium storing instructions that, when executed by a computing system, cause the computing system to perform a process for performing customer service representative (CSR) call verification, the process comprising:

receiving a first indication of A) a call initiated by a CSR of a provider and B) a customer to which the call was placed;

recording, based on the first indication, a second indication of the call, wherein the second indication of the call is associated with the CSR who initiated the call;

receiving a login request from the customer to a provider portal of the provider and, in response, serving data for a first user interface of the provider portal, wherein the data includes a call status indicator specifying that there is an ongoing call between an agent of the provider and the customer, based on the second indication of the call;

as a result of a selection of the call status indicator via the first user interface, serving additional data for the first user interface of the provider portal, the additional data including i) the second indication of the call, ii) a third indication of the CSR who initiated the call, and iii) a generated personal key for the call; and

providing data for a second user interface displayed to the CSR who initiated the call, wherein the second user interface includes the generated personal key;

wherein the CSR provides the generated personal key to the customer to verify the call.

9. The non-transitory computer-readable storage medium of claim 8, wherein the second indication of the call is provided automatically by a CSR verification system when the CSR initiates the call via the CSR verification system.

10. The non-transitory computer-readable storage medium of claim 8, wherein the recording is done in a CSR verification database via an API accessible by each of: a CSR portal that can present the second user interface, a mobile application that can present a first version of the first user interface, and a website that can present a second version of the first user interface.

11. The non-transitory computer-readable storage medium of claim 8, wherein the first user interface includes,

16

based on the association between the call and the CSR who initiated the call, an identifier of the CSR who initiated the call.

12. The non-transitory computer-readable storage medium of claim 8, wherein the generated personal key for the call is updated after a set period and the updated version of the personal key is provided for display in the first user interface and the second user interface.

13. The non-transitory computer-readable storage medium of claim 8, wherein the generated personal key for the call is updated in response to a customer command to generate a new personal key and the updated version of the personal key is provided for display in the first user interface and the second user interface.

14. The non-transitory computer-readable storage medium of claim 9, wherein the generated personal key for the call is a randomly generated number or phrase.

15. A computing system for performing customer service representative (CSR) call verification, the computing system comprising:

one or more processors; and

one or more memories storing instructions that, when executed by the one or more processors, cause the computing system to perform a process comprising:

receiving a first indication of A) a call initiated by a CSR of a provider and B) a customer to which the call was placed;

recording, based on the first indication, a second indication of the call, wherein the second indication of the call is associated with the CSR who initiated the call;

receiving a login request from the customer to a provider portal of the provider and, in response, serving data for a first user interface of the provider portal, wherein the data includes a call status indicator specifying that there is an ongoing call between an agent of the provider and the customer, based on the second indication of the call;

as a result of selection of the call status indicator via the first user interface, serving additional data for the first user interface of the provider portal, the additional data including i) the second indication of the call, ii) a third indication of the CSR who initiated the call, and iii) a generated personal key for the call; and

providing data for a second user interface displayed to the CSR who initiated the call, wherein the second user interface includes the generated personal key; wherein the CSR provides the generated personal key to the customer to verify the call.

16. The computing system of claim 15, wherein the second indication of the call is provided automatically by a CSR verification system when the CSR initiates the call via the CSR verification system.

17. The computing system of claim 15, wherein the first user interface includes, based on the association between the call and the CSR who initiated the call, an identifier of the CSR who initiated the call.

18. The computing system of claim 15, wherein the generated personal key for the call is updated after a set period and the updated version of the personal key is provided for display in the first user interface and the second user interface.

19. The computing system of claim 15, wherein the generated personal key for the call is a randomly generated number or phrase.

17

20. The computing system of claim **15**, wherein the generated personal key for the call is updated in response to a customer command to generate a new personal key and the updated version of the personal key is provided for display in the first user interface and the second user interface. 5

* * * * *

18