

(12) CERTIFIED INNOVATION PATENT
(19) AUSTRALIAN PATENT OFFICE

(11) Application No. **AU 2016102031 B4**

(54) Title
User interface for payments

(51) International Patent Classification(s)
G06Q 20/32 (2012.01) **H04B 5/00** (2006.01)
G06K 9/62 (2006.01)

(21) Application No: **2016102031** (22) Date of Filing: **2016.11.24**

(45) Publication Date: **2016.12.22**
(45) Publication Journal Date: **2016.12.22**
(45) Granted Journal Date: **2016.12.22**
(45) Certified Journal Date: **2017.08.24**

(62) Divisional of:
2016100090

(71) Applicant(s)
Apple Inc.

(72) Inventor(s)
VAN OS, Marcel;DICKER, George R.;ANTON, Peter D.;STEELE, Glen W.;CARO, Pablo F.;PITSCHER, Donald W.

(74) Agent / Attorney
FPA Patent Attorneys Pty Ltd, ANZ Tower 161 Castlereagh Street, Sydney, NSW, 2000, AU

(56) Related Art
US 2012/0284185 A1
US 2009/0173784 A1
US 2008/0052181 A1
US 2006/0179404 A1

2016102031 24 Nov 2016

ABSTRACT

The present disclosure generally relates to making payments with a mobile device. In one example process, the device receives first authentication data, such as fingerprint authentication information, and second authentication data, such as a bank authorization code. The device then transmits a transaction request for a payment transactions. In another example process, the device detects activation of a physical input mechanism and detects a fingerprint using a biometric sensor. The device is enabled to participate in NFC payment transactions. In another example process, the device displays a live preview of images obtained via a camera sensor while the device detects partial credit card information of a credit card in a field of view of the camera sensor.

USER INTERFACE FOR PAYMENTS**CROSS-REFERENCE TO RELATED APPLICATIONS**

[0001] This application claims priority from U.S. Provisional Patent Application Serial No. 62/110,566, entitled “USER INTERFACE FOR PAYMENTS”, filed February 1, 2015, and U.S. Provisional Patent Application Serial No. 62/172,000, entitled “USER INTERFACE FOR PAYMENTS”, filed June 5, 2015, each of which is hereby incorporated by reference in its entirety for all purposes.

[0002] This application relates to the following applications: U.S. Patent Application Serial No. 62/004,886, entitled “USER INTERFACE FOR PAYMENTS”, filed May 29, 2014, (Reference No. P22848USP1); U.S. Patent Application Serial No. 62/047,545, entitled “USER INTERFACE FOR PAYMENTS”, filed September 8, 2014, (Reference No. P22848USP2); U.S. Patent Application Serial No. 62/127,790, entitled “USER INTERFACE FOR PAYMENTS”, filed March 3, 2015, (Reference No. P22848USP3); U.S. Patent Application Serial No. 61/912,727, entitled “PROVISIONING AND AUTHENTICATING CREDENTIALS ON AN ELECTRONIC DEVICE”, filed December 6, 2013, (Reference No. P19543USP1); U.S. Patent Application Serial No. 61/909,717, entitled “PROVISIONING OF CREDENTIALS ON AN ELECTRONIC DEVICE USING PASSWORDS COMMUNICATED OVER VERIFIED CHANNELS”, filed November 27, 2013, (Reference No. P19950USP1); U.S. Patent Application Serial No. 62/004,182, entitled “ONLINE PAYMENTS USING A SECURE ELEMENT OF AN ELECTRONIC DEVICE”, filed May 28, 2014, (Reference No. P20450USP4); U.S. Patent Application Serial No. 61/920,029, entitled “DELETION OF CREDENTIALS FROM AN ELECTRONIC DEVICE”, filed December 23, 2013, (Reference No. P21084USP1); U.S. Patent Application Serial No. 61/899,737, entitled “USING BIOAUTHENTICATION IN NEAR-FIELD-COMMUNICATION TRANSACTIONS”, filed November 4, 2013, (Reference No. P21646USP1); U.S. Patent Application Serial No. 61/905,035, entitled “GENERATING TRANSACTION IDENTIFIERS”, filed November 15, 2013, (Reference No. P21714USP1); U.S. Patent Application Serial No. 61/905,042, entitled “ELECTRONIC RECEIPTS FOR NFC-BASED FINANCIAL TRANSACTIONS”, filed November 15, 2013, (Reference No. 21734USP1); U.S. Patent Application Serial Nos. 62/004,798, entitled “FINANCIAL-

2016102031 24 Nov 2016

TRANSACTION NOTIFICATIONS”, filed May 29, 2014, (Reference No. P23211USP1); U.S. Patent Application Serial No. 62/004,837, entitled “METHODS FOR MANAGING PAYMENT APPLETTS ON A SECURE ELEMENT TO CONDUCT MOBILE PAYMENT TRANSACTIONS”, filed May 29, 2014, (Reference No. P23215USP1); U.S. Patent Application Serial No. 62/004,840, entitled “METHODS FOR OPERATING A PORTABLE ELECTRONIC DEVICE TO CONDUCT MOBILE PAYMENT TRANSACTIONS”, filed May 29, 2014, (Reference No. P23223USP1); U.S. Patent Application Serial No. 62/004,835, entitled “METHODS FOR USING A PRIMARY USER DEVICE TO PROVISION CREDENTIALS ONTO A SECONDARY USER DEVICE”, filed May 29, 2014, (Reference No. P23224USP1); U.S. Patent Application Serial No. 62/004,832, entitled “METHODS FOR USING A RANDOM AUTHORIZATION NUMBER TO PROVIDE ENHANCED SECURITY FOR A SECURE ELEMENT”, filed May 29, 2014, (Reference No. P23261USP1); U.S. Patent Application Serial No. 62/004,338, entitled “USER DEVICE SECURE PARTICIPATION IN TRANSACTIONS VIA LOCAL SECURE ELEMENT DETECTION OF MECHANICAL INPUT”, filed May 29, 2014, (Reference No. P22931USP1); and U.S. Utility Patent Application Serial No. 14/092,205, entitled “SECURE PROVISIONING OF CREDENTIALS ON AN ELECTRONIC DEVICE”, filed November 27, 2013, (Reference No. P19545US1); which are hereby incorporated by reference in their entirety.

FIELD

[0003] The present disclosure relates generally to user interfaces, and more specifically to techniques for conducting payment transactions and linking payment accounts to electronic devices.

BACKGROUND

[0004] The use of electronic devices for making payments at point-of-sale terminals and over the Internet has increased significantly in recent years. Exemplary point-of-sale terminals include Near Field Communication-enabled (NFC-enabled) terminals, Bluetooth-enabled terminals, and barcode scanner-enabled terminals. Electronic devices can be used in conjunction with these exemplary terminals to enable the user of the electronic device to make a payment for the purchase of, for example, goods or services. Similarly, electronic devices can be used in

conjunction with Internet shopping carts to enable the user to make a payment by entering their credit card information.

[0004a] Reference to any prior art in the specification is not, and should not be taken as, an acknowledgment or any form of suggestion that this prior art forms part of the common general knowledge in Australia or any other jurisdiction.

BRIEF SUMMARY

[0005] Some techniques for conducting payment transactions and linking payment accounts for payment transactions using electronic devices, however, are generally cumbersome and inefficient. For example, existing techniques use a complex and time-consuming user interface, which may include multiple key presses or keystrokes. Existing techniques require more time than necessary, wasting user time and device energy. This latter consideration is particularly important in battery-operated devices.

[0006] Accordingly, there is a need for electronic devices with faster, more efficient methods and interfaces for conducting payment transactions and linking payment accounts for payment transactions, while maintaining a high level of security. Such methods and interfaces optionally complement or replace other methods for conducting payment transactions and linking payment accounts for payment transactions. Such methods and interfaces reduce the cognitive burden on a user and produce a more efficient human-machine interface. For battery-operated computing devices, such methods and interfaces conserve power and increase the time between battery charges.

[0007] In accordance with some embodiments, a method is performed at an electronic device. The method includes: detecting a request to initiate a payment transaction; in response to detecting the request to initiate the payment transaction, displaying a payment user interface; while displaying the payment user interface, receiving first authorization data; after receiving the first authorization data, determining whether the first authorization data is valid; receiving second authorization data; after receiving the first authorization data and the second authorization data, transmitting a transaction request that corresponds to the payment transaction to one or more remote servers; receiving a reply to the transaction request; and in response to

receiving the reply to the transaction request: in accordance with a determination that the transaction request was successful, dismissing the payment user interface; and in accordance with a determination that the transaction request failed, maintaining display of the payment user interface and updating the payment user interface to display an indication of a reason for failure of the transaction request.

[0008] In accordance with some embodiments, a method is performed at an electronic device with a short-range communication radio and a physical input mechanism that includes an integrated biometric sensor. The method includes: while the electronic device is not enabled to participate in payment transactions via the short-range communication radio: detecting activation of the physical input mechanism; in response to detecting at least a portion of the activation of the physical input mechanism, detecting a fingerprint using the integrated biometric sensor; and determining whether the fingerprint is consistent with an enrolled fingerprint that is enabled to authorize payment transactions; and in accordance with a determination that the fingerprint is consistent with an enrolled fingerprint that is enabled to authorize payment transactions, enabling the device to participate in payment transactions via the short-range communication radio.

[0009] According to one aspect of the invention there is provided a method performed at an electronic device with a display and a camera sensor. The method includes: displaying, on the display, a user interface comprising: a credit card input affordance for receiving, at the electronic device, at least partial credit card information; receiving selection of the credit card input affordance; in response to receiving the selection of the credit card input affordance, concurrently displaying, on the display: a live preview of images obtained via the camera sensor; and a manual credit card entry affordance that, when selected, triggers display of one or more text entry fields and a character entry control that includes a plurality of character keys for entering characters into a text entry field of the one or more text entry fields; and while concurrently displaying the live preview of images obtained via the camera sensor and the manual credit card entry affordance: in accordance with detection of at least partial credit card information of a credit card in a field of view of the camera sensor, ceasing to display the manual credit card entry affordance and displaying the

1001866987

detected at least partial credit card information of the credit card on the display once the at least partial credit card information has been detected in the field of view of the camera sensor.

[0010] In accordance with some embodiments, a method is performed at an electronic device with a short-range communication radio and a physical input mechanism that includes an integrated biometric sensor. While the electronic device is locked and in a first short-range communication radio payment mode: detecting activation of the physical input mechanism; detecting a fingerprint using the integrated biometric sensor; determining whether the fingerprint is consistent with an enrolled fingerprint; and determining whether a set of one or more criteria is met, wherein the set of one or more criteria includes a criterion that is met when the physical input mechanism is reactivated within a predetermined period of time after the activation of the

physical input mechanism; in accordance with a determination that the fingerprint is consistent with the enrolled fingerprint and a determination that the set of one or more criteria is met, transitioning to a second short-range communication radio payment mode different from the first short-range communication radio payment mode; and in accordance with a determination that the fingerprint is consistent with the enrolled fingerprint and a determination that the set of one or more criteria is not met, unlocking the device.

[0011] In accordance with some embodiments, a method is performed at an electronic device with a short-range communication radio and a physical input mechanism that includes an integrated biometric sensor. While the electronic device is locked and in a first short-range communication radio payment mode: detecting a fingerprint using the integrated biometric sensor; determining whether the fingerprint is consistent with an enrolled fingerprint; determining whether a set of one or more criteria is met, wherein the set of one or more criteria includes a criterion that is met when the physical input mechanism is activated within a first predetermined period of time after detecting the fingerprint using the biometric sensor; in accordance with a determination that the fingerprint is consistent with an enrolled fingerprint and a determination that the set of one or more criteria is not met, unlocking the device; and in accordance with a determination that the set of one or more criteria is met: determining whether the physical input mechanism is reactivated within a second predetermined period of time after the activation of the physical input mechanism; in accordance with a determination that the physical input mechanism is not reactivated within the second predetermined period of time and a determination that the fingerprint is consistent with an enrolled fingerprint, unlocking the device; and in accordance with a determination that the physical input mechanism is reactivated within the second predetermined period of time and in accordance with a determination that the fingerprint is consistent with an enrolled fingerprint, transitioning to a second short-range communication radio payment mode different from the first short-range communication radio payment mode.

[0012] Executable instructions for performing these functions are, optionally, included in a non-transitory computer-readable storage medium or other computer program product configured for execution by one or more processors. Executable instructions for performing

these functions are, optionally, included in a transitory computer-readable storage medium or other computer program product configured for execution by one or more processors.

[0013] Thus, devices are provided with faster, more efficient methods and interfaces for conducting payment transactions and linking payment accounts for payment transactions, thereby increasing the effectiveness, efficiency, and user satisfaction with such devices. Such methods and interfaces may complement or replace other methods for conducting payment transactions and linking payment accounts for payment transactions.

DESCRIPTION OF THE FIGURES

[0014] For a better understanding of the various described embodiments, reference should be made to the Description of Embodiments below, in conjunction with the following drawings in which like reference numerals refer to corresponding parts throughout the figures.

[0015] FIG. 1A is a block diagram illustrating a portable multifunction device with a touch-sensitive display in accordance with some embodiments.

[0016] FIG. 1B is a block diagram illustrating exemplary components for event handling in accordance with some embodiments.

[0017] FIG. 2 illustrates a portable multifunction device having a touch screen in accordance with some embodiments.

[0018] FIG. 3 is a block diagram of an exemplary multifunction device with a display and a touch-sensitive surface in accordance with some embodiments.

[0019] FIG. 4A illustrates an exemplary user interface for a menu of applications on a portable multifunction device in accordance with some embodiments.

[0020] FIG. 4B illustrates an exemplary user interface for a multifunction device with a touch-sensitive surface that is separate from the display in accordance with some embodiments.

[0021] FIG. 5A illustrates a personal electronic device in accordance with some embodiments.

2016102031 24 Nov 2016

[0022] FIG. 5B is a block diagram illustrating a personal electronic device in accordance with some embodiments.

[0023] FIG. 5C illustrates exemplary devices connected via one or more communication channels to complete a payment transaction in accordance with some embodiments.

[0024] FIGS. 6A-6O illustrate exemplary user interfaces for conducting a payment transaction in accordance with some embodiments.

[0025] FIG. 7 is a flow diagram illustrating a method for conducting a payment transaction in accordance with some embodiments.

[0026] FIGS. 8A-8K illustrate exemplary techniques and user interfaces for conducting a payment transaction using a short-range communication radio in accordance with some embodiments.

[0027] FIG. 9 is a flow diagram illustrating a method for conducting a payment transaction using a short-range communication radio in accordance with some embodiments.

[0028] FIGS. 10A-10I illustrate exemplary user interfaces for linking a payment account to an electronic device in accordance with some embodiments.

[0029] FIG. 11 is a flow diagram illustrating a method for linking a payment account to an electronic device in accordance with some embodiments.

[0030] FIG. 12 illustrates a functional block diagram in accordance with some embodiments.

[0031] FIGS. 13A-13E illustrate exemplary techniques and user interfaces for enabling an electronic device to participate in a payment transaction in accordance with some embodiments.

[0032] FIG. 14 is a flow diagram illustrating a method for enabling an electronic device to participate in a payment transaction in accordance with some embodiments.

[0033] FIGS. 15A-15E illustrate exemplary techniques and user interfaces for enabling an electronic device to participate in a payment transaction in accordance with some embodiments.

2016102031 24 Nov 2016

[0034] FIG. 16 is a flow diagram illustrating a method for enabling an electronic device to participate in a payment transaction in accordance with some embodiments.

[0035] FIGS. 17-18 illustrate functional block diagrams in accordance with some embodiments.

DESCRIPTION OF EMBODIMENTS

[0036] The following description sets forth exemplary methods, parameters, and the like. It should be recognized, however, that such description is not intended as a limitation on the scope of the present disclosure but is instead provided as a description of exemplary embodiments.

[0037] Aspects of method 700 (FIGS. 6A-6O, FIG. 7), method 900 (FIGS. 8A-8K, FIG. 9), method 1100 (FIGS. 10A-10I, FIG. 11), method 1400 (FIGS. 13A-13E, FIG. 14), and method 1600 (FIGS. 15A-15E, FIG. 16) may be incorporated with one another. Additionally, aspects of U.S. Provisional Patent Application Serial No. 62/004,886 (the “’886 Application”), entitled “USER INTERFACE FOR PAYMENTS”, filed May 29, 2014, (Reference No. P22848USP1) and aspects of co-pending U.S. Provisional Patent Application Serial No. 62/047,545 (the “’545 Application”), entitled “USER INTERFACE FOR PAYMENTS”, filed September 8, 2014, (Reference No. P22848USP2) may be incorporated with the techniques described below.

[0038] For example, aspects of method 600 (FIG. 6A-6C), method 800 (FIG. 8A-8B), method 1000 (FIG. 10A-10B), and method 1200 (FIG. 12A-12C) of the ’886 Application may be incorporated with one another and may also be incorporated with aspects of method 600 (FIG. 6), method 800 (FIG. 8), method 1000 (FIG. 10), method 1200 (FIG. 12), and method 1400 (FIG. 14) of the ’545 Application, and may also be incorporated with aspects of method 700 (FIG. 7), method 900 (FIG. 9), and method 1100 (FIG. 11). Thus, the techniques described with respect to each method of the ’886 Application, the ’545 Application, and the present application may be relevant to every other method of the ’886 Application, the ’545 Application, and the present application.

[0039] There is a need for electronic devices that provide efficient methods and interfaces for conducting payment transactions and linking payment accounts for payment transactions. Such techniques can reduce the cognitive burden on a user who access event notifications, thereby

enhancing productivity. Further, such techniques can reduce processor and battery power otherwise wasted on redundant user inputs.

[0040] Below, FIGS. 1A-1B, 2, 3, 4A-4B, and 5A-5B provide a description of exemplary devices for performing the techniques for conducting payment transactions and linking payment accounts for payment transactions. FIGS. 6A-6O, 8A-8K, 10A-10I, 13A-13D, and 15A-15D illustrate exemplary techniques and user interfaces for conducting payment transactions and linking payment accounts. The user interfaces in the figures are also used to illustrate the processes described below, including the processes in FIGS. 7, 9, 11, 14, and 16.

[0041] Although the following description uses terms “first,” “second,” etc. to describe various elements, these elements should not be limited by the terms. These terms are only used to distinguish one element from another. For example, a first touch could be termed a second touch, and, similarly, a second touch could be termed a first touch, without departing from the scope of the various described embodiments. The first touch and the second touch are both touches, but they are not the same touch.

[0042] The terminology used in the description of the various described embodiments herein is for the purpose of describing particular embodiments only and is not intended to be limiting. As used in the description of the various described embodiments and the appended claims, the singular forms “a,” “an,” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will also be understood that the term “and/or” as used herein refers to and encompasses any and all possible combinations of one or more of the associated listed items. It will be further understood that the terms “includes,” “including,” “comprises,” and/or “comprising,” when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

[0043] The term “if” may be construed to mean “when” or “upon” or “in response to determining” or “in response to detecting,” depending on the context. Similarly, the phrase “if it is determined” or “if [a stated condition or event] is detected” may be construed to mean “upon

determining” or “in response to determining” or “upon detecting [the stated condition or event]” or “in response to detecting [the stated condition or event],” depending on the context.

[0044] Embodiments of electronic devices, user interfaces for such devices, and associated processes for using such devices are described. In some embodiments, the device is a portable communications device, such as a mobile telephone, that also contains other functions, such as PDA and/or music player functions. Exemplary embodiments of portable multifunction devices include, without limitation, the iPhone®, iPod Touch®, and iPad® devices from Apple Inc. of Cupertino, California. Other portable electronic devices, such as laptops or tablet computers with touch-sensitive surfaces (e.g., touch screen displays and/or touchpads), are, optionally, used. It should also be understood that, in some embodiments, the device is not a portable communications device, but is a desktop computer with a touch-sensitive surface (e.g., a touch screen display and/or a touchpad).

[0045] In the discussion that follows, an electronic device that includes a display and a touch-sensitive surface is described. It should be understood, however, that the electronic device optionally includes one or more other physical user-interface devices, such as a physical keyboard, a mouse, and/or a joystick.

[0046] The device may support a variety of applications, such as one or more of the following: a drawing application, a presentation application, a word processing application, a website creation application, a disk authoring application, a spreadsheet application, a gaming application, a telephone application, a video conferencing application, an e-mail application, an instant messaging application, a workout support application, a photo management application, a digital camera application, a digital video camera application, a web browsing application, a digital music player application, and/or a digital video player application.

[0047] The various applications that are executed on the device optionally use at least one common physical user-interface device, such as the touch-sensitive surface. One or more functions of the touch-sensitive surface as well as corresponding information displayed on the device are, optionally, adjusted and/or varied from one application to the next and/or within a respective application. In this way, a common physical architecture (such as the touch-sensitive

surface) of the device optionally supports the variety of applications with user interfaces that are intuitive and transparent to the user.

[0048] Attention is now directed toward embodiments of portable devices with touch-sensitive displays. FIG. 1A is a block diagram illustrating portable multifunction device 100 with touch-sensitive display system 112 in accordance with some embodiments. Touch-sensitive display 112 is sometimes called a “touch screen” for convenience and is sometimes known as or called a “touch-sensitive display system.” Device 100 includes memory 102 (which optionally includes one or more computer-readable storage mediums), memory controller 122, one or more processing units (CPUs) 120, peripherals interface 118, RF circuitry 108, audio circuitry 110, speaker 111, microphone 113, input/output (I/O) subsystem 106, other input control devices 116, and external port 124. Device 100 optionally includes one or more optical sensors 164. Device 100 optionally includes one or more contact intensity sensors 165 for detecting intensity of contacts on device 100 (e.g., a touch-sensitive surface such as touch-sensitive display system 112 of device 100). Device 100 optionally includes one or more tactile output generators 167 for generating tactile outputs on device 100 (e.g., generating tactile outputs on a touch-sensitive surface such as touch-sensitive display system 112 of device 100 or touchpad 355 of device 300). These components optionally communicate over one or more communication buses or signal lines 103.

[0049] As used in the specification and claims, the term “intensity” of a contact on a touch-sensitive surface refers to the force or pressure (force per unit area) of a contact (e.g., a finger contact) on the touch-sensitive surface, or to a substitute (proxy) for the force or pressure of a contact on the touch-sensitive surface. The intensity of a contact has a range of values that includes at least four distinct values and more typically includes hundreds of distinct values (e.g., at least 256). Intensity of a contact is, optionally, determined (or measured) using various approaches and various sensors or combinations of sensors. For example, one or more force sensors underneath or adjacent to the touch-sensitive surface are, optionally, used to measure force at various points on the touch-sensitive surface. In some implementations, force measurements from multiple force sensors are combined (e.g., a weighted average) to determine an estimated force of a contact. Similarly, a pressure-sensitive tip of a stylus is, optionally, used to determine a pressure of the stylus on the touch-sensitive surface. Alternatively, the size of the

contact area detected on the touch-sensitive surface and/or changes thereto, the capacitance of the touch-sensitive surface proximate to the contact and/or changes thereto, and/or the resistance of the touch-sensitive surface proximate to the contact and/or changes thereto are, optionally, used as a substitute for the force or pressure of the contact on the touch-sensitive surface. In some implementations, the substitute measurements for contact force or pressure are used directly to determine whether an intensity threshold has been exceeded (e.g., the intensity threshold is described in units corresponding to the substitute measurements). In some implementations, the substitute measurements for contact force or pressure are converted to an estimated force or pressure, and the estimated force or pressure is used to determine whether an intensity threshold has been exceeded (e.g., the intensity threshold is a pressure threshold measured in units of pressure). Using the intensity of a contact as an attribute of a user input allows for user access to additional device functionality that may otherwise not be accessible by the user on a reduced-size device with limited real estate for displaying affordances (e.g., on a touch-sensitive display) and/or receiving user input (e.g., via a touch-sensitive display, a touch-sensitive surface, or a physical/mechanical control such as a knob or a button).

[0050] As used in the specification and claims, the term “tactile output” refers to physical displacement of a device relative to a previous position of the device, physical displacement of a component (e.g., a touch-sensitive surface) of a device relative to another component (e.g., housing) of the device, or displacement of the component relative to a center of mass of the device that will be detected by a user with the user’s sense of touch. For example, in situations where the device or the component of the device is in contact with a surface of a user that is sensitive to touch (e.g., a finger, palm, or other part of a user’s hand), the tactile output generated by the physical displacement will be interpreted by the user as a tactile sensation corresponding to a perceived change in physical characteristics of the device or the component of the device. For example, movement of a touch-sensitive surface (e.g., a touch-sensitive display or trackpad) is, optionally, interpreted by the user as a “down click” or “up click” of a physical actuator button. In some cases, a user will feel a tactile sensation such as an “down click” or “up click” even when there is no movement of a physical actuator button associated with the touch-sensitive surface that is physically pressed (e.g., displaced) by the user’s movements. As another example, movement of the touch-sensitive surface is, optionally, interpreted or sensed by the user as “roughness” of the touch-sensitive surface, even when there is no change in smoothness

2016102031 24 Nov 2016

of the touch-sensitive surface. While such interpretations of touch by a user will be subject to the individualized sensory perceptions of the user, there are many sensory perceptions of touch that are common to a large majority of users. Thus, when a tactile output is described as corresponding to a particular sensory perception of a user (e.g., an “up click,” a “down click,” “roughness”), unless otherwise stated, the generated tactile output corresponds to physical displacement of the device or a component thereof that will generate the described sensory perception for a typical (or average) user.

[0051] It should be appreciated that device 100 is only one example of a portable multifunction device, and that device 100 optionally has more or fewer components than shown, optionally combines two or more components, or optionally has a different configuration or arrangement of the components. The various components shown in FIG. 1A are implemented in hardware, software, or a combination of both hardware and software, including one or more signal processing and/or application-specific integrated circuits.

[0052] Memory 102 may include one or more computer-readable storage mediums. The computer-readable storage mediums may be tangible and non-transitory. Memory 102 may include high-speed random access memory and may also include non-volatile memory, such as one or more magnetic disk storage devices, flash memory devices, or other non-volatile solid-state memory devices. Memory controller 122 may control access to memory 102 by other components of device 100.

[0053] Peripherals interface 118 can be used to couple input and output peripherals of the device to CPU 120 and memory 102. The one or more processors 120 run or execute various software programs and/or sets of instructions stored in memory 102 to perform various functions for device 100 and to process data. In some embodiments, peripherals interface 118, CPU 120, and memory controller 122 may be implemented on a single chip, such as chip 104. In some other embodiments, they may be implemented on separate chips.

[0054] RF (radio frequency) circuitry 108 receives and sends RF signals, also called electromagnetic signals. RF circuitry 108 converts electrical signals to/from electromagnetic signals and communicates with communications networks and other communications devices via the electromagnetic signals. RF circuitry 108 optionally includes well-known circuitry for

2016102031 24 Nov 2016

performing these functions, including but not limited to an antenna system, an RF transceiver, one or more amplifiers, a tuner, one or more oscillators, a digital signal processor, a CODEC chipset, a subscriber identity module (SIM) card, memory, and so forth. RF circuitry 108 optionally communicates with networks, such as the Internet, also referred to as the World Wide Web (WWW), an intranet and/or a wireless network, such as a cellular telephone network, a wireless local area network (LAN) and/or a metropolitan area network (MAN), and other devices by wireless communication. The RF circuitry 108 optionally includes well-known circuitry for detecting near field communication (NFC) fields, such as by a short-range communication radio. The wireless communication optionally uses any of a plurality of communications standards, protocols, and technologies, including but not limited to Global System for Mobile Communications (GSM), Enhanced Data GSM Environment (EDGE), high-speed downlink packet access (HSDPA), high-speed uplink packet access (HSUPA), Evolution, Data-Only (EV-DO), HSPA, HSPA+, Dual-Cell HSPA (DC-HSPDA), long term evolution (LTE), near field communication (NFC), wideband code division multiple access (W-CDMA), code division multiple access (CDMA), time division multiple access (TDMA), Bluetooth, Bluetooth Low Energy (BTLE), Wireless Fidelity (Wi-Fi) (e.g., IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, and/or IEEE 802.11ac), voice over Internet Protocol (VoIP), Wi-MAX, a protocol for e-mail (e.g., Internet message access protocol (IMAP) and/or post office protocol (POP)), instant messaging (e.g., extensible messaging and presence protocol (XMPP), Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE), Instant Messaging and Presence Service (IMPS)), and/or Short Message Service (SMS), or any other suitable communication protocol, including communication protocols not yet developed as of the filing date of this document.

[0055] Audio circuitry 110, speaker 111, and microphone 113 provide an audio interface between a user and device 100. Audio circuitry 110 receives audio data from peripherals interface 118, converts the audio data to an electrical signal, and transmits the electrical signal to speaker 111. Speaker 111 converts the electrical signal to human-audible sound waves. Audio circuitry 110 also receives electrical signals converted by microphone 113 from sound waves. Audio circuitry 110 converts the electrical signal to audio data and transmits the audio data to peripherals interface 118 for processing. Audio data may be retrieved from and/or transmitted to memory 102 and/or RF circuitry 108 by peripherals interface 118. In some embodiments, audio

2016102031 24 Nov 2016

circuitry 110 also includes a headset jack (e.g., 212, FIG. 2). The headset jack provides an interface between audio circuitry 110 and removable audio input/output peripherals, such as output-only headphones or a headset with both output (e.g., a headphone for one or both ears) and input (e.g., a microphone).

[0056] I/O subsystem 106 couples input/output peripherals on device 100, such as touch screen 112 and other input control devices 116, to peripherals interface 118. I/O subsystem 106 optionally includes display controller 156, optical sensor controller 158, intensity sensor controller 159, haptic feedback controller 161, and one or more input controllers 160 for other input or control devices. The one or more input controllers 160 receive/send electrical signals from/to other input control devices 116. The other input control devices 116 optionally include physical buttons (e.g., push buttons, rocker buttons, etc.), dials, slider switches, joysticks, click wheels, and so forth. In some alternate embodiments, input controller(s) 160 are, optionally, coupled to any (or none) of the following: a keyboard, an infrared port, a USB port, and a pointer device such as a mouse. The one or more buttons (e.g., 208, FIG. 2) optionally include an up/down button for volume control of speaker 111 and/or microphone 113. The one or more buttons optionally include a push button (e.g., 206, FIG. 2).

[0057] A quick press of the push button may disengage a lock of touch screen 112 or begin a process that uses gestures on the touch screen to unlock the device, as described in U.S. Patent Application 11/322,549, “Unlocking a Device by Performing Gestures on an Unlock Image,” filed December 23, 2005, U.S. Pat. No. 7,657,849, which is hereby incorporated by reference in its entirety. A longer press of the push button (e.g., 206) may turn power to device 100 on or off. The user may be able to customize a functionality of one or more of the buttons. Touch screen 112 is used to implement virtual or soft buttons and one or more soft keyboards.

[0058] Touch-sensitive display 112 provides an input interface and an output interface between the device and a user. Display controller 156 receives and/or sends electrical signals from/to touch screen 112. Touch screen 112 displays visual output to the user. The visual output may include graphics, text, icons, video, and any combination thereof (collectively termed “graphics”). In some embodiments, some or all of the visual output may correspond to user-interface objects.

2016102031 24 Nov 2016

[0059] Touch screen 112 has a touch-sensitive surface, sensor, or set of sensors that accepts input from the user based on haptic and/or tactile contact. Touch screen 112 and display controller 156 (along with any associated modules and/or sets of instructions in memory 102) detect contact (and any movement or breaking of the contact) on touch screen 112 and convert the detected contact into interaction with user-interface objects (e.g., one or more soft keys, icons, web pages, or images) that are displayed on touch screen 112. In an exemplary embodiment, a point of contact between touch screen 112 and the user corresponds to a finger of the user.

[0060] Touch screen 112 may use LCD (liquid crystal display) technology, LPD (light emitting polymer display) technology, or LED (light emitting diode) technology, although other display technologies may be used in other embodiments. Touch screen 112 and display controller 156 may detect contact and any movement or breaking thereof using any of a plurality of touch sensing technologies now known or later developed, including but not limited to capacitive, resistive, infrared, and surface acoustic wave technologies, as well as other proximity sensor arrays or other elements for determining one or more points of contact with touch screen 112. In an exemplary embodiment, projected mutual capacitance sensing technology is used, such as that found in the iPhone® and iPod Touch® from Apple Inc. of Cupertino, California.

[0061] A touch-sensitive display in some embodiments of touch screen 112 may be analogous to the multi-touch sensitive touchpads described in the following U.S. Patents: 6,323,846 (Westerman et al.), 6,570,557 (Westerman et al.), and/or 6,677,932 (Westerman), and/or U.S. Patent Publication 2002/0015024A1, each of which is hereby incorporated by reference in its entirety. However, touch screen 112 displays visual output from device 100, whereas touch-sensitive touchpads do not provide visual output.

[0062] A touch-sensitive display in some embodiments of touch screen 112 may be as described in the following applications: (1) U.S. Patent Application No. 11/381,313, “Multipoint Touch Surface Controller,” filed May 2, 2006; (2) U.S. Patent Application No. 10/840,862, “Multipoint Touchscreen,” filed May 6, 2004; (3) U.S. Patent Application No. 10/903,964, “Gestures For Touch Sensitive Input Devices,” filed July 30, 2004; (4) U.S. Patent Application No. 11/048,264, “Gestures For Touch Sensitive Input Devices,” filed January 31, 2005; (5) U.S.

2016102031 24 Nov 2016

Patent Application No. 11/038,590, “Mode-Based Graphical User Interfaces For Touch Sensitive Input Devices,” filed January 18, 2005; (6) U.S. Patent Application No. 11/228,758, “Virtual Input Device Placement On A Touch Screen User Interface,” filed September 16, 2005; (7) U.S. Patent Application No. 11/228,700, “Operation Of A Computer With A Touch Screen Interface,” filed September 16, 2005; (8) U.S. Patent Application No. 11/228,737, “Activating Virtual Keys Of A Touch-Screen Virtual Keyboard,” filed September 16, 2005; and (9) U.S. Patent Application No. 11/367,749, “Multi-Functional Hand-Held Device,” filed March 3, 2006. All of these applications are incorporated by reference herein in their entirety.

[0063] Touch screen 112 may have a video resolution in excess of 100 dpi. In some embodiments, the touch screen has a video resolution of approximately 160 dpi. The user may make contact with touch screen 112 using any suitable object or appendage, such as a stylus, a finger, and so forth. In some embodiments, the user interface is designed to work primarily with finger-based contacts and gestures, which can be less precise than stylus-based input due to the larger area of contact of a finger on the touch screen. In some embodiments, the device translates the rough finger-based input into a precise pointer/cursor position or command for performing the actions desired by the user.

[0064] In some embodiments, in addition to the touch screen, device 100 may include a touchpad (not shown) for activating or deactivating particular functions. In some embodiments, the touchpad is a touch-sensitive area of the device that, unlike the touch screen, does not display visual output. The touchpad may be a touch-sensitive surface that is separate from touch screen 112 or an extension of the touch-sensitive surface formed by the touch screen.

[0065] Device 100 also includes power system 162 for powering the various components. Power system 162 may include a power management system, one or more power sources (e.g., battery, alternating current (AC)), a recharging system, a power failure detection circuit, a power converter or inverter, a power status indicator (e.g., a light-emitting diode (LED)) and any other components associated with the generation, management and distribution of power in portable devices.

[0066] Device 100 may also include one or more optical sensors 164. FIG. 1A shows an optical sensor coupled to optical sensor controller 158 in I/O subsystem 106. Optical sensor 164

2016102031 24 Nov 2016

may include charge-coupled device (CCD) or complementary metal-oxide semiconductor (CMOS) phototransistors. Optical sensor 164 receives light from the environment, projected through one or more lenses, and converts the light to data representing an image. In conjunction with imaging module 143 (also called a camera module), optical sensor 164 may capture still images or video. In some embodiments, an optical sensor is located on the back of device 100, opposite touch screen display 112 on the front of the device so that the touch screen display may be used as a viewfinder for still and/or video image acquisition. In some embodiments, an optical sensor is located on the front of the device so that the user's image may be obtained for video conferencing while the user views the other video conference participants on the touch screen display. In some embodiments, the position of optical sensor 164 can be changed by the user (e.g., by rotating the lens and the sensor in the device housing) so that a single optical sensor 164 may be used along with the touch screen display for both video conferencing and still and/or video image acquisition.

[0067] Device 100 optionally also includes one or more contact intensity sensors 165. FIG. 1A shows a contact intensity sensor coupled to intensity sensor controller 159 in I/O subsystem 106. Contact intensity sensor 165 optionally includes one or more piezoresistive strain gauges, capacitive force sensors, electric force sensors, piezoelectric force sensors, optical force sensors, capacitive touch-sensitive surfaces, or other intensity sensors (e.g., sensors used to measure the force (or pressure) of a contact on a touch-sensitive surface). Contact intensity sensor 165 receives contact intensity information (e.g., pressure information or a proxy for pressure information) from the environment. In some embodiments, at least one contact intensity sensor is collocated with, or proximate to, a touch-sensitive surface (e.g., touch-sensitive display system 112). In some embodiments, at least one contact intensity sensor is located on the back of device 100, opposite touch screen display 112, which is located on the front of device 100.

[0068] Device 100 may also include one or more proximity sensors 166. FIG. 1A shows proximity sensor 166 coupled to peripherals interface 118. Alternately, proximity sensor 166 may be coupled to input controller 160 in I/O subsystem 106. Proximity sensor 166 may perform as described in U.S. Patent Application Nos. 11/241,839, "Proximity Detector In Handheld Device"; 11/240,788, "Proximity Detector In Handheld Device"; 11/620,702, "Using

24 Nov 2016

2016102031

Ambient Light Sensor To Augment Proximity Sensor Output”; 11/586,862, “Automated Response To And Sensing Of User Activity In Portable Devices”; and 11/638,251, “Methods And Systems For Automatic Configuration Of Peripherals,” which are hereby incorporated by reference in their entirety. In some embodiments, the proximity sensor turns off and disables touch screen 112 when the multifunction device is placed near the user’s ear (e.g., when the user is making a phone call).

[0069] Device 100 optionally also includes one or more tactile output generators 167. FIG. 1A shows a tactile output generator coupled to haptic feedback controller 161 in I/O subsystem 106. Tactile output generator 167 optionally includes one or more electroacoustic devices such as speakers or other audio components and/or electromechanical devices that convert energy into linear motion such as a motor, solenoid, electroactive polymer, piezoelectric actuator, electrostatic actuator, or other tactile output generating component (e.g., a component that converts electrical signals into tactile outputs on the device). Contact intensity sensor 165 receives tactile feedback generation instructions from haptic feedback module 133 and generates tactile outputs on device 100 that are capable of being sensed by a user of device 100. In some embodiments, at least one tactile output generator is collocated with, or proximate to, a touch-sensitive surface (e.g., touch-sensitive display system 112) and, optionally, generates a tactile output by moving the touch-sensitive surface vertically (e.g., in/out of a surface of device 100) or laterally (e.g., back and forth in the same plane as a surface of device 100). In some embodiments, at least one tactile output generator sensor is located on the back of device 100, opposite touch screen display 112, which is located on the front of device 100.

[0070] Device 100 may also include one or more accelerometers 168. FIG. 1A shows accelerometer 168 coupled to peripherals interface 118. Alternately, accelerometer 168 may be coupled to an input controller 160 in I/O subsystem 106. Accelerometer 168 may perform as described in U.S. Patent Publication No. 20050190059, “Acceleration-based Theft Detection System for Portable Electronic Devices,” and U.S. Patent Publication No. 20060017692, “Methods And Apparatuses For Operating A Portable Device Based On An Accelerometer,” both of which are incorporated by reference herein in their entirety. In some embodiments, information is displayed on the touch screen display in a portrait view or a landscape view based on an analysis of data received from the one or more accelerometers. Device 100 optionally

2016102031 24 Nov 2016

includes, in addition to accelerometer(s) 168, a magnetometer (not shown) and a GPS (or GLONASS or other global navigation system) receiver (not shown) for obtaining information concerning the location and orientation (e.g., portrait or landscape) of device 100.

[0071] In some embodiments, the software components stored in memory 102 include operating system 126, communication module (or set of instructions) 128, contact/motion module (or set of instructions) 130, graphics module (or set of instructions) 132, text input module (or set of instructions) 134, Global Positioning System (GPS) module (or set of instructions) 135, and applications (or sets of instructions) 136. Furthermore, in some embodiments, memory 102 (FIG. 1A) or 370 (FIG. 3) stores device/global internal state 157, as shown in FIGS. 1A and 3. Device/global internal state 157 includes one or more of: active application state, indicating which applications, if any, are currently active; display state, indicating what applications, views or other information occupy various regions of touch screen display 112; sensor state, including information obtained from the device's various sensors and input control devices 116; and location information concerning the device's location and/or attitude.

[0072] Operating system 126 (e.g., Darwin, RTXC, LINUX, UNIX, OS X, iOS, WINDOWS, or an embedded operating system such as VxWorks) includes various software components and/or drivers for controlling and managing general system tasks (e.g., memory management, storage device control, power management, etc.) and facilitates communication between various hardware and software components.

[0073] Communication module 128 facilitates communication with other devices over one or more external ports 124 and also includes various software components for handling data received by RF circuitry 108 and/or external port 124. External port 124 (e.g., Universal Serial Bus (USB), FIREWIRE, etc.) is adapted for coupling directly to other devices or indirectly over a network (e.g., the Internet, wireless LAN, etc.). In some embodiments, the external port is a multi-pin (e.g., 30-pin) connector that is the same as, or similar to and/or compatible with, the 30-pin connector used on iPod® (trademark of Apple Inc.) devices.

[0074] Contact/motion module 130 optionally detects contact with touch screen 112 (in conjunction with display controller 156) and other touch-sensitive devices (e.g., a touchpad or

2016102031 24 Nov 2016

physical click wheel). Contact/motion module 130 includes various software components for performing various operations related to detection of contact, such as determining if contact has occurred (e.g., detecting a finger-down event), determining an intensity of the contact (e.g., the force or pressure of the contact or a substitute for the force or pressure of the contact), determining if there is movement of the contact and tracking the movement across the touch-sensitive surface (e.g., detecting one or more finger-dragging events), and determining if the contact has ceased (e.g., detecting a finger-up event or a break in contact). Contact/motion module 130 receives contact data from the touch-sensitive surface. Determining movement of the point of contact, which is represented by a series of contact data, optionally includes determining speed (magnitude), velocity (magnitude and direction), and/or an acceleration (a change in magnitude and/or direction) of the point of contact. These operations are, optionally, applied to single contacts (e.g., one finger contacts) or to multiple simultaneous contacts (e.g., “multitouch”/multiple finger contacts). In some embodiments, contact/motion module 130 and display controller 156 detect contact on a touchpad.

[0075] In some embodiments, contact/motion module 130 uses a set of one or more intensity thresholds to determine whether an operation has been performed by a user (e.g., to determine whether a user has “clicked” on an icon). In some embodiments, at least a subset of the intensity thresholds are determined in accordance with software parameters (e.g., the intensity thresholds are not determined by the activation thresholds of particular physical actuators and can be adjusted without changing the physical hardware of device 100). For example, a mouse “click” threshold of a trackpad or touch screen display can be set to any of a large range of predefined threshold values without changing the trackpad or touch screen display hardware. Additionally, in some implementations, a user of the device is provided with software settings for adjusting one or more of the set of intensity thresholds (e.g., by adjusting individual intensity thresholds and/or by adjusting a plurality of intensity thresholds at once with a system-level click “intensity” parameter).

[0076] Contact/motion module 130 optionally detects a gesture input by a user. Different gestures on the touch-sensitive surface have different contact patterns (e.g., different motions, timings, and/or intensities of detected contacts). Thus, a gesture is, optionally, detected by detecting a particular contact pattern. For example, detecting a finger tap gesture includes

detecting a finger-down event followed by detecting a finger-up (liftoff) event at the same position (or substantially the same position) as the finger-down event (e.g., at the position of an icon). As another example, detecting a finger swipe gesture on the touch-sensitive surface includes detecting a finger-down event followed by detecting one or more finger-dragging events, and subsequently followed by detecting a finger-up (liftoff) event.

[0077] Graphics module 132 includes various known software components for rendering and displaying graphics on touch screen 112 or other display, including components for changing the visual impact (e.g., brightness, transparency, saturation, contrast, or other visual property) of graphics that are displayed. As used herein, the term “graphics” includes any object that can be displayed to a user, including, without limitation, text, web pages, icons (such as user-interface objects including soft keys), digital images, videos, animations, and the like.

[0078] In some embodiments, graphics module 132 stores data representing graphics to be used. Each graphic is, optionally, assigned a corresponding code. Graphics module 132 receives, from applications etc., one or more codes specifying graphics to be displayed along with, if necessary, coordinate data and other graphic property data, and then generates screen image data to output to display controller 156.

[0079] Haptic feedback module 133 includes various software components for generating instructions used by tactile output generator(s) 167 to produce tactile outputs at one or more locations on device 100 in response to user interactions with device 100.

[0080] Text input module 134, which may be a component of graphics module 132, provides soft keyboards for entering text in various applications (e.g., contacts 137, e-mail 140, IM 141, browser 147, and any other application that needs text input).

[0081] GPS module 135 determines the location of the device and provides this information for use in various applications (e.g., to telephone 138 for use in location-based dialing; to camera 143 as picture/video metadata; and to applications that provide location-based services such as weather widgets, local yellow page widgets, and map/navigation widgets).

[0082] Applications 136 may include the following modules (or sets of instructions), or a subset or superset thereof:

2016102031 24 Nov 2016

- Contacts module 137 (sometimes called an address book or contact list);
- Telephone module 138;
- Video conferencing module 139;
- E-mail client module 140;
- Instant messaging (IM) module 141;
- Workout support module 142;
- Camera module 143 for still and/or video images;
- Image management module 144;
- Video player module;
- Music player module;
- Browser module 147;
- Calendar module 148;
- Widget modules 149, which may include one or more of: weather widget 149-1, stocks widget 149-2, calculator widget 149-3, alarm clock widget 149-4, dictionary widget 149-5, and other widgets obtained by the user, as well as user-created widgets 149-6;
- Widget creator module 150 for making user-created widgets 149-6;
- Search module 151;
- Video and music player module 152, which merges video player module and music player module;
- Notes module 153;
- Map module 154; and/or

- Online video module 155.

[0083] Examples of other applications 136 that may be stored in memory 102 include other word processing applications, other image editing applications, drawing applications, presentation applications, JAVA-enabled applications, encryption, digital rights management, voice recognition, and voice replication.

[0084] In conjunction with touch screen 112, display controller 156, contact/motion module 130, graphics module 132, and text input module 134, contacts module 137 may be used to manage an address book or contact list (e.g., stored in application internal state 192 of contacts module 137 in memory 102 or memory 370), including: adding name(s) to the address book; deleting name(s) from the address book; associating telephone number(s), e-mail address(es), physical address(es) or other information with a name; associating an image with a name; categorizing and sorting names; providing telephone numbers or e-mail addresses to initiate and/or facilitate communications by telephone 138, video conference 139, e-mail 140, or IM 141; and so forth.

[0085] In conjunction with RF circuitry 108, audio circuitry 110, speaker 111, microphone 113, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, and text input module 134, telephone module 138 may be used to enter a sequence of characters corresponding to a telephone number, access one or more telephone numbers in contacts module 137, modify a telephone number that has been entered, dial a respective telephone number, conduct a conversation, and disconnect or hang up when the conversation is completed. As noted above, the wireless communication may use any of a plurality of communications standards, protocols, and technologies.

[0086] In conjunction with RF circuitry 108, audio circuitry 110, speaker 111, microphone 113, touch screen 112, display controller 156, optical sensor 164, optical sensor controller 158, contact/motion module 130, graphics module 132, text input module 134, contacts module 137, and telephone module 138, video conference module 139 includes executable instructions to initiate, conduct, and terminate a video conference between a user and one or more other participants in accordance with user instructions.

2016102031 24 Nov 2016

[0087] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, and text input module 134, e-mail client module 140 includes executable instructions to create, send, receive, and manage e-mail in response to user instructions. In conjunction with image management module 144, e-mail client module 140 makes it very easy to create and send e-mails with still or video images taken with camera module 143.

[0088] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, and text input module 134, the instant messaging module 141 includes executable instructions to enter a sequence of characters corresponding to an instant message, to modify previously entered characters, to transmit a respective instant message (for example, using a Short Message Service (SMS) or Multimedia Message Service (MMS) protocol for telephony-based instant messages or using XMPP, SIMPLE, or IMPS for Internet-based instant messages), to receive instant messages, and to view received instant messages. In some embodiments, transmitted and/or received instant messages may include graphics, photos, audio files, video files and/or other attachments as are supported in an MMS and/or an Enhanced Messaging Service (EMS). As used herein, “instant messaging” refers to both telephony-based messages (e.g., messages sent using SMS or MMS) and Internet-based messages (e.g., messages sent using XMPP, SIMPLE, or IMPS).

[0089] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, text input module 134, GPS module 135, map module 154, and music player module, workout support module 142 includes executable instructions to create workouts (e.g., with time, distance, and/or calorie burning goals); communicate with workout sensors (sports devices); receive workout sensor data; calibrate sensors used to monitor a workout; select and play music for a workout; and display, store, and transmit workout data.

[0090] In conjunction with touch screen 112, display controller 156, optical sensor(s) 164, optical sensor controller 158, contact/motion module 130, graphics module 132, and image management module 144, camera module 143 includes executable instructions to capture still

images or video (including a video stream) and store them into memory 102, modify characteristics of a still image or video, or delete a still image or video from memory 102.

[0091] In conjunction with touch screen 112, display controller 156, contact/motion module 130, graphics module 132, text input module 134, and camera module 143, image management module 144 includes executable instructions to arrange, modify (e.g., edit), or otherwise manipulate, label, delete, present (e.g., in a digital slide show or album), and store still and/or video images.

[0092] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, and text input module 134, browser module 147 includes executable instructions to browse the Internet in accordance with user instructions, including searching, linking to, receiving, and displaying web pages or portions thereof, as well as attachments and other files linked to web pages.

[0093] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, text input module 134, e-mail client module 140, and browser module 147, calendar module 148 includes executable instructions to create, display, modify, and store calendars and data associated with calendars (e.g., calendar entries, to-do lists, etc.) in accordance with user instructions.

[0094] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, text input module 134, and browser module 147, widget modules 149 are mini-applications that may be downloaded and used by a user (e.g., weather widget 149-1, stocks widget 149-2, calculator widget 149-3, alarm clock widget 149-4, and dictionary widget 149-5) or created by the user (e.g., user-created widget 149-6). In some embodiments, a widget includes an HTML (Hypertext Markup Language) file, a CSS (Cascading Style Sheets) file, and a JavaScript file. In some embodiments, a widget includes an XML (Extensible Markup Language) file and a JavaScript file (e.g., Yahoo! Widgets).

[0095] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact/motion module 130, graphics module 132, text input module 134, and browser module

147, the widget creator module 150 may be used by a user to create widgets (e.g., turning a user-specified portion of a web page into a widget).

[0096] In conjunction with touch screen 112, display controller 156, contact/motion module 130, graphics module 132, and text input module 134, search module 151 includes executable instructions to search for text, music, sound, image, video, and/or other files in memory 102 that match one or more search criteria (e.g., one or more user-specified search terms) in accordance with user instructions.

[0097] In conjunction with touch screen 112, display controller 156, contact/motion module 130, graphics module 132, audio circuitry 110, speaker 111, RF circuitry 108, and browser module 147, video and music player module 152 includes executable instructions that allow the user to download and play back recorded music and other sound files stored in one or more file formats, such as MP3 or AAC files, and executable instructions to display, present, or otherwise play back videos (e.g., on touch screen 112 or on an external, connected display via external port 124). In some embodiments, device 100 optionally includes the functionality of an MP3 player, such as an iPod (trademark of Apple Inc.).

[0098] In conjunction with touch screen 112, display controller 156, contact/motion module 130, graphics module 132, and text input module 134, notes module 153 includes executable instructions to create and manage notes, to-do lists, and the like in accordance with user instructions.

[0099] In conjunction with RF circuitry 108, touch screen 112, display controller 156, contact module 130, graphics module 132, text input module 134, GPS module 135, and browser module 147, map module 154 may be used to receive, display, modify, and store maps and data associated with maps (e.g., driving directions, data on stores and other points of interest at or near a particular location, and other location-based data) in accordance with user instructions.

[00100] In conjunction with touch screen 112, display controller 156, contact module 130, graphics module 132, audio circuitry 110, speaker 111, RF circuitry 108, text input module 134, e-mail client module 140, and browser module 147, online video module 155 includes instructions that allow the user to access, browse, receive (e.g., by streaming and/or download),

play back (e.g., on the touch screen or on an external, connected display via external port 124), send an e-mail with a link to a particular online video, and otherwise manage online videos in one or more file formats, such as H.264. In some embodiments, instant messaging module 141, rather than e-mail client module 140, is used to send a link to a particular online video.

Additional description of the online video application can be found in U.S. Provisional Patent Application No. 60/936,562, “Portable Multifunction Device, Method, and Graphical User Interface for Playing Online Videos,” filed June 20, 2007, and U.S. Patent Application No. 11/968,067, “Portable Multifunction Device, Method, and Graphical User Interface for Playing Online Videos,” filed December 31, 2007, the contents of which are hereby incorporated by reference in their entirety.

[00101] Each of the above-identified modules and applications corresponds to a set of executable instructions for performing one or more functions described above and the methods described in this application (e.g., the computer-implemented methods and other information processing methods described herein). These modules (e.g., sets of instructions) need not be implemented as separate software programs, procedures, or modules, and thus various subsets of these modules may be combined or otherwise rearranged in various embodiments. For example, video player module may be combined with music player module into a single module (e.g., video and music player module 152, FIG. 1A). In some embodiments, memory 102 may store a subset of the modules and data structures identified above. Furthermore, memory 102 may store additional modules and data structures not described above.

[00102] In some embodiments, device 100 is a device where operation of a predefined set of functions on the device is performed exclusively through a touch screen and/or a touchpad. By using a touch screen and/or a touchpad as the primary input control device for operation of device 100, the number of physical input control devices (such as push buttons, dials, and the like) on device 100 may be reduced.

[00103] The predefined set of functions that are performed exclusively through a touch screen and/or a touchpad optionally include navigation between user interfaces. In some embodiments, the touchpad, when touched by the user, navigates device 100 to a main, home, or root menu from any user interface that is displayed on device 100. In such embodiments, a “menu button”

2016102031 24 Nov 2016

is implemented using a touchpad. In some other embodiments, the menu button is a physical push button or other physical input control device instead of a touchpad.

[00104] FIG. 1B is a block diagram illustrating exemplary components for event handling in accordance with some embodiments. In some embodiments, memory 102 (FIG. 1A) or 370 (FIG. 3) includes event sorter 170 (e.g., in operating system 126) and a respective application 136-1 (e.g., any of the aforementioned applications 137-151, 155, 380-390).

[00105] Event sorter 170 receives event information and determines the application 136-1 and application view 191 of application 136-1 to which to deliver the event information. Event sorter 170 includes event monitor 171 and event dispatcher module 174. In some embodiments, application 136-1 includes application internal state 192, which indicates the current application view(s) displayed on touch-sensitive display 112 when the application is active or executing. In some embodiments, device/global internal state 157 is used by event sorter 170 to determine which application(s) is (are) currently active, and application internal state 192 is used by event sorter 170 to determine application views 191 to which to deliver event information.

[00106] In some embodiments, application internal state 192 includes additional information, such as one or more of: resume information to be used when application 136-1 resumes execution, user interface state information that indicates information being displayed or that is ready for display by application 136-1, a state queue for enabling the user to go back to a prior state or view of application 136-1, and a redo/undo queue of previous actions taken by the user.

[00107] Event monitor 171 receives event information from peripherals interface 118. Event information includes information about a sub-event (e.g., a user touch on touch-sensitive display 112, as part of a multi-touch gesture). Peripherals interface 118 transmits information it receives from I/O subsystem 106 or a sensor, such as proximity sensor 166, accelerometer(s) 168, and/or microphone 113 (through audio circuitry 110). Information that peripherals interface 118 receives from I/O subsystem 106 includes information from touch-sensitive display 112 or a touch-sensitive surface.

[00108] In some embodiments, event monitor 171 sends requests to the peripherals interface 118 at predetermined intervals. In response, peripherals interface 118 transmits event

information. In other embodiments, peripherals interface 118 transmits event information only when there is a significant event (e.g., receiving an input above a predetermined noise threshold and/or for more than a predetermined duration).

[00109] In some embodiments, event sorter 170 also includes a hit view determination module 172 and/or an active event recognizer determination module 173.

[00110] Hit view determination module 172 provides software procedures for determining where a sub-event has taken place within one or more views when touch-sensitive display 112 displays more than one view. Views are made up of controls and other elements that a user can see on the display.

[00111] Another aspect of the user interface associated with an application is a set of views, sometimes herein called application views or user interface windows, in which information is displayed and touch-based gestures occur. The application views (of a respective application) in which a touch is detected may correspond to programmatic levels within a programmatic or view hierarchy of the application. For example, the lowest level view in which a touch is detected may be called the hit view, and the set of events that are recognized as proper inputs may be determined based, at least in part, on the hit view of the initial touch that begins a touch-based gesture.

[00112] Hit view determination module 172 receives information related to sub-events of a touch-based gesture. When an application has multiple views organized in a hierarchy, hit view determination module 172 identifies a hit view as the lowest view in the hierarchy which should handle the sub-event. In most circumstances, the hit view is the lowest level view in which an initiating sub-event occurs (e.g., the first sub-event in the sequence of sub-events that form an event or potential event). Once the hit view is identified by the hit view determination module 172, the hit view typically receives all sub-events related to the same touch or input source for which it was identified as the hit view.

[00113] Active event recognizer determination module 173 determines which view or views within a view hierarchy should receive a particular sequence of sub-events. In some embodiments, active event recognizer determination module 173 determines that only the hit

24 Nov 2016

2016102031

view should receive a particular sequence of sub-events. In other embodiments, active event recognizer determination module 173 determines that all views that include the physical location of a sub-event are actively involved views, and therefore determines that all actively involved views should receive a particular sequence of sub-events. In other embodiments, even if touch sub-events were entirely confined to the area associated with one particular view, views higher in the hierarchy would still remain as actively involved views.

[00114] Event dispatcher module 174 dispatches the event information to an event recognizer (e.g., event recognizer 180). In embodiments including active event recognizer determination module 173, event dispatcher module 174 delivers the event information to an event recognizer determined by active event recognizer determination module 173. In some embodiments, event dispatcher module 174 stores in an event queue the event information, which is retrieved by a respective event receiver 182.

[00115] In some embodiments, operating system 126 includes event sorter 170. Alternatively, application 136-1 includes event sorter 170. In yet other embodiments, event sorter 170 is a stand-alone module, or a part of another module stored in memory 102, such as contact/motion module 130.

[00116] In some embodiments, application 136-1 includes a plurality of event handlers 190 and one or more application views 191, each of which includes instructions for handling touch events that occur within a respective view of the application's user interface. Each application view 191 of the application 136-1 includes one or more event recognizers 180. Typically, a respective application view 191 includes a plurality of event recognizers 180. In other embodiments, one or more of event recognizers 180 are part of a separate module, such as a user interface kit (not shown) or a higher level object from which application 136-1 inherits methods and other properties. In some embodiments, a respective event handler 190 includes one or more of: data updater 176, object updater 177, GUI updater 178, and/or event data 179 received from event sorter 170. Event handler 190 may utilize or call data updater 176, object updater 177, or GUI updater 178 to update the application internal state 192. Alternatively, one or more of the application views 191 include one or more respective event handlers 190. Also, in some

embodiments, one or more of data updater 176, object updater 177, and GUI updater 178 are included in a respective application view 191.

[00117] A respective event recognizer 180 receives event information (e.g., event data 179) from event sorter 170 and identifies an event from the event information. Event recognizer 180 includes event receiver 182 and event comparator 184. In some embodiments, event recognizer 180 also includes at least a subset of: metadata 183, and event delivery instructions 188 (which may include sub-event delivery instructions).

[00118] Event receiver 182 receives event information from event sorter 170. The event information includes information about a sub-event, for example, a touch or a touch movement. Depending on the sub-event, the event information also includes additional information, such as location of the sub-event. When the sub-event concerns motion of a touch, the event information may also include speed and direction of the sub-event. In some embodiments, events include rotation of the device from one orientation to another (e.g., from a portrait orientation to a landscape orientation, or vice versa), and the event information includes corresponding information about the current orientation (also called device attitude) of the device.

[00119] Event comparator 184 compares the event information to predefined event or sub-event definitions and, based on the comparison, determines an event or sub-event, or determines or updates the state of an event or sub-event. In some embodiments, event comparator 184 includes event definitions 186. Event definitions 186 contain definitions of events (e.g., predefined sequences of sub-events), for example, event 1 (187-1), event 2 (187-2), and others. In some embodiments, sub-events in an event (187) include, for example, touch begin, touch end, touch movement, touch cancellation, and multiple touching. In one example, the definition for event 1 (187-1) is a double tap on a displayed object. The double tap, for example, comprises a first touch (touch begin) on the displayed object for a predetermined phase, a first liftoff (touch end) for a predetermined phase, a second touch (touch begin) on the displayed object for a predetermined phase, and a second liftoff (touch end) for a predetermined phase. In another example, the definition for event 2 (187-2) is a dragging on a displayed object. The dragging, for example, comprises a touch (or contact) on the displayed object for a predetermined phase, a movement of the touch across touch-sensitive display 112, and liftoff of the touch (touch end).

In some embodiments, the event also includes information for one or more associated event handlers 190.

[00120] In some embodiments, event definition 187 includes a definition of an event for a respective user-interface object. In some embodiments, event comparator 184 performs a hit test to determine which user-interface object is associated with a sub-event. For example, in an application view in which three user-interface objects are displayed on touch-sensitive display 112, when a touch is detected on touch-sensitive display 112, event comparator 184 performs a hit test to determine which of the three user-interface objects is associated with the touch (sub-event). If each displayed object is associated with a respective event handler 190, the event comparator uses the result of the hit test to determine which event handler 190 should be activated. For example, event comparator 184 selects an event handler associated with the sub-event and the object triggering the hit test.

[00121] In some embodiments, the definition for a respective event (187) also includes delayed actions that delay delivery of the event information until after it has been determined whether the sequence of sub-events does or does not correspond to the event recognizer's event type.

[00122] When a respective event recognizer 180 determines that the series of sub-events do not match any of the events in event definitions 186, the respective event recognizer 180 enters an event impossible, event failed, or event ended state, after which it disregards subsequent sub-events of the touch-based gesture. In this situation, other event recognizers, if any, that remain active for the hit view continue to track and process sub-events of an ongoing touch-based gesture.

[00123] In some embodiments, a respective event recognizer 180 includes metadata 183 with configurable properties, flags, and/or lists that indicate how the event delivery system should perform sub-event delivery to actively involved event recognizers. In some embodiments, metadata 183 includes configurable properties, flags, and/or lists that indicate how event recognizers may interact, or are enabled to interact, with one another. In some embodiments, metadata 183 includes configurable properties, flags, and/or lists that indicate whether sub-events are delivered to varying levels in the view or programmatic hierarchy.

[00124] In some embodiments, a respective event recognizer 180 activates event handler 190 associated with an event when one or more particular sub-events of an event are recognized. In some embodiments, a respective event recognizer 180 delivers event information associated with the event to event handler 190. Activating an event handler 190 is distinct from sending (and deferred sending) sub-events to a respective hit view. In some embodiments, event recognizer 180 throws a flag associated with the recognized event, and event handler 190 associated with the flag catches the flag and performs a predefined process.

[00125] In some embodiments, event delivery instructions 188 include sub-event delivery instructions that deliver event information about a sub-event without activating an event handler. Instead, the sub-event delivery instructions deliver event information to event handlers associated with the series of sub-events or to actively involved views. Event handlers associated with the series of sub-events or with actively involved views receive the event information and perform a predetermined process.

[00126] In some embodiments, data updater 176 creates and updates data used in application 136-1. For example, data updater 176 updates the telephone number used in contacts module 137, or stores a video file used in video player module. In some embodiments, object updater 177 creates and updates objects used in application 136-1. For example, object updater 177 creates a new user-interface object or updates the position of a user-interface object. GUI updater 178 updates the GUI. For example, GUI updater 178 prepares display information and sends it to graphics module 132 for display on a touch-sensitive display.

[00127] In some embodiments, event handler(s) 190 includes or has access to data updater 176, object updater 177, and GUI updater 178. In some embodiments, data updater 176, object updater 177, and GUI updater 178 are included in a single module of a respective application 136-1 or application view 191. In other embodiments, they are included in two or more software modules.

[00128] It shall be understood that the foregoing discussion regarding event handling of user touches on touch-sensitive displays also applies to other forms of user inputs to operate multifunction devices 100 with input devices, not all of which are initiated on touch screens. For example, mouse movement and mouse button presses, optionally coordinated with single or

multiple keyboard presses or holds; contact movements such as taps, drags, scrolls, etc. on touchpads; pen stylus inputs; movement of the device; oral instructions; detected eye movements; biometric inputs; and/or any combination thereof are optionally utilized as inputs corresponding to sub-events which define an event to be recognized.

[00129] FIG. 2 illustrates a portable multifunction device 100 having a touch screen 112 in accordance with some embodiments. The touch screen optionally displays one or more graphics within user interface (UI) 200. In this embodiment, as well as others described below, a user is enabled to select one or more of the graphics by making a gesture on the graphics, for example, with one or more fingers 202 (not drawn to scale in the figure) or one or more styluses 203 (not drawn to scale in the figure). In some embodiments, selection of one or more graphics occurs when the user breaks contact with the one or more graphics. In some embodiments, the gesture optionally includes one or more taps, one or more swipes (from left to right, right to left, upward and/or downward), and/or a rolling of a finger (from right to left, left to right, upward and/or downward) that has made contact with device 100. In some implementations or circumstances, inadvertent contact with a graphic does not select the graphic. For example, a swipe gesture that sweeps over an application icon optionally does not select the corresponding application when the gesture corresponding to selection is a tap.

[00130] Device 100 may also include one or more physical buttons, such as “home” or menu button 204. As described previously, menu button 204 may be used to navigate to any application 136 in a set of applications that may be executed on device 100. Alternatively, in some embodiments, the menu button is implemented as a soft key in a GUI displayed on touch screen 112.

[00131] In one embodiment, device 100 includes touch screen 112, menu button 204, push button 206 for powering the device on/off and locking the device, volume adjustment button(s) 208, subscriber identity module (SIM) card slot 210, headset jack 212, and docking/charging external port 124. Push button 206 is, optionally, used to turn the power on/off on the device by depressing the button and holding the button in the depressed state for a predefined time interval; to lock the device by depressing the button and releasing the button before the predefined time interval has elapsed; and/or to unlock the device or initiate an unlock process. In an alternative

embodiment, device 100 also accepts verbal input for activation or deactivation of some functions through microphone 113. Device 100 also, optionally, includes one or more contact intensity sensors 165 for detecting intensity of contacts on touch screen 112 and/or one or more tactile output generators 167 for generating tactile outputs for a user of device 100.

[00132] FIG. 3 is a block diagram of an exemplary multifunction device with a display and a touch-sensitive surface in accordance with some embodiments. Device 300 need not be portable. In some embodiments, device 300 is a laptop computer, a desktop computer, a tablet computer, a multimedia player device, a navigation device, an educational device (such as a child's learning toy), a gaming system, or a control device (e.g., a home or industrial controller). Device 300 typically includes one or more processing units (CPUs) 310, one or more network or other communications interfaces 360, memory 370, and one or more communication buses 320 for interconnecting these components. Communication buses 320 optionally include circuitry (sometimes called a chipset) that interconnects and controls communications between system components. Device 300 includes input/output (I/O) interface 330 comprising display 340, which is typically a touch screen display. I/O interface 330 also optionally includes a keyboard and/or mouse (or other pointing device) 350 and touchpad 355, tactile output generator 357 for generating tactile outputs on device 300 (e.g., similar to tactile output generator(s) 167 described above with reference to FIG. 1A), sensors 359 (e.g., optical, acceleration, proximity, touch-sensitive, and/or contact intensity sensors similar to contact intensity sensor(s) 165 described above with reference to FIG. 1A). Memory 370 includes high-speed random access memory, such as DRAM, SRAM, DDR RAM, or other random access solid state memory devices; and optionally includes non-volatile memory, such as one or more magnetic disk storage devices, optical disk storage devices, flash memory devices, or other non-volatile solid state storage devices. Memory 370 optionally includes one or more storage devices remotely located from CPU(s) 310. In some embodiments, memory 370 stores programs, modules, and data structures analogous to the programs, modules, and data structures stored in memory 102 of portable multifunction device 100 (FIG. 1A), or a subset thereof. Furthermore, memory 370 optionally stores additional programs, modules, and data structures not present in memory 102 of portable multifunction device 100. For example, memory 370 of device 300 optionally stores drawing module 380, presentation module 382, word processing module 384, website creation module

386, disk authoring module 388, and/or spreadsheet module 390, while memory 102 of portable multifunction device 100 (FIG. 1A) optionally does not store these modules.

[00133] Each of the above-identified elements in FIG. 3 may be stored in one or more of the previously mentioned memory devices. Each of the above-identified modules corresponds to a set of instructions for performing a function described above. The above-identified modules or programs (e.g., sets of instructions) need not be implemented as separate software programs, procedures, or modules, and thus various subsets of these modules may be combined or otherwise rearranged in various embodiments. In some embodiments, memory 370 may store a subset of the modules and data structures identified above. Furthermore, memory 370 may store additional modules and data structures not described above.

[00134] Attention is now directed towards embodiments of user interfaces that may be implemented on, for example, portable multifunction device 100.

[00135] FIG. 4A illustrates an exemplary user interface for a menu of applications on portable multifunction device 100 in accordance with some embodiments. Similar user interfaces may be implemented on device 300. In some embodiments, user interface 400 includes the following elements, or a subset or superset thereof:

- Signal strength indicator(s) 402 for wireless communication(s), such as cellular and Wi-Fi signals;
- Time 404;
- Bluetooth indicator 405;
- Battery status indicator 406;
- Tray 408 with icons for frequently used applications, such as:
 - Icon 416 for telephone module 138, labeled “Phone,” which optionally includes an indicator 414 of the number of missed calls or voicemail messages;

2016102031 24 Nov 2016

- Icon 418 for e-mail client module 140, labeled “Mail,” which optionally includes an indicator 410 of the number of unread e-mails;
- Icon 420 for browser module 147, labeled “Browser;” and
- Icon 422 for video and music player module 152, also referred to as iPod (trademark of Apple Inc.) module 152, labeled “iPod;” and
- Icons for other applications, such as:
 - Icon 424 for IM module 141, labeled “Messages;”
 - Icon 426 for calendar module 148, labeled “Calendar;”
 - Icon 428 for image management module 144, labeled “Photos;”
 - Icon 430 for camera module 143, labeled “Camera;”
 - Icon 432 for online video module 155, labeled “Online Video;”
 - Icon 434 for stocks widget 149-2, labeled “Stocks;”
 - Icon 436 for map module 154, labeled “Maps;”
 - Icon 438 for weather widget 149-1, labeled “Weather;”
 - Icon 440 for alarm clock widget 149-4, labeled “Clock;”
 - Icon 442 for workout support module 142, labeled “Workout Support;”
 - Icon 444 for notes module 153, labeled “Notes;” and
 - Icon 446 for a settings application or module, labeled “Settings,” which provides access to settings for device 100 and its various applications 136.

[00136] It should be noted that the icon labels illustrated in FIG. 4A are merely exemplary. For example, icon 422 for video and music player module 152 may optionally be labeled “Music” or “Music Player.” Other labels are, optionally, used for various application icons. In some embodiments, a label for a respective application icon includes a name of an application corresponding to the respective application icon. In some embodiments, a label for a particular

application icon is distinct from a name of an application corresponding to the particular application icon.

[00137] FIG. 4B illustrates an exemplary user interface on a device (e.g., device 300, FIG. 3) with a touch-sensitive surface 451 (e.g., a tablet or touchpad 355, FIG. 3) that is separate from the display 450 (e.g., touch screen display 112). Device 300 also, optionally, includes one or more contact intensity sensors (e.g., one or more of sensors 357) for detecting intensity of contacts on touch-sensitive surface 451 and/or one or more tactile output generators 359 for generating tactile outputs for a user of device 300.

[00138] Although some of the examples which follow will be given with reference to inputs on touch screen display 112 (where the touch-sensitive surface and the display are combined), in some embodiments, the device detects inputs on a touch-sensitive surface that is separate from the display, as shown in FIG. 4B. In some embodiments, the touch-sensitive surface (e.g., 451 in FIG. 4B) has a primary axis (e.g., 452 in FIG. 4B) that corresponds to a primary axis (e.g., 453 in FIG. 4B) on the display (e.g., 450). In accordance with these embodiments, the device detects contacts (e.g., 460 and 462 in FIG. 4B) with the touch-sensitive surface 451 at locations that correspond to respective locations on the display (e.g., in FIG. 4B, 460 corresponds to 468 and 462 corresponds to 470). In this way, user inputs (e.g., contacts 460 and 462, and movements thereof) detected by the device on the touch-sensitive surface (e.g., 451 in FIG. 4B) are used by the device to manipulate the user interface on the display (e.g., 450 in FIG. 4B) of the multifunction device when the touch-sensitive surface is separate from the display. It should be understood that similar methods are, optionally, used for other user interfaces described herein.

[00139] Additionally, while the following examples are given primarily with reference to finger inputs (e.g., finger contacts, finger tap gestures, finger swipe gestures), it should be understood that, in some embodiments, one or more of the finger inputs are replaced with input from another input device (e.g., a mouse-based input or stylus input). For example, a swipe gesture is, optionally, replaced with a mouse click (e.g., instead of a contact) followed by movement of the cursor along the path of the swipe (e.g., instead of movement of the contact). As another example, a tap gesture is, optionally, replaced with a mouse click while the cursor is located over the location of the tap gesture (e.g., instead of detection of the contact followed by

ceasing to detect the contact). Similarly, when multiple user inputs are simultaneously detected, it should be understood that multiple computer mice are, optionally, used simultaneously, or a mouse and finger contacts are, optionally, used simultaneously.

[00140] FIG. 5A illustrates exemplary personal electronic device 500. Device 500 includes body 502. In some embodiments, device 500 can include some or all of the features described with respect to devices 100 and 300 (e.g., FIGS. 1A-4B). In some embodiments, device 500 has touch-sensitive display screen 504, hereafter touch screen 504. Alternatively, or in addition to touch screen 504, device 500 has a display and a touch-sensitive surface. As with devices 100 and 300, in some embodiments, touch screen 504 (or the touch-sensitive surface) may have one or more intensity sensors for detecting intensity of contacts (e.g., touches) being applied. The one or more intensity sensors of touch screen 504 (or the touch-sensitive surface) can provide output data that represents the intensity of touches. The user interface of device 500 can respond to touches based on their intensity, meaning that touches of different intensities can invoke different user interface operations on device 500.

[00141] Techniques for detecting and processing touch intensity may be found, for example, in related applications: International Patent Application Serial No. PCT/US2013/040061, titled “Device, Method, and Graphical User Interface for Displaying User Interface Objects Corresponding to an Application,” filed May 8, 2013, and International Patent Application Serial No. PCT/US2013/069483, titled “Device, Method, and Graphical User Interface for Transitioning Between Touch Input to Display Output Relationships,” filed November 11, 2013, each of which is hereby incorporated by reference in their entirety.

[00142] In some embodiments, device 500 has one or more input mechanisms 506 and 508. Input mechanisms 506 and 508, if included, can be physical. Examples of physical input mechanisms include push buttons and rotatable mechanisms. In some embodiments, device 500 has one or more attachment mechanisms. Such attachment mechanisms, if included, can permit attachment of device 500 with, for example, hats, eyewear, earrings, necklaces, shirts, jackets, bracelets, watch straps, chains, trousers, belts, shoes, purses, backpacks, and so forth. These attachment mechanisms may permit device 500 to be worn by a user.

[00143] FIG. 5B depicts exemplary personal electronic device 500. In some embodiments, device 500 can include some or all of the components described with respect to FIGS. 1A, 1B, and 3. Device 500 has bus 512 that operatively couples I/O section 514 with one or more computer processors 516 and memory 518. I/O section 514 can be connected to display 504, which can have touch-sensitive component 522 and, optionally, touch-intensity sensitive component 524. In addition, I/O section 514 can be connected with communication unit 530 for receiving application and operating system data, using Wi-Fi, Bluetooth, near field communication (NFC), cellular, and/or other wireless communication techniques. Device 500 can include input mechanisms 506 and/or 508. Input mechanism 506 may be a rotatable input device or a depressible and rotatable input device, for example. Input mechanism 508 may be a button, in some examples.

[00144] Input mechanism 508 may be a microphone, in some examples. Personal electronic device 500 can include various sensors, such as GPS sensor 532, accelerometer 534, directional sensor 540 (e.g., compass), gyroscope 536, motion sensor 538, and/or a combination thereof, all of which can be operatively connected to I/O section 514.

[00145] Memory 518 of personal electronic device 500 can be a non-transitory computer-readable storage medium, for storing computer-executable instructions, which, when executed by one or more computer processors 516, for example, can cause the computer processors to perform the techniques described above, including processes 700 (FIG. 7), 900 (FIG. 9), 1100 (FIG. 11), 1400, (FIG. 14), and 1600 (FIG. 16). The computer-executable instructions can also be stored and/or transported within any non-transitory computer-readable storage medium for use by or in connection with an instruction execution system, apparatus, or device, such as a computer-based system, processor-containing system, or other system that can fetch the instructions from the instruction execution system, apparatus, or device and execute the instructions. For purposes of this document, a “non-transitory computer-readable storage medium” can be any medium that can tangibly contain or store computer-executable instructions for use by or in connection with the instruction execution system, apparatus, or device. The non-transitory computer-readable storage medium can include, but is not limited to, magnetic, optical, and/or semiconductor storages. Examples of such storage include magnetic disks, optical discs based on CD, DVD, or Blu-ray technologies, as well as persistent solid-state

memory such as flash, solid-state drives, and the like. Personal electronic device 500 is not limited to the components and configuration of FIG. 5B, but can include other or additional components in multiple configurations.

[00146] As used here, the term “affordance” refers to a user-interactive graphical user interface object that may be displayed on the display screen of devices 100, 300, and/or 500 (FIGS. 1, 3, and 5). For example, an image (e.g., icon), a button, and text (e.g., hyperlink) may each constitute an affordance.

[00147] As used herein, the term “focus selector” refers to an input element that indicates a current part of a user interface with which a user is interacting. In some implementations that include a cursor or other location marker, the cursor acts as a “focus selector” so that when an input (e.g., a press input) is detected on a touch-sensitive surface (e.g., touchpad 355 in FIG. 3 or touch-sensitive surface 451 in FIG. 4B) while the cursor is over a particular user interface element (e.g., a button, window, slider or other user interface element), the particular user interface element is adjusted in accordance with the detected input. In some implementations that include a touch screen display (e.g., touch-sensitive display system 112 in FIG. 1A or touch screen 112 in FIG. 4A) that enables direct interaction with user interface elements on the touch screen display, a detected contact on the touch screen acts as a “focus selector” so that when an input (e.g., a press input by the contact) is detected on the touch screen display at a location of a particular user interface element (e.g., a button, window, slider, or other user interface element), the particular user interface element is adjusted in accordance with the detected input. In some implementations, focus is moved from one region of a user interface to another region of the user interface without corresponding movement of a cursor or movement of a contact on a touch screen display (e.g., by using a tab key or arrow keys to move focus from one button to another button); in these implementations, the focus selector moves in accordance with movement of focus between different regions of the user interface. Without regard to the specific form taken by the focus selector, the focus selector is generally the user interface element (or contact on a touch screen display) that is controlled by the user so as to communicate the user’s intended interaction with the user interface (e.g., by indicating, to the device, the element of the user interface with which the user is intending to interact). For example, the location of a focus selector (e.g., a cursor, a contact, or a selection box) over a respective button while a press input

is detected on the touch-sensitive surface (e.g., a touchpad or touch screen) will indicate that the user is intending to activate the respective button (as opposed to other user interface elements shown on a display of the device).

[00148] As used in the specification and claims, the term “characteristic intensity” of a contact refers to a characteristic of the contact based on one or more intensities of the contact. In some embodiments, the characteristic intensity is based on multiple intensity samples. The characteristic intensity is, optionally, based on a predefined number of intensity samples, or a set of intensity samples collected during a predetermined time period (e.g., 0.05, 0.1, 0.2, 0.5, 1, 2, 5, 10 seconds) relative to a predefined event (e.g., after detecting the contact, prior to detecting liftoff of the contact, before or after detecting a start of movement of the contact, prior to detecting an end of the contact, before or after detecting an increase in intensity of the contact, and/or before or after detecting a decrease in intensity of the contact). A characteristic intensity of a contact is, optionally based on one or more of: a maximum value of the intensities of the contact, a mean value of the intensities of the contact, an average value of the intensities of the contact, a top 10 percentile value of the intensities of the contact, a value at the half maximum of the intensities of the contact, a value at the 90 percent maximum of the intensities of the contact, or the like. In some embodiments, the duration of the contact is used in determining the characteristic intensity (e.g., when the characteristic intensity is an average of the intensity of the contact over time). In some embodiments, the characteristic intensity is compared to a set of one or more intensity thresholds to determine whether an operation has been performed by a user. For example, the set of one or more intensity thresholds may include a first intensity threshold and a second intensity threshold. In this example, a contact with a characteristic intensity that does not exceed the first threshold results in a first operation, a contact with a characteristic intensity that exceeds the first intensity threshold and does not exceed the second intensity threshold results in a second operation, and a contact with a characteristic intensity that exceeds the second threshold results in a third operation. In some embodiments, a comparison between the characteristic intensity and one or more thresholds is used to determine whether or not to perform one or more operations (e.g., whether to perform a respective operation or forgo performing the respective operation) rather than being used to determine whether to perform a first operation or a second operation.

[00149] In some embodiments, a portion of a gesture is identified for purposes of determining a characteristic intensity. For example, a touch-sensitive surface may receive a continuous swipe contact transitioning from a start location and reaching an end location, at which point the intensity of the contact increases. In this example, the characteristic intensity of the contact at the end location may be based on only a portion of the continuous swipe contact, and not the entire swipe contact (e.g., only the portion of the swipe contact at the end location). In some embodiments, a smoothing algorithm may be applied to the intensities of the swipe contact prior to determining the characteristic intensity of the contact. For example, the smoothing algorithm optionally includes one or more of: an unweighted sliding-average smoothing algorithm, a triangular smoothing algorithm, a median filter smoothing algorithm, and/or an exponential smoothing algorithm. In some circumstances, these smoothing algorithms eliminate narrow spikes or dips in the intensities of the swipe contact for purposes of determining a characteristic intensity.

[00150] The intensity of a contact on the touch-sensitive surface may be characterized relative to one or more intensity thresholds, such as a contact-detection intensity threshold, a light press intensity threshold, a deep press intensity threshold, and/or one or more other intensity thresholds. In some embodiments, the light press intensity threshold corresponds to an intensity at which the device will perform operations typically associated with clicking a button of a physical mouse or a trackpad. In some embodiments, the deep press intensity threshold corresponds to an intensity at which the device will perform operations that are different from operations typically associated with clicking a button of a physical mouse or a trackpad. In some embodiments, when a contact is detected with a characteristic intensity below the light press intensity threshold (e.g., and above a nominal contact-detection intensity threshold below which the contact is no longer detected), the device will move a focus selector in accordance with movement of the contact on the touch-sensitive surface without performing an operation associated with the light press intensity threshold or the deep press intensity threshold. Generally, unless otherwise stated, these intensity thresholds are consistent between different sets of user interface figures.

[00151] An increase of characteristic intensity of the contact from an intensity below the light press intensity threshold to an intensity between the light press intensity threshold and the deep

press intensity threshold is sometimes referred to as a “light press” input. An increase of characteristic intensity of the contact from an intensity below the deep press intensity threshold to an intensity above the deep press intensity threshold is sometimes referred to as a “deep press” input. An increase of characteristic intensity of the contact from an intensity below the contact-detection intensity threshold to an intensity between the contact-detection intensity threshold and the light press intensity threshold is sometimes referred to as detecting the contact on the touch-surface. A decrease of characteristic intensity of the contact from an intensity above the contact-detection intensity threshold to an intensity below the contact-detection intensity threshold is sometimes referred to as detecting liftoff of the contact from the touch-surface. In some embodiments the contact-detection intensity threshold is zero. In some embodiments, the contact-detection intensity threshold is greater than zero.

[00152] In some embodiments described herein, one or more operations are performed in response to detecting a gesture that includes a respective press input or in response to detecting the respective press input performed with a respective contact (or a plurality of contacts), where the respective press input is detected based at least in part on detecting an increase in intensity of the contact (or plurality of contacts) above a press-input intensity threshold. In some embodiments, the respective operation is performed in response to detecting the increase in intensity of the respective contact above the press-input intensity threshold (e.g., a “down stroke” of the respective press input). In some embodiments, the press input includes an increase in intensity of the respective contact above the press-input intensity threshold and a subsequent decrease in intensity of the contact below the press-input intensity threshold, and the respective operation is performed in response to detecting the subsequent decrease in intensity of the respective contact below the press-input threshold (e.g., an “up stroke” of the respective press input).

[00153] In some embodiments, the device employs intensity hysteresis to avoid accidental inputs sometimes termed “jitter,” where the device defines or selects a hysteresis intensity threshold with a predefined relationship to the press-input intensity threshold (e.g., the hysteresis intensity threshold is X intensity units lower than the press-input intensity threshold or the hysteresis intensity threshold is 75%, 90%, or some reasonable proportion of the press-input intensity threshold). Thus, in some embodiments, the press input includes an increase in

intensity of the respective contact above the press-input intensity threshold and a subsequent decrease in intensity of the contact below the hysteresis intensity threshold that corresponds to the press-input intensity threshold, and the respective operation is performed in response to detecting the subsequent decrease in intensity of the respective contact below the hysteresis intensity threshold (e.g., an “up stroke” of the respective press input). Similarly, in some embodiments, the press input is detected only when the device detects an increase in intensity of the contact from an intensity at or below the hysteresis intensity threshold to an intensity at or above the press-input intensity threshold and, optionally, a subsequent decrease in intensity of the contact to an intensity at or below the hysteresis intensity, and the respective operation is performed in response to detecting the press input (e.g., the increase in intensity of the contact or the decrease in intensity of the contact, depending on the circumstances).

[00154] For ease of explanation, the descriptions of operations performed in response to a press input associated with a press-input intensity threshold or in response to a gesture including the press input are, optionally, triggered in response to detecting either: an increase in intensity of a contact above the press-input intensity threshold, an increase in intensity of a contact from an intensity below the hysteresis intensity threshold to an intensity above the press-input intensity threshold, a decrease in intensity of the contact below the press-input intensity threshold, and/or a decrease in intensity of the contact below the hysteresis intensity threshold corresponding to the press-input intensity threshold. Additionally, in examples where an operation is described as being performed in response to detecting a decrease in intensity of a contact below the press-input intensity threshold, the operation is, optionally, performed in response to detecting a decrease in intensity of the contact below a hysteresis intensity threshold corresponding to, and lower than, the press-input intensity threshold.

[00155] FIG. 5C illustrates exemplary devices connected via one or more communication channels to complete a payment transaction in accordance with some embodiments. One or more exemplary electronic devices (e.g., devices 100, 300, and 500) are configured to optionally detect input (e.g., a particular user input, an NFC field) and optionally transmit payment information (e.g., using NFC). The one or more electronic devices optionally include NFC hardware and are configured to be NFC-enabled.

[00156] The electronic devices (e.g., devices 100, 300, and 500) are optionally configured to store payment account information associated with each of one or more payment accounts. Payment account information includes, for example, one or more of: a person's or company's name, a billing address, a login, a password, an account number, an expiration date, a security code, a telephone number, a bank associated with the payment account (e.g., an issuing bank), and a card network identifier. In some examples, payment account information includes include an image, such as a picture of a payment card (e.g., taken by the device and/or received at the device). In some examples, the electronic devices receive user input including at least some payment account information (e.g., receiving user-entered credit, debit, account, or gift card number and expiration date). In some examples, the electronic devices detect at least some payment account information from an image (e.g., of a payment card captured by a camera sensor of the device). In some examples, the electronic devices receive at least some payment account information from another device (e.g., another user device or a server). In some examples, the electronic device receives payment account information from a server associated with another service for which an account for a user or user device previously made a purchase or identified payment account data (e.g., an app for renting or selling audio and/or video files).

[00157] In some embodiments, a payment account is added to an electronic device (e.g., device 100, 300, and 500), such that payment account information is securely stored on the electronic device. In some examples, after a user initiates such process, the electronic device transmits information for the payment account to a transaction-coordination server, which then communicates with a server operated by a payment network for the account (e.g., a payment server) to ensure a validity of the information. The electronic device is optionally configured to receive a script from the server that allows the electronic device to program payment information for the account onto the secure element.

[00158] In some embodiments, communication among electronic devices 100, 300, and 500 facilitates transactions (e.g., generally or specific transactions). For example, a first electronic device (e.g., 100) can serve as a provisioning or managing device, and can send notifications of new or updated payment account data (e.g., information for a new account, updated information for an existing account, and/or an alert pertaining to an existing account) to a second electronic device (e.g., 500). In another example, a first electronic device (e.g., 100) can send data to a

second election device, wherein the data reflects information about payment transactions facilitated at the first electronic device. The information optionally includes one or more of: a payment amount, an account used, a time of purchase, and whether a default account was changed. The second device (e.g., 500) optionally uses such information to update a default payment account (e.g., based on a learning algorithm or explicit user input).

[00159] Electronic devices (e.g., 100, 300, 500) are configured to communicate with each other over any of a variety of networks. For example, the devices communicate using a Bluetooth connection 550 (e.g., which includes a traditional Bluetooth connection or a Bluetooth Low Energy connection) or using a WiFi network 552. Communications among user devices are, optionally, conditioned to reduce the possibility of inappropriately sharing information across devices. For example, communications relating to payment information requires that the communicating devices be paired (e.g., be associated with each other via an explicit user interaction) or be associated with a same user account.

[00160] In some embodiments, an electronic device (e.g., 100, 300, 500) is used to communicate with a point-of-sale (POS) payment terminal 850, which is optionally NFC-enabled. The communication optionally occurs using a variety of communication channels and/or technologies. In one examples, electronic device (e.g., 100, 300, 500) communicates with payment terminal 850 using an NFC channel 554. In some examples, payment terminal 850 communicates with an electronic device (e.g., 100, 300, 500) using a peer-to-peer NFC mode. Electronic device (e.g., 100, 300, 500) is optionally configured transmit a signal to payment terminal 850 that includes payment information for a payment account (e.g., a default account or an account selected for the particular transaction).

[00161] In some embodiments, generation of and/or transmission of the signal is controlled by a secure element in the electronic device (e.g., 100, 300, 500). The secure element optionally requires a particular user input prior to releasing payment information. For example, the secure element optionally requires detection that the electronic device is being worn, detection of a button press, detection of entry of a passcode, detection of a touch, detection of one or more option selections (e.g., received while interacting with an application), detection of a fingerprint signature, detection of a voice or voice command, and or detection of a gesture or movement

(e.g., rotation or acceleration). In some examples, if a communication channel (e.g., an NFC communication channel) with another device (e.g., payment terminal 850) is established within a defined time period from detection of the input, the secure element releases payment information to be transmitted to the other device (e.g., payment terminal 850). In some examples, the secure element is a hardware component that controls release of secure information. In some examples, the secure element is a software component that controls release of secure information.

[00162] In some embodiments, protocols related to transaction participation depend on, for example, device types. For example, a condition for generating and/or transmitting payment information can be different for a wearable device (e.g., device 500) and a phone (e.g., device 100). For example, a generation and/or transmission condition for a wearable device includes detecting that a button has been pressed (e.g., after a security verification), while a corresponding condition for a phone does not require button-depression and instead requires detection of particular interaction with an application. In some examples, a condition for transmitting and/or releasing payment information includes receiving particular input on each of multiple devices. For example, release of payment information optionally requires detection of a fingerprint and/or passcode at the device (e.g., device 100) and detection of a mechanical input (e.g., button press) on another device (e.g., device 500).

[00163] Payment terminal 850 optionally uses the payment information to generate a signal to transmit to a payment server 560 to determine whether the payment is authorized. Payment server 560 optionally includes any device or system configured to receive payment information associated with a payment account and to determine whether a proposed purchase is authorized. In some examples, payment server 560 includes a server of an issuing bank. Payment terminal 850 communicates with payment server 560 directly or indirectly via one or more other devices or systems (e.g., a server of an acquiring bank and/or a server of a card network).

[00164] Payment server 560 optionally uses at least some of the payment information to identify a user account from among a database of user accounts (e.g., 562). For example, each user account includes payment information. An account is, optionally, located by locating an account with particular payment information matching that from the POS communication. In some examples, a payment is denied when provided payment information is not consistent (e.g.,

an expiration date does not correspond to a credit, debit or gift card number) or when no account includes payment information matching that from the POS communication.

[00165] In some embodiments, data for the user account further identifies one or more restrictions (e.g., credit limits); current or previous balances; previous transaction dates, locations and/or amounts; account status (e.g., active or frozen), and/or authorization instructions. In some examples, the payment server (e.g., 560) uses such data to determine whether to authorize a payment. For example, a payment server denies a payment when a purchase amount added to a current balance would result in exceeding an account limit, when an account is frozen, when a previous transaction amount exceeds a threshold, or when a previous transaction count or frequency exceeds a threshold.

[00166] In some embodiments, payment server 560 responds to POS payment terminal 850 with an indication as to whether a proposed purchase is authorized or denied. In some examples, POS payment terminal 850 transmits a signal to the electronic device (e.g., 100, 300, 500) to identify the result. For example, POS payment terminal 850 sends a receipt to the electronic device (e.g., 100, 300, 500) when a purchase is authorized (e.g., via a transaction-coordination server that manages a transaction app on the user device). In some instances, POS payment terminal 850 presents an output (e.g., a visual or audio output) indicative of the result. Payment can be sent to a merchant as part of the authorization process or can be subsequently sent.

[00167] In some embodiments, the electronic device (e.g., 100, 300, 500) participates in a transaction that is completed without involvement of POS payment terminal 850. For example, upon detecting that a mechanical input has been received, a secure element in the electronic device (e.g., 100, 300, 500) releases payment information to allow an application on the electronic device to access the information (e.g., and to transmit the information to a server associated with the application).

[00168] FIGS. 6A-6O illustrate exemplary user interfaces for conducting a payment transaction in accordance with some embodiments. The user interfaces in these figures are used to illustrate the processes described below, including the process in FIG. 7.

[00169] The payment technique allows a user to both authorize with the electronic device (e.g., using a fingerprint or a device passcode) and to authorize with a remote server (such as a bank). The two authorizations each require their own authorization data, which are provided by the user. This payment technique is more secure and convenient than other payment techniques.

[00170] FIG. 6A illustrates an exemplary user interface for conducting a payment transaction in accordance with some embodiments. At FIG. 6A, an electronic device 100 displays a user interface for a first application 602 (e.g., a third-party merchant application or a web browser-accessed website). The user interface for the first application 602 includes a payment affordance 610 (e.g., a submit button to buy contents of a shopping cart) associated with a payment transaction (e.g., a purchase to be made). For example, the payment affordance 610 may be a submit button to initiate the purchase of the contents of an electronic shopping cart 604. In the illustrated example of FIG. 6A, the electronic shopping cart 604 includes multiple clothing items 606.

[00171] The electronic device detects a request to initiate a payment transaction (e.g., detecting selection of payment affordance 610 associated with the payment transaction; a user taps the payment affordance 610). In response to detecting the request to initiate the payment transaction, the device displays a payment user interface 620, as illustrated in FIG. 6B.

[00172] In some embodiments, the payment user interface is of a second application. For example, the second application may be part of the operating system of the electronic device, and the second application has access to an electronic wallet of the device. In some embodiments, the second application is a first-party application provided by a provider of the operating system of the electronic device, and the second application has access to an electronic wallet of the device.

[00173] At FIG. 6B, the payment user interface 620 optionally includes an indication of a default/selected payment account 624, a name (e.g., cardholder's name) associated with the payment account, billing address, ship-to address 626, shipping method 628, contact information 630, a subtotal 630, a tax amount 634, a shipping amount 636, and a total 638.

[00174] FIGS. 6C-6D illustrate exemplary user interfaces for changing an option of the payment transaction in accordance with some embodiments. In some embodiments, the electronic device receives a selection of (e.g., user taps on) a purchase detail affordance (e.g., caret associated with payment account 624A, shipping address 626A, shipping method 628A, contact information 630A) displayed on the payment user interface 620. The first purchase detail affordance 624A is associated with a first purchase detail (e.g., the selected payment account, shipping address, shipping method, contact information) of the payment transaction. In response to receiving selection of the first purchase detail affordance 624A, the device displays one or more affordances (e.g., displays different options for payment accounts) for selecting an alternate value for the first purchase detail of the payment transaction. For example, when a user selects caret 624A in FIG. 6C, which relates to a payment account for the first purchase detail, the device displays several payment account options 660 and 662 for the first purchase detail, as illustrated in FIG. 6D. The currently selected payment account option 660 is identified, such as by checkmark 664. Thus, the user can change the default payment account 624 that will be used for the payment transaction.

[00175] At FIGS. 6E-6F, while displaying the payment user interface 620, the electronic device receives first authorization data (e.g., fingerprint authentication information or a device passcode). In this example, a fingerprint authentication technique is illustrated, as indicated by visual indicator 650A of FIG. 6E instructing the user to provide authentication using fingerprint sensor 204 and visual indicator 650B of FIG. 6F indicating to the user that the user's fingerprint is being read using fingerprint sensor 204.

[00176] After receiving the first authorization data, the electronic device determines (e.g., at the electronic device) whether the first authorization data is valid (e.g., the electronic device confirms that the fingerprint or device passcode is authorized for payments). At FIG. 6G, the device has determined that the first authorization data is valid (e.g., that the fingerprint is authorized for payments), as indicated by visual indicator 656.

[00177] At FIG. 6H, the electronic device receives second authorization data (e.g., a bank personal identification number (pin) authorization code, such as a six-digit numerical value). In this example, the electronic device prompts the user for the second authorization data and

receives the second authorization data after receiving the first authorization data. In the example of FIG. 6H, the user may enter the second authorization data using, for example, a keypad. The second authorization data is not limited to keypad entry. The user may provide the second authorization data using a fingerprint sensor, voice commands, or using other techniques. In some examples, the electronic device may receive the second authorization data before receiving the first authorization data.

[00178] After receiving the first authorization data and the second authorization data, the electronic device transmits a transaction request (e.g., the transaction request is based on the second authorization data) that corresponds to the payment transaction to one or more remote servers. The electronic device receives a reply to the transaction request. For example, the reply to the transaction request is received from the one or more remote servers or a separate server in communication with the one or more remote servers.

[00179] In response to receiving the reply to the transaction request, in accordance with a determination that the transaction request was successful (e.g., that the reply indicates that the transaction request contains valid or authorized second authorization data), the device dismisses the payment user interface (and, optionally, provides an indication of the success of the transaction). For example, at FIG. 6I, the electronic device has received the reply to the transaction request and determined that the transaction request was successful. In accordance with the determination, the device dismisses the payment user interface 620 (e.g., payment user interface 620 is no longer displayed) and displays a confirmation user interface 662 of the first application, including an order number 664.

[00180] In response to receiving the reply to the transaction request, in accordance with a determination that the transaction request failed (e.g., that the reply indicates that the transaction request did not contain a valid or authorized second authorization data or because of insufficient funds in the payment account), the electronic device maintains display of the payment user interface 620 and updates the payment user interface 620 to display an indication of a reason for failure 666 of the transaction request, such as illustrated in FIG. 6J.

[00181] In some embodiments, the indication of the reason for failure of the transaction request comprises an indication that the transaction request failed due to a merchant associated

with the payment transaction (e.g., the items from the shopping cart can't be shipped to the provided address or the items from the shopping cart are out of stock) or an indication (e.g., indication 666 of FIG. 6J) that the transaction request failed due to a financial institution (e.g., a bank or other authorizing agent) associated with the payment transaction (e.g., the financial institution determined that there are insufficient funds or that the second authorization data is invalid or not authorized).

[00182] In some embodiments, displaying the payment user interface 620 (e.g., a user interface of an operating system) comprises displaying the payment user interface 620 over only a portion of a first user interface (e.g., a user interface of a third-party merchant application or a web browser-accessed website). For example, payment user interface 620 is displayed such that the payment user interface 620 only covers a portion and not all of the first user interface (e.g., the user interface for first application 602, a third-party merchant application, or a web browser-accessed website), thus providing context of the payment transaction initiated using the first user interface. For example, in FIG. 6B, the payment user interface 620 (which, for example, includes displayed items 624, 626, 628, 630, 624A, 626A, 628A, 630A, 632, 634, 636, 638, and 650A) covers the bottom portion of the display of device 100, leaving the top portion of the user interface for the first application 602 visible, including part of the electronic shopping cart 604 and one of the clothing items 606 (e.g., the navy blue shirt for \$85.00).

[00183] In some embodiments, transmitting the transaction request comprises transmitting the transaction request while displaying the payment user interface 620 and receiving the reply to the transaction request comprises receiving the reply to the transaction request while displaying the payment user interface 620. Thus, the transaction request is sent and a reply is received while the payment user interface 620 is displayed. This limits the need to display different user interfaces.

[00184] In some embodiments, in accordance with a determination that the transaction request was successful (and optionally a determination that the second authorization data (e.g., a bank pin authorization code) is not currently stored), the electronic device stores (e.g., in memory of the electronic device) the second authorization data (e.g., the bank pin authorization code) and/or stores (e.g., in memory of the electronic device) a representation of the second authorization data

(e.g., an encrypted version of the bank pin authorization code). In accordance with a determination that the transaction request failed, the electronic device forgoes storing (e.g., not storing in memory of the electronic device) the second authorization data (e.g., a bank pin authorization code). Thus, when the user conducts a payment transaction, the device determines whether the payment transaction was successful. If the payment transaction was not successful (e.g., the financial institution indicated that the second authorization data was invalid or not authorized), the electronic device does not store the second authorization data for re-use in the future (because the second authorization data is invalid) and associating the stored second authorization data with the selected payment account.

[00185] As illustrated in FIG. 6K, in some embodiments, the electronic device detects a second request (e.g., detecting selection of second payment affordance 676 associated with a second payment transaction; a user taps the second payment affordance 676 during a different shopping experience using an application different from the first application) to initiate a second payment transaction. For example, as illustrated in FIG. 6K, the second payment affordance 676 may be displayed as part of a user interface 670 of an application that is different from the first application. The user interface 670 may include an advertisement 672 and items 674 in an electronic shopping cart.

[00186] At FIG. 6L, in response to detecting the second request to initiate the second payment transaction, the electronic device displays a second payment user interface 676. At FIG. 6M, while displaying the second payment user interface 676, the electronic device receives third authorization data (e.g., fingerprint authentication information or device passcode). In some examples, the third authorization data has the same value (or represents the same fingerprint) as the first authorization data. After receiving the third authorization data, the electronic device determines (e.g., at the electronic device) whether the third authorization data is valid (e.g., the electronic device confirms that the fingerprint or device passcode is authorized for payments), as indicated by indicator 678 of FIG. 6M and indicator 680 of FIG. 6N.

[00187] After receiving the third authorization data (and without receiving the second authorization data from the user again (e.g., without requesting or receiving the bank pin authorization code again from the user)), the electronic device transmits a second transaction

request (e.g., based on (or including) the stored second authorization data or a representation of the stored second authorization data) that corresponds to the second payment transaction to one or more remote servers. The second transaction request is based at least in part on a stored representation of the second authorization data. Optionally, the electronic device transmits the second transaction request only after determining that the third authorization data is valid, such as indicated by indicator 680 of FIG. 6N. The electronic device receives (e.g., from the one or more remote servers) a reply to the second transaction request.

[00188] In response to receiving the reply to the second transaction request, in accordance with a determination that the second transaction request was successful, the electronic device dismisses the second payment user interface (and, optionally, providing an indication of the success of the transaction), as illustrated in FIG. 6O. In response to receiving the reply to the second transaction request, in accordance with a determination that the second transaction request failed, maintaining display of the second payment user interface and updating the second payment user interface to display a second indication of a second reason for failure of the second transaction request.

[00189] In some embodiments, transmitting the transaction request (e.g., based on the stored second authorization data) that corresponds to the payment transaction to the one or more remote servers comprises transmitting the second authorization data to a financial institution (e.g., a bank or other authorizing agent).

[00190] In some embodiments, in accordance with the determination that the transaction request failed (e.g., insufficient funds, wrong pin): while displaying the payment user interface, the electronic device receives third authorization data (e.g., fingerprint authentication information or a device passcode); after receiving the third authorization data, the electronic device determines (e.g., at the electronic device) whether the third authorization data is valid (e.g., confirms that the fingerprint or device passcode is authorized for payments). The electronic device receives fourth authorization data (e.g., a bank pin authorization code). After receiving the third authorization data and the fourth authorization data, the electronic device transmits a second transaction request (e.g., based on the stored second authorization data) that corresponds to the payment transaction to one or more remote servers; and the electronic device

2016102031 24 Nov 2016

receives a second reply to the transaction request (e.g., from the one or more remote servers). Thus, for example, if the transaction request fails, as illustrated in FIG. 6J, and the user initiates a second attempt to complete the transaction, the user must again authenticate using two authentication methods, such as using fingerprint authorization that is authenticated locally, as illustrated in FIG. 6F, and using a bank pin authorization code that is authenticated at a remote server, as illustrated in FIG. 6H.

[00191] In some embodiments, receiving first authorization data (e.g., fingerprint authentication information or a device passcode) comprises detecting a respective fingerprint on a fingerprint sensor of the electronic device, and wherein determining (e.g., at the electronic device) whether the first authorization data is valid (e.g., confirm that the fingerprint authentication information or device passcode is authorized for payments) comprises determining whether the respective fingerprint is consistent with an enrolled fingerprint that is enabled to authorize payment transactions.

[00192] In some embodiments, receiving first authorization data (e.g., fingerprint authentication information or a device passcode) comprises receiving a payment passcode (e.g., using a physical or displayed keypad), and determining (e.g., at the electronic device) whether the first authorization data is valid (e.g., confirming that the fingerprint or device passcode is authorized for payments) comprises determining whether the payment passcode is consistent with an enrolled passcode that is enabled to authorize payment transactions.

[00193] In some embodiments, the first authorization data is different from the second authorization data (e.g., the device passcode is different than the bank pin authorization code). For example, the user may have previously selected a device passcode for making payments using the electronic device (and/or unlocking the electronic device) and the user may have previously selected (or have been assigned) a separate bank pin authorization code for making payments using a particular payment account.

[00194] In some embodiments, the second authorization data may not be needed when the electronic device is within a particular country or region, and the second authorization data may be needed when the electronic device is not within the particular country or region. This policy may be, for example, set by the bank that services the payment account. The electronic device

determines a current location of the electronic device. The second authorization data is requested from the user (and subsequently received) in accordance with determining that the current location of the electronic device is within a first predefined geographical area (e.g., a first country or other geographical area in which a second form of authentication is required to authorize payment transactions). In contrast, in accordance with a determination that the electronic device is in a second predefined geographical area (e.g., outside of the first predefined geographical area or in a second country different from the first country), the electronic device authenticates the payment transaction with only a single form of authentication (e.g., the electronic device only requests and uses the first authorization data). For example, the bank processing the payment request may require that the payment request include the bank pin authorization code when the electronic device is within a particular country.

[00195] In some embodiments, the electronic device determines whether a payment amount of the payment transaction meets a predefined criteria (e.g., the payment amount is larger than a threshold payment amount). The second authorization data is (e.g., only) requested from the user (and subsequently received) in accordance with a determination that the payment amount of the payment transaction meets a predefined criteria (e.g., the payment amount is larger than a threshold payment amount). In contrast, in accordance with a determination that the payment amount of the payment transaction does not meet the predefined criteria (e.g., the payment amount is equal to or less than the threshold payment amount), the electronic device authenticates the payment transaction with only a single form of authentication (e.g., the electronic device only requests and uses the first authorization data). For example, the user may have previously requested that the bank pin authorization code only be transmitted to the one or more servers when the total amount (e.g., price) of the transaction exceeds a certain amount. For another example, the bank processing the payment request may require that the payment request include the bank pin authorization code when the total amount of the transaction exceeds a certain amount.

[00196] In some embodiments, a first entropy of the first authorization data is higher than a second entropy of the second authorization data (e.g., it is more difficult to guess the user's device passcode than to guess the bank pin authorization code). This is particularly helpful when

the electronic device stores the bank pin authorization code (or a representation of the bank pin authorization code) and thus the electronic device must protect the bank pin authorization code.

[00197] FIG. 7 is a flow diagram illustrating a method for conducting a payment transaction using an electronic device in accordance with some embodiments. Method 700 is performed at a device (e.g., 100, 300, 500). Some operations in method 700 may be combined, the order of some operations may be changed, and some operations may be omitted.

[00198] As described below, method 700 provides an intuitive way for conducting a payment transaction. The method reduces the cognitive burden on a user for conducting the payment transaction, thereby creating a more efficient human-machine interface. For battery-operated computing devices, enabling a user to conduct payment transactions faster and more efficiently conserves power and increases the time between battery charges.

[00199] At block 702, the electronic device detects a request to initiate a payment transaction. For example, the device detects selection of a payment affordance (e.g., 610 of FIG. 6A) associated with a payment transaction.

[00200] At block 704, in response to detecting the request to initiate the payment transaction, the electronic device displays a payment user interface (e.g., 620 of FIG. 6B).

[00201] At block 706, while displaying the payment user interface, the electronic device receives first authorization data (e.g., fingerprint authentication information or a device passcode).

[00202] At block 708, after receiving the first authorization data, the electronic device determines (e.g., at the electronic device) whether the first authorization data is valid (e.g., the electronic device confirms that the fingerprint or device passcode is authorized for payments).

[00203] At block 710, the electronic device receives second authorization data (e.g., a bank pin authorization code).

[00204] At block 712, after receiving the first authorization data (e.g., fingerprint authentication information or a device passcode) and the second authorization data (e.g., a bank pin authorization code), the electronic device transmits a transaction request (e.g., based on the

2016102031 24 Nov 2016

second authorization data) that corresponds to the payment transaction to one or more remote servers.

[00205] At block 714, the electronic device receives a reply to the transaction request.

[00206] At block 716, in response to receiving the reply to the transaction request: in accordance with a determination that the transaction request was successful, the electronic device dismisses the payment user interface (and, optionally, providing an indication of the success of the transaction); and in accordance with a determination that the transaction request failed (e.g., because of insufficient funds, wrong bank pin authorization code), the electronic device maintains display of the payment user interface (e.g., 620) and updates the payment user interface (e.g., 620) to display an indication (e.g., 666 of FIG. 6J) of a reason for failure of the transaction request.

[00207] In some embodiments, the indication (e.g., 666 of FIG. 6J) of the reason for failure of the transaction request comprises: an indication that the transaction request failed due to a merchant associated with the payment transaction (e.g., items can't be shipped to provided address or items out of stock); or an indication (e.g., 666 of FIG. 6J) that the transaction request failed due to a financial institution (e.g., a bank or other authorizing agent) associated with the payment transaction (e.g., insufficient funds, wrong bank pin authorization code).

[00208] In some embodiments, displaying the payment user interface (e.g., 620) comprises displaying the payment user interface (e.g., 620) over only a portion of a first user interface (e.g., 602) (e.g., such that the payment user interface only covers a portion and not all of the first user interface, thus providing context of the transaction initiated using the first user interface).

[00209] In some embodiments, transmitting the transaction request comprises transmitting the transaction request while displaying the payment user interface (e.g., 620) and wherein receiving the reply to the transaction request comprises receiving the reply to the transaction request while displaying the payment user interface (e.g., 620).

[00210] In some embodiments, in accordance with a determination that the transaction request was successful (and optionally a determination that the bank pin authorization code is not currently stored), the electronic device stores (e.g., in memory of the electronic device) the

second authorization data (e.g., the bank pin authorization code). In accordance with a determination that the transaction request failed, the electronic device forgoes storing (e.g., not storing in memory of the electronic device) the second authorization data (e.g., a bank pin authorization code).

[00211] In some embodiments, the electronic device detects a second request to initiate a second payment transaction (e.g., detecting selection of another payment affordance 676 associated with a second payment transaction). In response to detecting the second request to initiate the second payment transaction, the electronic device displays a second payment user interface (e.g., 676). While displaying the second payment user interface, the electronic device receives third authorization data (e.g., fingerprint authentication information or a device passcode). After receiving the third authorization data, the electronic device determines (e.g., at the electronic device) whether the third authorization data is valid (e.g., confirms that the fingerprint authentication information or device passcode is authorized for payments). After receiving the third authorization data (and without receiving the second authorization data from the user again (e.g., the bank pin authorization code)), the electronic device transmits a second transaction request (e.g., based on the stored second authorization data) that corresponds to the second payment transaction to one or more remote servers, wherein the second transaction request is based at least in part on a stored representation of the second authorization data. The electronic device receives a second reply to the second transaction request.

[00212] In some embodiments, in response to receiving the second reply to the second transaction request: in accordance with a determination that the second transaction request was successful, the electronic device dismisses the second payment user interface (and, optionally, provides an indication of the success of the transaction); and in accordance with a determination that the second transaction request failed, the electronic device maintains display of the second payment user interface and updates the second payment user interface to display a second indication of a second reason for failure of the second transaction request.

[00213] In some embodiments, transmitting the transaction request (e.g., based on the stored second authorization data) that corresponds to the payment transaction to the one or more remote

servers comprises transmitting the second authorization data to a financial institution (e.g., a bank or other authorizing agent).

[00214] In some embodiments, in accordance with the determination that the transaction request failed (e.g., insufficient funds, wrong pin): while displaying the payment user interface, the electronic device receives third authorization data (e.g., fingerprint authentication information or a device passcode); after receiving the third authorization data, the electronic device determines (e.g., at the electronic device) whether the third authorization data is valid (e.g., confirms that the fingerprint or device passcode is authorized for payments); the electronic device receives fourth authorization data (e.g., a bank pin authorization code); after receiving the third authorization data and the fourth authorization data, the electronic device transmits a second transaction request (e.g., based on the stored second authorization data) that corresponds to the payment transaction to one or more remote servers; and the electronic device receives a second reply to the transaction request.

[00215] In some embodiments, receiving first authorization data (e.g., fingerprint authorization information or device passcode) comprises detecting a respective fingerprint on a fingerprint sensor of the electronic device, and wherein determining (e.g., at the electronic device) whether the first authorization data is valid (e.g., confirm that the fingerprint or device passcode is authorized for payments) comprises determining whether the respective fingerprint is consistent with an enrolled fingerprint that is enabled to authorize payment transactions.

[00216] In some embodiments, receiving first authorization data (e.g., fingerprint authorization information or device passcode) comprises receiving a payment passcode (e.g., using a keypad), and wherein determining (e.g., at the electronic device) whether the first authorization data is valid (e.g., confirm that the fingerprint or device pin is authorized for payments) comprises determining whether the payment passcode is consistent with an enrolled passcode that is enabled to authorize payment transactions.

[00217] In some embodiments, the first authorization data is different from the second authorization data (e.g., the payment passcode is different from the bank pin authorization code).

[00218] In some embodiments, the second authorization data is requested from the user (and subsequently received) in accordance with a determination that a current location of the electronic device is within a first predefined geographical area (e.g., a first country or other geographical area in which a second form of authentication is required to authorize payment transactions). In contrast, in accordance with a determination that the electronic device is in a second predefined geographical area (e.g., outside of the first predefined geographical area or in a second country different from the first country), the electronic device authenticates the payment transaction with only a single form of authentication (e.g., the first authorization data).

[00219] In some embodiments, the second authorization data is requested from the user (and subsequently received) in accordance with a determination that a payment amount of the payment transaction meets a predefined criteria (e.g., the payment amount is larger than a threshold payment amount). In contrast, in accordance with a determination that the payment amount of the payment transaction does not meet the predefined criteria (e.g., the payment amount is not larger than the threshold payment amount), the electronic device authenticates the payment transaction with only a single form of authentication (e.g., the first authorization data).

[00220] Note that details of the processes described above with respect to method 700 (e.g., FIG. 7) are also applicable in an analogous manner to the methods described below. For example, methods 900 and 1100 may include one or more of the characteristics of the various methods described above with reference to method 700. For brevity, these details are not repeated below.

[00221] FIGS. 8A-8K illustrate exemplary techniques and user interfaces for conducting a payment transaction using a short-range communication radio, such as a near field communication (NFC) radio, in accordance with some embodiments. The techniques and user interfaces in these figures are used to illustrate the processes described below, including the process in FIG. 9.

[00222] The NFC standards, which are related to radio-frequency identification (RFID) standards, describe communication protocols for transferring information between two devices, such as for making payments. It should be appreciated, however, that other communications standards and techniques may also be used.

2016102031 24 Nov 2016

[00223] Devices 100 (and devices 300 and 500) may include near field communications circuitry, such as a short range communication radio and physical input mechanism 204 (e.g., mechanical or capacitive button) that includes an integrated biometric sensor. Accordingly, device 100 can wirelessly communicate with external equipment, such as NFC-enabled contactless payment transaction terminal 850, using near field communications. For example, the near field communications circuitry in device 100 may include a near field transmitter and a near field receiver. Near field communications for device 100 may be supported using capacitive coupling near field communications structures and/or inductive coupling near field communications structures. In near field communications techniques, wireless signals are typically conveyed, for example, over distances of 1 m or less, 100 cm or less, 10 cm or less, or 1 cm or less, and are not conveyed over longer distances.

[00224] In FIG. 8A, the NFC-enabled contactless payment transaction terminal 850 generates a field 852. For example, an NFC-enabled device that enters the field 852 can communicate with the contactless payment transaction terminal 850 using NFC. In FIG. 8A, the electronic device 100 has not been placed in the field 852. The contactless payment transaction terminal 850 may be part of a payment system (e.g., check register) installed in a retail store for processing payment transactions, such as purchases of products and services.

[00225] In some embodiments, electronic device 100 receives authorization (e.g., from the user, as described in detail below) to enable the electronic device to participate in payment transaction via short-range communication radio. Optionally, the authorization is only valid for a predetermined period of time (e.g., up to 30 seconds). If the user places the device into field 852 after receiving authorization and before the predetermined period of time has elapsed, the device will proceed with the payment transaction (e.g., a payment of funds being solicited by the contactless payment transaction terminal 850). After the predetermined period of time has elapsed, the device will no longer be enabled to participate in payment transaction via short-range communication radio (unless the user authorizes the device again), and accordingly the device will not proceed with the payment transaction, even if placed within range of the field 852. Thus, optionally, the electronic device does not stay enabled indefinitely after being enabled to participate in payment transaction via short-range communication radio.

[00226] By enabling the electronic device to participate in a payment transactions via short-range communication radio prior to the electronic device being placed within range of the field 852, the user is able to reduce the user interactions required with the electronic device once the electronic device is placed within range of the field 852, facilitating a simplified user experienced. Further, some NFC-enabled contactless payment transaction terminals use a reduced timeout duration. This reduced timeout duration requires that, for a successful payment transaction, the payment transaction be completed within a short duration of time, starting from the time the contactless payment transaction terminal detects that a device has entered the field of the contactless payment transaction terminal. By enabling the electronic device to participate in payment transaction via the short-range communication radio prior to the electronic device being within range of the field 852, the rate of timeouts is decreased and the rate of successful payment transactions is increase.

[00227] Electronic device 100 includes a short-range communication radio (e.g., NFC radio) and a physical input mechanism 204 (e.g., mechanical or capacitive button). The physical input mechanism 204 includes an integrated biometric sensor, such as a fingerprint sensor.

[00228] At both FIG. 8B and FIG. 8C, the electronic device 100 is not enabled to participant in payment transactions via the short-range communication radio. At FIG. 8B, the display of the device is turned off (e.g., disabled, not displaying anything). At FIG. 8B, the device may also be in a lock state or an unlock state.

[00229] In the lock state, the electronic device 100 is powered on and operational but is prevented from performing a predefined set of operations in response to the user input. The predefined set of operations may include navigation between user interfaces, activation or deactivation of a predefined set of functions, and activation or deactivation of certain applications. The lock state may be used to prevent unintentional or unauthorized use of some functionality of the electronic device 100 or activation or deactivation of some functions on the electronic device 100. In the unlock state, the electronic device 100 is power on and operational and is not prevented from performing at least a portion of the predefined set of operations that cannot be performed while in the lock state.

[00230] When the device 100 is in the lock state, the device 100 may be said to be locked. In some embodiments, the device 100 in the lock state may respond to a limited set of user inputs, including input that corresponds to an attempt to transition the device 100 to the user-interface unlock state or input that corresponds to powering the device 100 off.

[00231] At FIG. 8C, the display of the device 100 is turned on (e.g., displaying a current date or other information) and the device is in a lock state (e.g., locked).

[00232] While the electronic device is not enabled to participate in payment transactions via the short-range communication radio (whether the display is on or not, and whether or not the device is in a lock state or unlock state), the device detects activation of the physical input mechanism 204. For example, activating the physical input mechanism may require two presses (or clicks) of a mechanical or capacitive button within a predetermined period of time. Thus, the user can initiate the activation of the physical input mechanism 204 at either FIG. 8B or FIG. 8C.

[00233] In response to detecting at least a portion of the activation of the physical input mechanism (e.g., the first click or the button down portion of the first click), the electronic device detects a fingerprint using the integrated biometric sensor, as illustrated in FIG. 8D and as indicated by indicator 804. The electronic device also determines (e.g., at the electronic device) whether the fingerprint is consistent with an enrolled fingerprint that is enabled to authorize payment transactions.

[00234] As illustrated in FIGS. 8E-8G, in accordance with a determination that the fingerprint is consistent with an enrolled fingerprint that is enabled to authorize payment transactions, the electronic device enables the device to participate in payment transactions via the short-range communication radio, as indicated by indicators 810A-810C. For example, the electronic device transitions to an armed state (e.g., the electronic device advertises using the short-range communication radio that the device can make an NFC payment) in preparation for a payment transaction.

[00235] Although FIGS. 8C-8H illustrate displaying user interfaces, the same technique described above can be performed while not turning on the display.

[00236] In some embodiments, in accordance with a determination that the fingerprint is consistent with an enrolled fingerprint that is enabled to authorize payment transactions, the electronic device displays an electronic wallet, as illustrated in FIGS. 8E-8G. The electronic wallet may optionally include a plurality of payment card affordances (such as payment card affordances 802 and 812). For example, the user interface of FIG. 8E allows the user to easily determine which payment account will be used if the electronic device is used for the payment transaction. In this example, the payment card affordance 802 is displayed at the top of the display, indicating that the payment account associated with the payment card affordance 802 will be used for payment. The user can select a different payment account for use in the payment transaction by, for example, activating one of the payment card affordances 812 associated with other payment accounts.

[00237] At FIG. 8H, in some embodiments, in accordance with a determination that the fingerprint is not consistent with an enrolled fingerprint that is enabled to authorize payment transactions, the electronic device forgoes enabling (e.g., does not enable) the electronic device to participate in payment transactions via the short-range communication radio, as indicated by indicator 806. Additionally, in some embodiments, in accordance with a determination that the fingerprint is not consistent with an enrolled fingerprint that is enabled to authorize payment transactions, the electronic device displays an affordance 808, which when activated, displays a user interface, such as illustrated in FIG. 8K, for receiving a device passcode (rather than use a fingerprint) to enable the device to authorize payment transactions.

[00238] FIG. 8I illustrates the user placing the electronic device within range of field 852 generated by contactless payment transaction terminal 850. While the device is enabled to participate in payment transactions via the short-range communication radio, the device detects, by the short-range communication radio, presence of a field 852 generated by a contactless payment transaction terminal 850; performs, using the short-range communication radio, a handshake with the contactless payment transaction terminal 850; and authorizes the payment transaction, as illustrated in FIG. 8J and as indicated by indicator 814. As a result, the user does not need to authenticate (e.g., using fingerprint authentication) while the device is within range of field 852, as the user has already enabled the device in anticipation of the payment.

[00239] In contrast, if the user places the electronic device within range of field 852 generated by contactless payment transaction terminal 850 while the device is not enabled to participate in payment transactions via the short-range communication radio, the device will detect the field 852, determine that the electronic device has not been preauthorized by the user for proceeding with payment transactions, and attempt to receive authorization from the user to enable the electronic device to participate in payment transactions via the short-range communication radio.

[00240] In some embodiments, activation of the physical input mechanism is detected while the device is in a lock state (e.g., the electronic device detects the activation of the physical input mechanism while the device is in a lock state), as illustrated in FIG. 8C.

[00241] In some embodiments, enabling the device to participate in payment transactions via the short-range communication radio comprises enabling the device to participate in payment transactions via the short-range communication radio while the device is (e.g., remains) in a lock state.

[00242] In some embodiments, enabling the device to participate in payment transactions via the short-range communication radio comprises enabling the electronic device to participate in payment transactions via the short-range communication radio without turning on a display (or any displays) of the device, as illustrated in FIG. 8B.

[00243] In some embodiments, while the electronic device is not enabled to participate in payment transactions via the short-range communication radio, the electronic device displays a first user interface (e.g., the lock screen user interface of FIG. 8C) and maintains (e.g., does not update) the first user interface subsequent to enabling the device to participate in payment transactions via the short-range communication radio.

[00244] In some embodiments, enabling the electronic device to participate in payment transactions via the short-range communication radio comprises configuring the electronic device to respond to a payment transaction request (e.g., a handshake and subsequent payment request) via the short-range communication radio with at least partial credit card information (e.g., account number, expiration date, and or cardholder's name) of a payment account (e.g., a bank card, credit card, or other account that was previously linked to the device, such as

described with respect to method 11 (FIGS. 10A-10I and 11), of a plurality of payment accounts linked to the device (e.g., a default payment account is used, but the device can be configured to use one of the other payment accounts of the plurality of payment accounts), and wherein the payment transaction request is received from a contactless payment transaction terminal 850 (e.g., an NFC equipped payment terminal located at a physical retail store).

[00245] In some embodiments, subsequent to enabling the electronic device to participate in payment transactions via the short-range communication radio and while the electronic device is enabled to participate in payment transactions via the short-range communication radio and while the device is in a lock state, the electronic device receives user input to place the device in an unlock state (e.g., the user unlocks the device by performing an unlock action, using fingerprint authentication, or entering a passcode). The electronic device receives user input selecting a second payment account of a plurality of payment accounts linked to the device for use in the payment transaction (e.g., the user selects a different credit card (not the default credit card) for this particular payment).

[00246] In some embodiments, enabling the device to participate in payment transactions via the short-range communication radio does not require detecting a field generated by a contactless payment transaction terminal (e.g., the user can arm the device for making NFC payments without being detecting (or being near) an NFC-enabled contactless payment transaction terminal).

[00247] In some embodiments, enabling the device to participate in payment transactions via the short-range communication radio comprises using the short-range communication radio to transmit a signal, the signal indicating that the device is configured for making payments using near field communication. In contrast, when the electronic device is not enabled to participate in payment transactions via the short-range communication radio, the electronic device does not immediately respond to a contactless payment transaction terminal using the short-range communication radio to transmit when the electronic device detects a field generated by a contactless payment transaction terminal. Rather, the electronic device requests (and receives) authorization from the user before responding to the contactless payment transaction terminal.

[00248] In some embodiments, subsequent to enabling the electronic device to participate in payment transactions via the short-range communication radio, in response to determining that a payment transaction has not been authorized using the short-range communication radio within a predetermined duration of time, the electronic device becomes disabled from participating in payment transactions via the short-range communication radio.

[00249] FIG. 9 is a flow diagram illustrating a method for conducting a payment transaction using a short-range communication radio in accordance with some embodiments. Method 900 is performed at a device (e.g., 100, 300, 500). Some operations in method 900 may be combined, the order of some operations may be changed, and some operations may be omitted.

[00250] As described below, method 900 provides an intuitive way for conducting a payment transaction using a short-range communication radio. The method reduces the cognitive burden on a user when conducting the payment transaction, thereby creating a more efficient human-machine interface. For battery-operated computing devices, enabling a user to conduct a payment transaction using a short-range communication radio faster and more efficiently conserves power and increases the time between battery charges.

[00251] At block 902, while the electronic device is not enabled to participate in payment transactions via the short-range communication radio: the electronic device detects, at block 904, activation of the physical input mechanism (e.g., two presses of the mechanical or capacitive button within a predetermined period of time); at block 906, in response to detecting at least a portion of the activation of the physical input mechanism (e.g., the first click, or the button down portion of the first click), the electronic device detects a fingerprint using the integrated biometric sensor; and at block 908, the electronic device determines (e.g., at the electronic device) whether the fingerprint is consistent with an enrolled fingerprint that is enabled to authorize payment transactions.

[00252] At block 910, in accordance with a determination that the fingerprint is consistent with an enrolled fingerprint that is enabled to authorize payment transactions, the electronic device enables the device to participate in payment transactions via the short-range communication radio (e.g., transitioning the electronic device to an armed state in preparation for a payment transaction).

[00253] In some embodiments, at block 912, in accordance with a determination that the fingerprint is not consistent with an enrolled fingerprint that is enabled to authorize payment transactions, the electronic device forgoes enabling the device to participate in payment transactions via the short-range communication radio.

[00254] In some embodiments, while the device is enabled to participate in payment transactions via the short-range communication radio: the electronic device detects, by the short-range communication radio, presence of a field generated by a contactless payment transaction terminal; the electronic device performs, using the short-range communication radio, a handshake with the contactless payment transaction terminal; and the electronic device authorizes the payment transaction.

[00255] In some embodiments, activation of the physical input mechanism is detected while the device is in a lock state.

[00256] In some embodiments, enabling the device to participate in payment transactions via the short-range communication radio comprises enabling the device to participate in payment transactions via the short-range communication radio while the device is in a lock state.

[00257] In some embodiments, enabling the device to participate in payment transactions via the short-range communication radio comprises enabling the device to participate in payment transactions via the short-range communication radio without turning on a display (or any displays) of the device.

[00258] In some embodiments, while the electronic device is not enabled to participate in payment transactions via the short-range communication radio, the electronic device displays a first user interface; and maintains (e.g., does not update) the first user interface subsequent to enabling the device to participate in payment transactions via the short-range communication radio.

[00259] In some embodiments, enabling the device to participate in payment transactions via the short-range communication radio comprises configuring the device to respond to a payment transaction request (e.g., a handshake and subsequent payment request) via the short-range communication radio with at least partial credit card information (e.g., account number,

2016102031 24 Nov 2016

expiration date, and or cardholder's name) of a payment account (e.g., a bank card, credit card, or other account that was previously linked to the device) of a plurality of payment accounts linked to the device (e.g., a default payment account is used, but the device can be configured to use one of the other payment accounts of the plurality of payment accounts), and wherein the payment transaction request is received from a contactless payment transaction terminal (e.g., 850 of FIG. 8A).

[00260] In some embodiments, subsequent to enabling the device to participate in payment transactions via the short-range communication radio and while the device is enabled to participate in payment transactions via the short-range communication radio and while the device is in a lock state, the electronic device receives user input to place the device in an unlock state (e.g., the user unlocks the device by performing an unlock action, using fingerprint authentication, or entering a passcode); and the electronic device receives user input selecting a second payment account of a plurality of payment accounts linked to the device for use in the payment transaction (e.g., the user selects a different credit card (not the default credit card) for this particular payment).

[00261] In some embodiments, enabling the electronic device to participate in payment transactions via the short-range communication radio does not require the electronic device to detect a field generated by a contactless payment transaction terminal (e.g., the user can arm the device for NFC payment without being near an NFC-enabled contactless payment transaction terminal).

[00262] In some embodiments, enabling the device to participate in payment transactions via the short-range communication radio comprises using the short-range communication radio to transmit a signal, the signal indicating that the device is configured for making payments using near field communication.

[00263] In some embodiments, subsequent to enabling the device to participate in payment transactions via the short-range communication radio: in response to determining that a payment transaction has not been authorized using the short-range communication radio within a predetermined duration of time, the electronic device disables the device from participating in payment transactions via the short-range communication radio.

[00264] Note that details of the processes described above with respect to method 900 (e.g., FIG. 9) are also applicable in an analogous manner to the methods described below and above. For example, methods 700 and 1100 may include one or more of the characteristics of the various methods described above with reference to method 900. For brevity, these details are not repeated below.

[00265] FIGS. 10A-10I illustrate exemplary user interfaces for linking a payment account to a respective device, in accordance with some embodiments. The user interfaces in these figures are used to illustrate the processes described below, including the process in FIG. 11.

[00266] FIGS. 10A-10I illustrate exemplary user interfaces for linking a payment account, such as a bank account or revolving credit account, associated with a credit card (e.g., a physical credit card or debit card issued to a user) to a respective device (e.g., a cell phone, a laptop, a wearable electronic device) in accordance with some embodiments.

[00267] For example, in FIG. 10A, an electronic wallet is displayed on the display of an electronic device with a display and a camera sensor. The electronic wallet comprises a first stack of card objects 1002 and a second stack of card objects 1008, 1010, and 1012. The first stack of card objects 1002 is visually separated from the second stack of card objects 1008, 1010, and 1012. In this example, one credit card (e.g., an American Express credit card) is already linked to the electronic device and is displayed as part of the first stack of card objects 1002. The electronic device displays affordance 1020. In response to the electronic device receiving activation of affordance 1020, the electronic device displays the user interface illustrated in FIG. 10B.

[00268] FIG. 10B illustrates a user interface for selecting from among an add payment card affordance 1014 to link a payment account to the device (e.g., to make the payment account available in the electronic wallet) and a scan code affordance 1016 to link a pass. If the device determines that selection of done affordance 1018 is received, the device returns to displaying the user interface of FIG. 10A. If the device receives selection of add payment card affordance 514, the device transitions to the user interface illustrated in FIG. 10C.

[00269] At FIG. 10C, the electronic device displays, on the display, a user interface comprising: a credit card import affordance 1024 for importing, from a remote server, at least partial credit card information (e.g., import credit/debit card from iTunes server) and a credit card input affordance 1026 for receiving, at the electronic device, at least partial credit card information (e.g., receive credit/debit card details using a camera or manual numerical entry). The electronic device receives selection of the credit card input affordance 1026.

[00270] In response to receiving the selection of the credit card input affordance 1026, the electronic device displays, on the display, a live preview 1004 of images obtained via the camera sensor. For example, the camera preview turns on to show a live preview 1004 of images to indicate that the user should place a credit card 1028 in the camera's field of view for linking the payment account associated with the credit card 1028 to the electronic device.

[00271] While the electronic device displays the live preview 1004 of images obtained via the camera sensor, the electronic device detects (e.g., using the camera sensor on the back of the electronic device) at least partial credit card information of the credit card 1028 in a field of view of the camera sensor. For example, as illustrated in FIG. 10D, the user places a credit card in the field of view of the camera sensor and the electronic device performs optical character recognition of one or more of (1) an account number displayed on the credit card, (2) an expiration date displayed on the credit card, (3) an account holder's name displayed on the credit card.

[00272] In some embodiments, the live preview 1004 is displayed on the display of the electronic device immediately in response to receiving the selection of the credit card input affordance 1026, and without displaying an intervening user interface on the display (e.g., no intervening user interface is displayed on the display for receiving manual user typed credit card information). Thus, in response to detecting selection of credit card input affordance 1026, the electronic device transitions directly from the user interface of FIG. 10C to the user interface of FIG. 10D.

[00273] In some embodiments, the electronic device displays, on the display, concurrently with the live preview of images obtained via the camera sensor, a manual credit card entry affordance 1006. For example, the manual credit card entry affordance 1006, when activated,

causes the electronic device to display a user interface for manually typing in credit card information. The electronic device receives selection of the manual credit card entry affordance 1006. In response to receiving the selection of the manual credit card entry affordance 1006, the electronic device displays a user interface for receiving at least partial credit card information via a displayed keyboard 1050, as illustrated in FIG. 10F.

[00274] In some embodiments, in response to receiving the selection of the credit card input affordance 1026, the electronic device displays a manual credit card entry affordance 1006 for activating a manual credit card entry user interface (such as illustrated in FIG. 10F) for receiving at least partial credit card information via a keyboard 1050.

[00275] In some embodiments, the electronic device receives selection of the manual credit card entry affordance, and in response to receiving the selection of the manual credit card entry affordance, the electronic device displays the manual credit card entry user interface, such as illustrated in FIG. 10F. The manual credit card entry user interface comprises one or more input fields 1042, 1044, 1046, and 1048 for receiving user-entered credit card information.

[00276] At FIG. 10F, the electronic device receives user input, such as a portion of the credit card number at field 1042. In accordance with a determination that the credit card is of a first type (e.g., based on the portion of the credit card number received), the electronic device forgoes displaying input field 1046 (the security code input field) and 1048 (the expiration date input field). In accordance with a determination that the credit card is not of the first type (e.g., based on the portion of the credit card number received), the electronic device displays input field 1046 (the security code input field) and 1048 (the expiration date input field). If a field is displayed, such as first entry field 1046 or second entry field 1048, and then the electronic device subsequently determines that the displayed field 1046 or 1048 is not needed (e.g., the user goes back and changes the inputted credit card number), the electronic device marks the displayed, but not needed field as “Not Applicable”, grays out the field, or otherwise indicates the data for that field is not needed, rather than removing the field.

[00277] In some embodiments, the manual credit card entry user interface comprises two or more input fields (e.g., 1042 and 1044) for receiving user-entered account information of a payment account, the two or more input fields selected from the group consisting of a name of a

cardholder associated with the payment account (e.g., pre-populated using a name from the device, but editable), an account number associated with the payment account (e.g., a credit card number), an expiration date associated with the payment account, and a security code associated with the payment account (e.g., a CCV).

[00278] Optionally, the credit card information that is detected while displaying the live preview 1004 of images may be used to determine how many (and which) fields are displayed. In some embodiments, the at least partial credit card information of the credit card includes a portion of an account number of the credit card. The electronic device determines, based on the portion of the account number of the credit card, whether the credit card is of a first type (e.g., the credit card number falls within a certain predetermined range of numbers). In accordance with a determination that the credit card is not of the first type (e.g., the credit card number does not fall within a certain predetermined range of numbers), the electronic device displays an expiration date of the credit card in a first entry field 1038 and a security code (and/or space for a security code, such as a CCV) of the credit card in a second entry field 1036, as illustrated in FIG. 10E. In accordance with a determination that the credit card is of the first type, the electronic device forgoes displaying the expiration date of the credit card in the first entry field 1038 and forgoes displaying the security code (or space for a security code of the credit card in the second entry field 1036 (e.g., the electronic device does not display the expiration and security code or their corresponding fields, as identified inside dotted line 1040 of FIG. 10E. If a field is displayed, such as first entry field 1038 or second entry field 1036, and then the electronic device subsequently determines that the displayed field is not needed, the electronic device marks the field as “Not Applicable”, grays out the field, or otherwise indicates the data for that field is not needed, rather than removing the field.

[00279] In some embodiments, the portion of the account number of the credit card includes a bin identification number of the credit card (e.g., the issuer identification number portion of the credit card number, the first six digits of the credit card), and determining, based on the portion of the account number of the credit card, whether the credit card is of the first type comprises determining, based on the bin identification number of the credit card (e.g., issuer identification number, the first six digits of the credit card), whether the card is of the first type (e.g., the first

type of card is cards where the issuer of the credit card requires the expiration date and security code for processing a payment).

[00280] In some embodiments, the electronic device displays two or more input fields (e.g., fields 1032, 1034, 1036, and 1038) associated with the credit card. The quantity of the two or more input fields is based on an image obtained via the camera sensor (e.g., the image includes the credit card number, which is used to determine if expiration date field 1038 and security code field 1036 are required).

[00281] In some embodiments however, the credit card number in the credit card field 1034 may be changed/updated by the user. The electronic device displays two or more input fields (e.g., account holder's name field 1032 and credit card number 1034) associated with the credit card (and not the fields within dotted line 1040). The electronic device receives a user input selecting a first field of the two or more input fields. In response to receiving the user input selecting the first field, displaying (e.g., without regard to the credit card number/bin) a supplementary user input field (e.g., an expiration date field or a security code field that was not previously displayed, such as those in dotted line 1040) in addition to the two or more input fields 1032 and 1034. Thus, in some cases the device determines (based on the credit card number) that the security code and expiration dates of the credit card are not needed for payment transactions and does not display those respective fields. If the electronic device later detects selection of one of the displayed fields 1032 or 1034, additional fields (such as those within dotted line 1040) are displayed, regardless of whether the credit card number indicates the card is or is not of the first type.

[00282] In some embodiments, once the supplementary user input fields are displayed (e.g., the fields in dotted line 1040), they are not removed, even if the device determines that the supplementary user input fields are not needed. Instead, the device identifies the fields as being inactive. The electronic device receives a user input on a keyboard at the first field of the two or more input fields (e.g., the user has selected the credit card number field 1034 and has used the keyboard to change the value of the field). The electronic device determines, based on the user input, whether the credit card is of the first type. In accordance with a determination that the credit card is not of the first type, the device forgoes marking the supplementary user input field

as inactive (e.g., so the user can select/edit the contents of the expiration date field and/or security code field) In accordance with a determination that the credit card is of the first type, the device marks the supplementary user input field as inactive (e.g., if the bin number of the credit card entered by the user indicates it is of the first type, gray out the field or mark it as “Not Applicable”).

[00283] FIG. 11 is a flow diagram illustrating a method for linking a payment account to an electronic device in accordance with some embodiments. Method 1100 is performed at a device (e.g., 100, 300, 500). Some operations in method 1100 may be combined, the order of some operations may be changed, and some operations may be omitted.

[00284] As described below, method 1100 provides an intuitive way for linking a payment account to an electronic device. The method reduces the cognitive burden on a user for linking a payment account to an electronic device, thereby creating a more efficient human-machine interface. For battery-operated computing devices, enabling a user to link a payment account to an electronic device faster and more efficiently conserves power and increases the time between battery charges.

[00285] At block 1102, the electronic device displays, on the display, a user interface (e.g., the user interface of FIG. 10C) comprising: a credit card import affordance (e.g., 1024 of FIG. 10C) for importing, from a remote server, at least partial credit card information; and a credit card input affordance (e.g., 1026 of FIG. 10C) for receiving, at the electronic device, at least partial credit card information.

[00286] At block 1104, the electronic device receives selection of the credit card input affordance (e.g., 1026 of FIG. 10C).

[00287] At block 1106, in response to receiving the selection of the credit card input affordance (e.g., 1026 of FIG. 10C), the electronic device displays, on the display, a live preview (e.g., 1004 of FIG. 10D) of images obtained via the camera sensor.

[00288] At block 1108, while displaying the live preview (e.g., 1004 of FIG. 10D) of images obtained via the camera sensor, the electronic device detects (e.g., using the camera sensor) at

least partial credit card information of a credit card (e.g., 1028 of FIG. 10D) in a field of view of the camera sensor.

[00289] In some embodiments, the live preview (e.g., 1004 of FIG. 10D) is displayed on the display immediately in response to receiving the selection of the credit card input affordance, and without displaying an intervening user interface on the display (e.g., no intervening user interface is displayed on the display for receiving manual user typed credit card information).

[00290] In some embodiments, at block 1110, the electronic device displays, on the display, concurrently with the live preview (e.g., 1004 of FIG. 10D) of images obtained via the camera sensor, a manual credit card entry affordance (e.g., 1006 of FIG. 10D).

[00291] In some embodiments, at block 1112, the electronic device receives selection of the manual credit card entry affordance (e.g., 1006 of FIG. 10D).

[00292] In some embodiments, at block 1114, in response to receiving the selection of the manual credit card entry affordance, the electronic device displays a user interface (e.g., the user interface of FIG. 10F) for receiving at least partial credit card information via a displayed keyboard (e.g., 1050 of FIG. 10F).

[00293] In some embodiments, in response to receiving the selection of the credit card input affordance (e.g., 1026 of FIG. 10C), the electronic device displays a manual credit card entry affordance (e.g., 1006 of FIG. 10D) for activating a manual credit card entry user interface (e.g., the user interface of FIG. 10F) for receiving at least partial credit card information via a keyboard (e.g., 1050 of FIG. 10F).

[00294] In some embodiments, the electronic device receives selection of the manual credit card entry affordance (e.g., 1006 of FIG. 10D). In response to receiving the selection of the manual credit card input affordance (e.g., 1006 of FIG. 10D), the electronic device displays the manual credit card entry user interface (e.g., the user interface of FIG. 10F). The manual credit card entry user interface (e.g., the user interface of FIG. 10F) comprises one or more input fields (e.g., 1042, 1044, 1046, 1048) for receiving user-entered credit card information.

[00295] In some embodiments, the manual credit card entry user interface (e.g., the user interface of FIG. 10F) comprises two or more input fields (e.g., 1042, 1044, 1046, 1048) for receiving user-entered account information of a payment account, the two or more input fields selected from the group consisting of: a name of a cardholder associated with the payment account (e.g., pre-populated using a name from the device, but editable), an account number associated with the payment account (e.g., a credit card number), an expiration date associated with the payment account, and a security code associated with the payment account (e.g., a CCV).

[00296] In some embodiments, the at least partial credit card information of the credit card includes a portion of an account number of the credit card. The electronic device determines, based on the portion of the account number of the credit card, whether the credit card is of a first type. In accordance with a determination that the credit card is not of the first type, the electronic device displays an expiration date of the credit card in a first entry field (e.g., 1038 of FIG. 10E) and a security code of the credit card in a second entry field (e.g., 1036 of FIG. 10E). In accordance with a determination that the credit card is of the first type, the electronic device forgoes displaying the expiration date of the credit card in the first entry field (e.g., 1038 of FIG. 10E) and forgoes displaying the security code of the credit card in the second entry field (e.g., 1036 of FIG. 10E) (e.g., don't display the expiration and security code or the fields).

[00297] In some embodiments, the portion of the account number of the credit card includes a bin identification number of the credit card (e.g., an issuer identification number, the first six digits of the credit card), and wherein determining, based on the portion of the account number of the credit card, whether the credit card is of the first type comprises determining, based on the bin identification number of the credit card (e.g., issuer identification number, the first six digits of the credit card), whether the card is of the first type (e.g., the first type of card is cards where the issuer of the credit card requires the expiration date and security code for processing a payment).

[00298] In some embodiments, the electronic device displays two or more input fields (e.g., 1032, 1034, 1036, 1038 of FIG. 10E) associated with the credit card. The quantity of the two or more input fields is based on an image obtained via the camera sensor (e.g., the image includes

the credit card number, which is used to determine if expiration date and security code fields are required).

[00299] In some embodiments, the electronic device displays two or more input fields (e.g., 1032, 1034 of FIG. 10E) associated with the credit card. The electronic device receives a user input selecting a first field (e.g., 1032 of FIG. 10E) of the two or more input fields (e.g., 1032, 1034 of FIG. 10E). In response to receiving the user input selecting the first field (e.g., 1032 of FIG. 10E), displaying (e.g., without regard to the credit card number/bin) a supplementary user input field (e.g., 1036 or 1038 of FIG. 10E; an expiration date field or a security code field that was not previously displayed) in addition to the two or more input fields.

[00300] In some embodiments, the electronic device receives a user input (e.g., using a keyboard) at the first field of the two or more input fields. The electronic device determines, based on the user input, whether the credit card is of the first type. In accordance with a determination that the credit card is not of the first type, the electronic device forgoes marking the supplementary user input field as inactive (e.g., so the user can select/edit the contents of the expiration date field and/or security code field). In accordance with a determination that the credit card is of the first type, the electronic device marks the supplementary user input field as inactive (e.g., if the bin number of the credit card entered by the user indicates it is of the first type, gray out the field or mark it as “Not Applicable”).

[00301] Note that details of the processes described above with respect to method 1100 (e.g., FIG. 11) are also applicable in an analogous manner to the methods described above. For example, methods 700 and 900 may include one or more of the characteristics of the various methods described above with reference to method 1100. For brevity, these details are not repeated below.

[00302] FIG. 12 shows exemplary functional blocks of an electronic device 1200 that, in some embodiments, perform the features described above. As shown in FIG. 12, an electronic device 1200 includes a display unit 1202 configured to display graphical objects; a touch-sensitive surface unit 1204 configured to receive user gestures (e.g., touches); one or more RF units 1206 configured to detect and communicate with external electronic devices; and a processing unit 1208 coupled to display unit 1202, touch-sensitive surface unit 1204, and RF units 1206. In

some embodiments, the processing unit 1208 includes a display enabling unit 1210, a receiving unit 1212, a determining unit 1214, a detecting unit 1216, a transmitting unit 1218, an enabling unit 1220, a communication unit 1222, an authorizing unit 1224, a configuring unit 1226, and a storing unit 1228. The units of FIG. 12 may be used to implement the various techniques and methods described above with respect to FIGS. 6- 11.

[00303] For example, the display enabling unit 1210 can be used for: displaying a payment user interface; displaying a live preview of images obtained via the camera sensor; displaying, on the display, a user interface comprising a credit card import affordance for importing, from a remote server, at least partial credit card information, and a credit card input affordance for receiving, at the electronic device, at least partial credit card information; dismissing the payment user interface; maintaining display of the payment user interface; updating the payment user interface to display an indication of a reason for failure of the transaction request; displaying the payment user interface over only a portion of a first user interface; displaying a second payment user interface; dismissing the second payment user interface; maintaining display of the second payment user interface; updating the second payment user interface to display a second indication of a second reason for failure of the second transaction request; displaying a first user interface; maintaining the first user interface; displaying concurrently with the live preview of images obtained via the camera sensor, a manual credit card entry affordance; displaying a user interface for receiving at least partial credit card information via a displayed keyboard; displaying a manual credit card entry affordance for activating a manual credit card entry user interface for receiving at least partial credit card information via a keyboard; displaying the manual credit card entry user interface; displaying an expiration date of the credit card in a first entry field and a security code of the credit card in a second entry field; and forgoing displaying the expiration date of the credit card in the first entry field and forgoing displaying the security code of the credit card in the second entry field.

[00304] For example, the receiving unit 1212 can be used for: receiving first authorization data; receiving second authorization data; receiving a reply to the transaction request; receiving selection of the credit card input affordance; receiving the reply to the transaction request while displaying the payment user interface; receiving third authorization data; receiving a second reply to the second transaction request; receiving third authorization data; receiving fourth

authorization data; receiving a second reply to the transaction request; receiving a payment passcode; receiving user input to place the device in an unlock state; receiving user input selecting a second payment account of a plurality of payment accounts linked to the device for use in the payment transaction; receiving selection of the manual credit card entry affordance; and receiving selection of the manual credit card entry affordance.

[00305] For example, the determining unit 1214 can be used for: determining whether the first authorization data is valid; determining whether the fingerprint is consistent with an enrolled fingerprint that is enabled to authorize payment transactions; determining whether the third authorization data is valid; determining whether the third authorization data is valid; determining whether the respective fingerprint is consistent with an enrolled fingerprint that is enabled to authorize payment transactions; determining whether the payment passcode is consistent with an enrolled passcode that is enabled to authorize payment transactions; determining, based on the portion of the account number of the credit card, whether the credit card is of a first type; and determining, based on the bin identification number of the credit card, whether the card is of the first type.

[00306] For example, the detecting unit 1216 can be used for: detecting a request to initiate a payment transaction; detecting activation of the physical input mechanism; detecting a fingerprint using the integrated biometric sensor; detecting at least partial credit card information of a credit card in a field of view of the camera sensor; detecting a second request to initiate a second payment transaction; detecting a respective fingerprint on a fingerprint sensor of the electronic device; and detecting, by the short-range communication radio, presence of a field generated by a contactless payment transaction terminal.

[00307] For example, the transmitting unit 1218 can be used for: transmitting a transaction request that corresponds to the payment transaction to one or more remote servers; transmitting the transaction request while displaying the payment user interface; transmitting a second transaction request that corresponds to the second payment transaction to one or more remote servers; transmitting the second authorization data to a financial institution; and transmitting a second transaction request that corresponds to the payment transaction to one or more remote servers.

[00308] For example, the enabling unit 1220 can be used for: enabling the device to participate in payment transactions via the short-range communication radio; forgoing enabling the device to participate in payment transactions via the short-range communication radio; and enabling the device to participate in payment transactions via the short-range communication radio while the device is in a lock state.

[00309] For example, the communication unit 1222 can be used for: performing, using the short-range communication radio, a handshake with the contactless payment transaction terminal.

[00310] For example, the authorizing unit 1224 can be used for: authorizing the payment transaction.

[00311] For example, the configuring unit 1226 can be used for: configuring the device to respond to a payment transaction request via the short-range communication radio with at least partial credit card information of a payment account of a plurality of payment accounts linked to the device; and disabling the device from participating in payment transactions via the short-range communication radio.

[00312] For example, the storing unit 1228 can be used for: storing the second authorization data; and forgoing storing the second authorization data.

[00313] The functional blocks of the device 1200 are, optionally, implemented by hardware, software, or a combination of hardware and software to carry out the principles of the various described examples. It is understood by persons of skill in the art that the functional blocks described in FIG. 12 are, optionally, combined or separated into sub-blocks to implement the principles of the various described examples. Therefore, the description herein optionally supports any possible combination or separation or further definition of the functional blocks described herein.

[00314] The operations described above with reference to the figures may be implemented by components depicted in FIGS. 1A-1B, 2, 3, and 5A-B. For example, detection operations, display operations, and determination operations may be implemented by event sorter 170, event recognizer 180, and event handler 190. Event monitor 171 in event sorter 170 detects a contact

on touch-sensitive display 112, and event dispatcher module 174 delivers the event information to application 136-1. A respective event recognizer 180 of application 136-1 compares the event information to respective event definitions 186, and determines whether a first contact at a first location on the touch-sensitive surface corresponds to a predefined event or sub event, such as activation of an affordance on a user interface. When a respective predefined event or sub-event is detected, event recognizer 180 activates an event handler 190 associated with the detection of the event or sub-event. Event handler 190 may utilize or call data updater 176 or object updater 177 to update the application internal state 192. In some embodiments, event handler 190 accesses a respective GUI updater 178 to update what is displayed by the application. Similarly, it would be clear to a person having ordinary skill in the art how other processes can be implemented based on the components depicted in FIGS. 1A-1B, 2, 3, and 5A-B.

[00315] FIGS. 13A-13E illustrate exemplary techniques and user interfaces for enabling an electronic device to participate in a payment transaction using a short-range communication radio in accordance with some embodiments. The user interfaces in these figures are used to illustrate the processes described below, including the processes in FIG. 14.

[00316] FIG. 13A illustrates electronic device 100 wherein the display is turned off, an integrated biometric sensor of physical input mechanism (menu button) 204 is not enabled to detect fingerprints, the device is locked, and a short-range communication radio (e.g., NFC radio) of the device is not enabled to participate in payment transactions (a first short-range communication radio payment mode). Generally, device 100 may be in this state when it has not recently been used by the user. Although the short-range communication radio may be monitoring for an NFC field, it is not enabled to participate in payment transactions.

[00317] The device may need to disambiguate between a user's request to unlock the device and a user's request to enable the device to participate in payment transactions. In some examples, (1) detecting a single press of the physical input mechanism 204 along with fingerprint authentication unlocks the device and alternatively (2) detecting a double press of the physical input mechanism 204 along with fingerprint authentication enables the device to participate in payment transactions. Additional details of this technique are described below.

2016102031 24 Nov 2016

[00318] At FIG. 13B, while the electronic device is locked and in the first short-range communication radio payment mode (e.g., not enabled to participate in payment transactions via the short-range communication radio), the device detects activation of the physical input mechanism 204 (e.g., a first press of the mechanical or capacitive button). The device detects a fingerprint (e.g., at least a portion of a finger, without having to identify or match a complete fingerprint) using the integrated biometric sensor. The device determines whether the fingerprint is consistent with an enrolled fingerprint. In some examples, the determination of whether the fingerprint is consistent with the enrolled fingerprint happens before or after detecting the activation of the physical input mechanism. The device determines (e.g., at the electronic device) whether a set of one or more criteria is met. The set of one or more criteria includes a criterion that is met when the physical input mechanism 204 is reactivated within a predetermined period of time (e.g., 300 ms) after the activation of the physical input mechanism (e.g., a second press of the mechanical or capacitive button, resulting in a double-press).

[00319] At FIG. 13C, in accordance with a determination that the fingerprint is consistent with the enrolled fingerprint and a determination that the set of one or more criteria is met (e.g., a double-press of the physical input mechanism 204 was detected), the device transitions to a second short-range communication radio payment mode different from the first short-range communication radio payment mode. For example, enabling the device to participate in payment transactions via the short-range communication radio or transitioning the electronic device to an armed state (e.g., advertising device can make a payment) in preparation for a payment transaction).

[00320] As illustrated in FIG. 13C, the user interface of the device while in the second short-range communication radio payment mode may include an indication 1302 of a payment account to be used for a payment transaction. The user interface may also include one or more affordance 1304, which when activated, change the payment account to be used for a payment transaction. While in the second short-range communication radio payment mode, the device will enabled a contactless payment terminal to engage in a payment transaction by transmitting payment account information to the contactless payment terminal. Thus, to make a payment using their electronic device while it is in a locked state, a user can merely double-press the

physical input mechanism 204 and place the device into a field of a contactless payment terminal.

[00321] At FIG. 13D, in accordance with a determination that the fingerprint is consistent with the enrolled fingerprint and a determination that the set of one or more criteria is not met, the device unlocks (e.g., transitioning the electronic device from a lock state to an unlock state). For example, in the unlock state one or more affordances 1306 may be displayed, which when activates, start and/or display a corresponding application.

[00322] In the lock state, the electronic device 100 is powered on and operational but is prevented from performing a predefined set of operations in response to the user input. The predefined set of operations may include navigation between user interfaces, activation or deactivation of a predefined set of functions, and activation or deactivation of certain applications. The lock state may be used to prevent unintentional or unauthorized use of some functionality of the electronic device 100 or activation or deactivation of some functions on the electronic device 100. In the unlock state, the electronic device 100 is power on and operational and is not prevented from performing at least a portion of the predefined set of operations that cannot be performed while in the lock state.

[00323] In some embodiments, in accordance with the determination that the fingerprint is consistent with the enrolled fingerprint and the determination that the set of one or more criteria is met (e.g., double-press), the device forgoes unlocking. As a result, the device is in the second short-range communication radio payment mode, but remains locked.

[00324] In some embodiments, in accordance with a determination that the fingerprint is consistent with the enrolled fingerprint and a determination that the set of one or more criteria (e.g., double-press) is not met, the device forgoes transitioning to the second short-range communication radio payment mode. For example, the device unlocks, but the device remains in the first short-range communication radio payment mode.

[00325] In some embodiments, as discussed above, the first short-range communication radio payment mode is a mode in which the device is not enabled to participate in payment transactions via the short-range communication radio and the second short-range communication

radio payment mode is a mode in which the device is enabled to participate in payment transactions via the short-range communication radio.

[00326] In some embodiments, the set of one or more criteria includes a criterion that is met when at least one payment account is linked to the device for use in payment transactions using the short-range communication radio (e.g., a credit card was previously provisioned on the device for NFC payments). Thus, the device must be provisioned for at least one payment account for the criteria is met. If the device is not provisioned for at least one payment account, the device does not meet the set of one or more criteria.

[00327] Thus, in one example the set of one or more criteria is satisfied when: (1) the physical input mechanism is reactivated within the predetermined period of time (e.g., 300ms) after the activation of the physical input mechanism and (2) at least one payment account is linked to the device for use in payment transactions using the short-range communication radio.

[00328] In some embodiments, in response to detecting activation of the physical input mechanism, the device enables the integrated biometric sensor to detect fingerprints. Accordingly, power savings can be achieved by keeping the integrated biometric sensor disabled (e.g., turned off) and enabling it after detecting the activation of the physical input mechanism.

[00329] In some embodiments, in response to detecting activation of the physical input mechanism, the device turns on the display of the device. As a result, the user is notified that the activation of the physical input mechanism was detected.

[00330] In some embodiments, unlocking the device does not enable the device to participate in payment transactions via the short-range communication radio. In some embodiments, enabling the device to participate in payment transactions via the short-range communication radio does not unlock the electronic device.

[00331] In some embodiments, the device determines whether the fingerprint is consistent with an enrolled fingerprint subsequent to determining whether the set of one or more criteria is met.

[00332] In some embodiments, in accordance with a determination that the fingerprint is not consistent with the enrolled fingerprint, the device forgoes transitioning to the second short-range communication radio payment mode and forgoes unlocking the device. Thus, if the user's fingerprint is not registered with the device, the device does not unlock and does not transition to the second short-range communication radio mode.

[00333] In some embodiments, to unlock the device, the device provides fingerprint sensor information (e.g., a confirmation of a fingerprint match) of the integrated biometric sensor to a first application of the electronic device. The first application is configured to unlock the device based on the fingerprint sensor information. For example, the integrated biometric sensor sends a single-use confirmation to the operating system that allows the operating system to unlock the device.

[00334] In some embodiments, in accordance with the determination that the fingerprint is consistent with the enrolled fingerprint and the determination that the set of one or more criteria is not met, the device transitions the integrated biometric sensor from a first sensor mode to a second sensor mode. For example, while in the second sensor mode, the integrated biometric sensor sends a single-use confirmation to the operating system that allows the operating system to unlock the device. In accordance with the determination that the fingerprint is consistent with the enrolled fingerprint and the determination that the set of one or more criteria is met, the device transitions the integrated biometric sensor from the first sensor mode to a third sensor mode. For example, while in the third sensor mode, the integrated biometric sensor sends a single-use confirmation to an electronic wallet application that allows the electronic wallet application to enable the device to participate in payment transactions via the short-range communication radio. However, while in the first sensor mode, the integrated biometric sensor does not send a confirmation to the operating system or to the electronic wallet application because it does not yet know whether the single-use confirmation should be sent to the operating system or to the electronic wallet application.

[00335] FIG. 13E illustrates exemplary timelines for detected activations of a physical input mechanism. In the first exemplary timeline 1320, prior to event 1322, the electronic device is locked and in the first short-range communication radio payment mode (e.g., not enabled to

participate in payment transactions via the short-range communication radio). At event 1322, the electronic device detects activation of the physical input mechanism (e.g., a first press of the mechanical or capacitive button). At event 1324, the device detects reactivation of the physical input mechanism within the 300 ms predetermined period of time. As a result, the device transitions to a second short-range communication radio payment mode (e.g., enabled to participate in payment transactions via the short-range communication radio) different from the first short-range communication radio payment mode (if a fingerprint of the user is authenticated).

[00336] In the second exemplary timeline 1330, prior to event 1332, the electronic device is locked and in the first short-range communication radio payment mode (e.g., not enabled to participate in payment transactions via the short-range communication radio). At event 1332, the electronic device detects activation of the physical input mechanism (e.g., a first press of the mechanical or capacitive button). At event 1334, the device unlocks because a second activation of the physical input mechanism was not detected within the 300ms predetermined period of time (if a fingerprint of the user is authenticated).

[00337] FIG. 14 is a flow diagram illustrating a method for enabling an electronic device to participate in a payment transaction using a short-range communication radio, in accordance with some embodiments. Method 1400 is performed at a device (e.g., 100, 300, 500) with a short-range communication radio (e.g., NFC radio) and a physical input mechanism (e.g., mechanical or capacitive button) that includes an integrated biometric sensor (e.g., fingerprint sensor). Some operations in method 1400 may be combined, the order of some operations may be changed, and some operations may be omitted.

[00338] As described below, method 1400 provides an intuitive way for enabling an electronic device to participate in a payment transaction using a short-range communication radio. The method reduces the cognitive burden on a user for enabling an electronic device to participate in a payment transaction, thereby creating a more efficient human-machine interface. For battery-operated computing devices, enabling a user to enabling an electronic device to participate in a payment transaction using a short-range communication radio faster and more efficiently conserves power and increases the time between battery charges.

2016102031 24 Nov 2016

[00339] At block 1402, the electronic device is locked and in a first short-range communication radio payment mode.

[00340] At block 1404, the electronic device detects activation of the physical input mechanism 204 (e.g., a first press of the mechanical or capacitive button).

[00341] At block 1406, the electronic device detects a fingerprint (e.g., at least a portion of a finger, without having to identify or match a complete fingerprint) using the integrated biometric sensor.

[00342] At block 1408, the electronic device determines whether the fingerprint is consistent with an enrolled fingerprint. In some examples, the determination of whether the fingerprint is consistent with the enrolled fingerprint happens before or after detecting the activation of the physical input mechanism.

[00343] At block 1410, the electronic device determines (e.g., at the electronic device) whether a set of one or more criteria is met, wherein the set of one or more criteria includes a criterion that is met when the physical input mechanism is reactivated within a predetermined period of time (e.g., 300ms) after the activation of the physical input mechanism (e.g., a second press of the mechanical or capacitive button, resulting in a double-press).

[00344] At block 1412, in accordance with a determination that the fingerprint is consistent with the enrolled fingerprint and a determination that the set of one or more criteria is met (e.g., double-press), transitioning to a second short-range communication radio payment mode different from the first short-range communication radio payment mode (e.g., enabling the device to participate in payment transactions via the short-range communication radio; transitioning the electronic device to an armed state (e.g., advertising device can make a payment) in preparation for a payment transaction).

[00345] At block 1414, in accordance with a determination that the fingerprint is consistent with the enrolled fingerprint and a determination that the set of one or more criteria is not met, unlocking the device.

[00346] In some embodiments, in accordance with the determination that the fingerprint is consistent with the enrolled fingerprint and the determination that the set of one or more criteria is met (e.g., double-press), the electronic device forgoes unlocking the device.

[00347] In some embodiments, in accordance with a determination that the fingerprint is consistent with the enrolled fingerprint and a determination that the set of one or more criteria (e.g., double-press) is not met, the electronic device forgoes transitioning to the second short-range communication radio payment mode (e.g., forgoing enabling the device to participate in payment transactions via the short-range communication radio).

[00348] In some embodiments, the first short-range communication radio payment mode is a mode in which the device is not enabled to participate in payment transactions via the short-range communication radio and the second short-range communication radio payment mode is a mode in which the device is enabled to participate in payment transactions via the short-range communication radio.

[00349] In some embodiments, the set of one or more criteria includes a criterion that is met when at least one payment account is linked to the device for use in payment transactions using the short-range communication radio (e.g., a credit card was previously provisioned on the device for NFC payments).

[00350] In some embodiments, in response to detecting activation of the physical input mechanism, the electronic device enables the integrated biometric sensor to detect fingerprints.

[00351] In some embodiments, the electronic device includes a display, and in response to detecting activation of the physical input mechanism, the electronic device turns on the display of the electronic device.

[00352] In some embodiments, unlocking the electronic device does not enable the electronic device to participate in payment transactions via the short-range communication radio. In some embodiments, enabling the electronic device to participate in payment transactions via the short-range communication radio does not unlock the electronic device.

[00353] In some embodiments, determining whether the fingerprint is consistent with an enrolled fingerprint occurs subsequent to determining whether the set of one or more criteria is met.

[00354] In some embodiments, in accordance with a determination that the fingerprint is not consistent with the enrolled fingerprint, the electronic device forgoes transitioning to the second short-range communication radio payment mode and forgoing unlocking the device.

[00355] In some embodiments, unlocking the device further comprises providing fingerprint sensor information (e.g., a confirmation of a fingerprint match) of the integrated biometric sensor to a first application of the electronic device, the first application configured to unlock the device. For example, the integrated biometric sensor sends a single-use confirmation to the OS that allows the operating system to unlock the device.

[00356] In some embodiments, in accordance with the determination that the fingerprint is consistent with the enrolled fingerprint and the determination that the set of one or more criteria is not met, the electronic device transitions the integrated biometric sensor from a first sensor mode to a second sensor mode. For example, while in the second sensor mode, the integrated biometric sensor sends a single-use confirmation to the operating system that allows the operating system to unlock the device.

[00357] In some embodiments, in accordance with the determination that the fingerprint is consistent with the enrolled fingerprint and the determination that the set of one or more criteria is met, the electronic device transitions the integrated biometric sensor from the first sensor mode to a third sensor mode. For example, while in the third sensor mode, the integrated biometric sensor sends a single-use confirmation to an electronic wallet application that allows the electronic wallet application to enable the device to participate in payment transactions via the short-range communication radio. However, while in the first sensor mode, the integrated biometric sensor does not send a confirmation to the operating system or the wallet application.

[00358] Note that details of the processes described above with respect to method 1400 (e.g., FIG. 14) are also applicable in an analogous manner to the methods described below and above. For example, method 1400 may include one or more of the characteristics of the various methods

described above and below with reference to method 700, method 900, method 1100, and method 1600. For brevity, these details are not repeated below.

[00359] FIGS. 15A-15E illustrate exemplary techniques and user interfaces for enabling an electronic device to participate in a payment transaction using a short-range communication radio in accordance with some embodiments. The user interfaces in these figures are used to illustrate the processes described below, including the processes in FIG. 16.

[00360] FIG. 15A illustrates electronic device 100 wherein the display is turned on, an integrated biometric sensor of physical input mechanism (menu button) 204 is enabled to detect fingerprints, the device is locked, and a short-range communication radio (e.g., NFC radio) of the device is not enabled to participate in payment transactions (a first short-range communication radio payment mode). Generally, device 100 may be in this state when the electronic device has been woken up by the user (such as by activating the physical input mechanism 204 or a button other than the physical input mechanism 204). Although the short-range communication radio may be monitoring for an NFC field, it is not enabled to participate in payment transactions.

[00361] The device may need to disambiguate between a user's request to unlock the device and a user's request to enable the device to participate in payment transactions. In some examples, (1) detecting a fingerprint without a press of the physical input mechanism 204 along with fingerprint authentication unlocks the device, (2) detecting a single press of the physical input mechanism 204 along with fingerprint authentication unlocks the device, and (3) detecting a double press of the physical input mechanism 204 along with fingerprint authentication enables the device to participate in payment transactions. Additional details of this technique are described below.

[00362] At FIG. 15B, while the electronic device is locked and in the first short-range communication radio payment mode (e.g., not enabled to participate in payment transactions via the short-range communication radio), the electronic device detects a fingerprint (e.g., at least a portion of a finger) using the integrated biometric sensor. The electronic device determines whether the fingerprint is consistent with an enrolled fingerprint. In some examples, the determination of whether the fingerprint is consistent with the enrolled fingerprint happens before or after detecting the activation of the physical input mechanism. The electronic device

determines (e.g., at the electronic device) whether a set of one or more criteria is met, wherein the set of one or more criteria includes a criterion that is met when the physical input mechanism 204 is activated within a first predetermined period of time (e.g., 300ms) after detecting the fingerprint using the biometric sensor (e.g., a first touch of the physical input mechanism).

[00363] In accordance with a determination that the fingerprint is consistent with an enrolled fingerprint and a determination that the set of one or more criteria is not met (e.g., no press within 300ms), the electronic device unlocks (e.g., transitioning the electronic device from a lock state to an unlock state), as illustrated in FIG. 15C. For example, in the unlock state one or more affordances 1506 may be displayed, which when activates, start and/or display a corresponding application.

[00364] In accordance with a determination that the set of one or more criteria is met (e.g., a press of the physical input mechanism within 300ms), the electronic device determines (e.g., at the electronic device) whether the physical input mechanism is reactivated within a second predetermined period of time (e.g., 300 ms) after the activation of the physical input mechanism (e.g., a second press of the mechanical or capacitive button, resulting in a double-press).

[00365] In accordance with a determination that the physical input mechanism is not reactivated within the second predetermined period of time (e.g., no second press within 300ms of the first press) and a determination that the fingerprint is consistent with an enrolled fingerprint, the electronic device locks (e.g., transitioning the electronic device from a lock state to an unlock state.), as illustrated in FIG. 15C. Thus, to unlock the electronic device, a user can place a finger on the physical input mechanism with the integrated biometric sensor and either (1) not press the physical input mechanism or (2) press the physical input mechanism once.

[00366] In accordance with a determination that the physical input mechanism is reactivated within the second predetermined period of time (e.g., a double-press) and in accordance with a determination that the fingerprint is consistent with an enrolled fingerprint, the electronic device transitions to a second short-range communication radio payment mode different from the first short-range communication radio payment mode (e.g., enabling the device to participate in payment transactions via the short-range communication radio; transitioning the electronic

device to an armed state (e.g., advertising device can make a payment) in preparation for a payment transaction), as illustrated in FIG. 15D.

[00367] As illustrated in FIG. 15D, the user interface of the device while in the second short-range communication radio payment mode may include an indication 1502 of a payment account to be used for a payment transaction. The user interface may also include one or more affordance 1504, which when activated, change the payment account to be used for a payment transaction. While in the second short-range communication radio payment mode, the device will enable a contactless payment terminal to engage in a payment transaction by transmitting payment account information to the contactless payment terminal. Thus, to make a payment using their electronic device while it is in a locked state, a user can merely double-press the physical input mechanism 204 and place the device into a field of a contactless payment terminal.

[00368] In the lock state, the electronic device 100 is powered on and operational but is prevented from performing a predefined set of operations in response to user input. The predefined set of operations may include navigation between user interfaces, activation or deactivation of a predefined set of functions, and activation or deactivation of certain applications. The lock state may be used to prevent unintentional or unauthorized use of some functionality of the electronic device 100 or activation or deactivation of some functions on the electronic device 100. In the unlock state, the electronic device 100 is power on and operational and is not prevented from performing at least a portion of the predefined set of operations that cannot be performed while in the lock state.

[00369] In some embodiments, in accordance with the determination that the fingerprint is consistent with the enrolled fingerprint and the determination that the set of one or more criteria is met (e.g., double-press), the electronic device forgoes unlocking.

[00370] In some embodiments, in accordance with a determination that the fingerprint is consistent with the enrolled fingerprint and a determination that the set of one or more criteria (e.g., double-press) is not met, the electronic device forgoes transitioning to the second short-range communication radio payment mode. (e.g., forgoing enabling the device to participate in payment transactions via the short-range communication radio.)

[00371] In some embodiments, the first short-range communication radio payment mode is a mode in which the device is not enabled to participate in payment transactions via the short-range communication radio and the second short-range communication radio payment mode is a mode in which the device is enabled to participate in payment transactions via the short-range communication radio.

[00372] In some embodiments, the set of one or more criteria includes a criterion that is met when at least one payment account is linked to the device for use in payment transactions using the short-range communication radio (e.g., a credit card was previously provisioned on the device for NFC payments).

[00373] Thus, in this example the set of one or more criteria is satisfied when: (1) the physical input mechanism is activated within the predetermined period of time after detection of a fingerprint and (2) at least one payment account is linked to the device for use in payment transactions using the short-range communication radio.

[00374] In some embodiments, unlocking the device does not enable the device to participate in payment transactions via the short-range communication radio. In some embodiments, enabling the device to participate in payment transactions via the short-range communication radio does not unlock the device.

[00375] In some embodiments, determining whether the fingerprint is consistent with an enrolled fingerprint occurs subsequent to determining whether the set of one or more criteria is met.

[00376] In some embodiments, in accordance with a determination that the fingerprint is not consistent with the enrolled fingerprint, the electronic device forgoes transitioning to the second short-range communication radio payment mode and forgoes unlocking the device.

[00377] In some embodiments, the electronic device includes a display and the display is on while detecting the fingerprint using the integrated biometric sensor.

[00378] In some embodiments, unlocking the device further comprises providing fingerprint sensor information (e.g., a confirmation of a fingerprint match) of the integrated biometric sensor

to a first application of the electronic device, the first application configured to unlock the device. For example, the integrated biometric sensor sends a single-use confirmation to the OS that allows the operating system to unlock the device.

[00379] In some embodiments, in accordance with the determination that: (1) the fingerprint is consistent with an enrolled fingerprint and (2) the set of one or more criteria is not met (e.g., no press within 300 ms), the electronic device transitions the integrated biometric sensor from a first sensor mode to a second sensor mode. For example, while in the second sensor mode, the integrated biometric sensor sends a single-use confirmation to the operating system that allows the operating system to unlock the device.

[00380] In some embodiments, in accordance with the determination that: (1) the set of one or more criteria is met (e.g., a press within 300 ms), (2) the physical input mechanism is not reactivated within the second predetermined period of time (e.g., no second press within 300 ms of the first press), and (3) the fingerprint is consistent with an enrolled fingerprint, the electronic device transitions the integrated biometric sensor from the first sensor mode to a second sensor mode. For example, while in the second sensor mode, the integrated biometric sensor sends a single-use confirmation to the operating system that allows the operating system to unlock the device.

[00381] In some embodiments, in accordance with the determination that: (1) the set of one or more criteria is met (e.g., a press within 300 ms), (2) the physical input mechanism is reactivated within the second predetermined period of time (e.g., within another 300 ms, resulting in a double-press), and (3) the fingerprint is consistent with an enrolled fingerprint, the electronic device transitions the integrated biometric sensor from the first sensor mode to a third sensor mode. For example, while in the third sensor mode, the integrated biometric sensor sends a single-use confirmation to a wallet application that allows the wallet application to enable the device to participate in payment transactions via the short-range communication radio. However, while in the first sensor mode, the integrated biometric sensor does not send a confirmation to the operating system or the wallet application.

[00382] Thus, (1) detecting a fingerprint without a press of the physical input mechanism 204 along with fingerprint authentication transitions the integrated biometric sensor from the first

sensor mode to a second sensor mode, (2) detecting a single press of the physical input mechanism 204 along with fingerprint authentication transitions the integrated biometric sensor from the first sensor mode to the second sensor mode, and (3) detecting a double press of the physical input mechanism 204 along with fingerprint authentication transitions the integrated biometric sensor from the first sensor mode to a third sensor mode.

[00383] FIG. 15E illustrates exemplary timelines for detected activations of a physical input mechanism. In the first exemplary timeline 1520, prior to event 1522, the electronic device is locked and in the first short-range communication radio payment mode (e.g., not enabled to participate in payment transactions via the short-range communication radio). At event 1522, the electronic device detects a finger on the fingerprint sensor. At event 1524, the device unlocks because an activation of the physical input mechanism was not detected within the 275ms predetermined period of time (if a fingerprint of the user is authenticated).

[00384] In the second exemplary timeline 1530, prior to event 1532, the electronic device is locked and in the first short-range communication radio payment mode (e.g., not enabled to participate in payment transactions via the short-range communication radio). At event 1532, the electronic device detects a finger on the fingerprint sensor. At event 1534, the device detects activation of the physical input mechanism within the 275ms predetermined period of time. At event 1536, the device unlocks because an reactivation of the physical input mechanism was not detected within the 300ms second predetermined period of time (if a fingerprint of the user is authenticated).

[00385] In the third exemplary timeline 1540, prior to event 1542, the electronic device is locked and in the first short-range communication radio payment mode (e.g., not enabled to participate in payment transactions via the short-range communication radio). At event 1542, the electronic device detects a finger on the fingerprint sensor. At event 1544, the device detects activation of the physical input mechanism within the 275ms predetermined period of time. At event 1546, the device detects reactivation of the physical input mechanism within the 300ms second predetermined period of time from the first activation and, as a result, the device transitions to a second short-range communication radio payment mode (e.g., enabled to participate in payment transactions via the short-range communication radio) different from the

first short-range communication radio payment mode (if a fingerprint of the user is authenticated).

[00386] FIG. 16 is a flow diagram illustrating a method for enabling an electronic device to participate in a payment transaction using a short-range communication radio, in accordance with some embodiments. Method 1600 is performed at a device (e.g., 100, 300, 500) with a short-range communication radio (e.g., NFC radio) and a physical input mechanism (e.g., mechanical or capacitive button) that includes an integrated biometric sensor (e.g., fingerprint sensor). Some operations in method 1600 may be combined, the order of some operations may be changed, and some operations may be omitted.

[00387] As described below, method 1600 provides an intuitive way for enabling an electronic device to participate in a payment transaction using a short-range communication radio. The method reduces the cognitive burden on a user for enabling an electronic device to participate in a payment transaction, thereby creating a more efficient human-machine interface. For battery-operated computing devices, enabling a user to enabling an electronic device to participate in a payment transaction using a short-range communication radio faster and more efficiently conserves power and increases the time between battery charges.

[00388] At block 1602, the electronic device is locked and in a first short-range communication radio payment mode.

[00389] At block 1604, the electronic device detects a fingerprint (e.g., at least a portion of a finger) using the integrated biometric sensor.

[00390] At block 1606, the electronic device determines whether the fingerprint is consistent with an enrolled fingerprint. In some examples, the determination of whether the fingerprint is consistent with the enrolled fingerprint happens before or after detecting the activation of the physical input mechanism.

[00391] At block 1608, the electronic device determines (e.g., at the electronic device) whether a set of one or more criteria is met, wherein the set of one or more criteria includes a criterion that is met when the physical input mechanism is activated within a first predetermined

period of time after detecting the fingerprint using the biometric sensor (e.g., a first touch of the mechanical or capacitive button).

[00392] At block 1610, in accordance with a determination that the fingerprint is consistent with an enrolled fingerprint and a determination that the set of one or more criteria is not met (e.g., no press), the electronic device unlocks (e.g., transitioning the electronic device from a lock state to an unlock state).

[00393] At block 1612, in accordance with a determination that the set of one or more criteria is met (e.g., a press), blocks 1614-1618 are assessed.

[00394] At block 1614, the device determines (e.g., at the electronic device) whether the physical input mechanism is reactivated within a second predetermined period of time after the activation of the physical input mechanism (e.g., a second press of the mechanical or capacitive button, resulting in a double-press).

[00395] At block 1616, in accordance with a determination that the physical input mechanism is not reactivated within the second predetermined period of time (e.g., a second press resulting in a double-press) and a determination that the fingerprint is consistent with an enrolled fingerprint, the electronic device unlocks (e.g., transitioning the electronic device from a lock state to an unlock state).

[00396] At block 1618, in accordance with a determination that the physical input mechanism is reactivated within the second predetermined period of time (e.g., a double-press) and in accordance with a determination that the fingerprint is consistent with an enrolled fingerprint, the electronic device transitions to a second short-range communication radio payment mode different from the first short-range communication radio payment mode (e.g., enabling the device to participate in payment transactions via the short-range communication radio; transitioning the electronic device to an armed state (e.g., advertising device can make a payment) in preparation for a payment transaction).

[00397] In some embodiments, in accordance with the determination that the fingerprint is consistent with the enrolled fingerprint and the determination that the set of one or more criteria is met (e.g., double-press), the electronic device forgoes unlocking.

[00398] In some embodiments, in accordance with a determination that the fingerprint is consistent with the enrolled fingerprint and a determination that the set of one or more criteria (e.g., double-press) is not met, the electronic device forgoes transitioning to the second short-range communication radio payment mode (e.g., forgoing enabling the device to participate in payment transactions via the short-range communication radio.).

[00399] In some embodiments, the first short-range communication radio payment mode is a mode in which the device is not enabled to participate in payment transactions via the short-range communication radio and the second short-range communication radio payment mode is a mode in which the device is enabled to participate in payment transactions via the short-range communication radio.

[00400] In some embodiments, the set of one or more criteria includes a criterion that is met when at least one payment account is linked to the device for use in payment transactions using the short-range communication radio (e.g., a credit card was previously provisioned on the device for NFC payments).

[00401] Thus, in this example the set of one or more criteria is satisfied when: (1) the physical input mechanism is activated within the predetermined period of time after detection of a fingerprint and (2) at least one payment account is linked to the device for use in payment transactions using the short-range communication radio.

[00402] In some embodiments, unlocking the device does not enable the device to participate in payment transactions via the short-range communication radio. In some embodiments, enabling the device to participate in payment transactions via the short-range communication radio does not unlock the device.

[00403] In some embodiments, determining whether the fingerprint is consistent with an enrolled fingerprint occurs subsequent to determining whether the set of one or more criteria is met.

[00404] In some embodiments, in accordance with a determination that the fingerprint is not consistent with the enrolled fingerprint, the electronic device forgoes transitioning to the second short-range communication radio payment mode and forgoes unlocking the device.

[00405] In some embodiments, the electronic device includes a display and the display is on while detecting the fingerprint using the integrated biometric sensor.

[00406] In some embodiments, unlocking the device further comprises providing fingerprint sensor information (e.g., a confirmation of a fingerprint match) of the integrated biometric sensor to a first application of the electronic device, the first application configured to unlock the device. For example, the integrated biometric sensor sends a single-use confirmation to the OS that allows the operating system to unlock the device.

[00407] In some embodiments, in accordance with the determination that: (1) the fingerprint is consistent with an enrolled fingerprint and (2) the set of one or more criteria is not met (e.g., no press within 300 ms), the electronic device transitions the integrated biometric sensor from a first sensor mode to a second sensor mode. For example, while in the second sensor mode, the integrated biometric sensor sends a single-use confirmation to the operating system that allows the operating system to unlock the device. In accordance with the determination that: (1) the set of one or more criteria is met (e.g., a press within 300 ms), (2) the physical input mechanism is not reactivated within the second predetermined period of time (e.g., no second press within 300 ms of the first press), and (3) the fingerprint is consistent with an enrolled fingerprint, the electronic device transitions the integrated biometric sensor from the first sensor mode to a second sensor mode. For example, while in the second sensor mode, the integrated biometric sensor sends a single-use confirmation to the operating system that allows the operating system to unlock the device. In accordance with the determination that: (1) the set of one or more criteria is met (e.g., a press within 300 ms), (2) the physical input mechanism is reactivated within the second predetermined period of time (e.g., within another 300 ms, resulting in a double-press), and (3) the fingerprint is consistent with an enrolled fingerprint, the electronic device transitions the integrated biometric sensor from the first sensor mode to a third sensor mode. For example, while in the third sensor mode, the integrated biometric sensor sends a single-use confirmation to a wallet application that allows the wallet application to enable the device to participate in payment transactions via the short-range communication radio. However, while in the first sensor mode, the integrated biometric sensor does not send a confirmation to the operating system or the wallet application.

[00408] Thus, (1) detecting a fingerprint without a press of the physical input mechanism 204 along with fingerprint authentication transitions the integrated biometric sensor from the first sensor mode to a second sensor mode, (2) detecting a single press of the physical input mechanism 204 along with fingerprint authentication transitions the integrated biometric sensor from the first sensor mode to the second sensor mode, and (3) detecting a double press of the physical input mechanism 204 along with fingerprint authentication transitions the integrated biometric sensor from the first sensor mode to a third sensor mode.

[00409] Note that details of the processes described above with respect to method 1600 (e.g., FIG. 16) are also applicable in an analogous manner to the methods described below and above. For example, method 1600 may include one or more of the characteristics of the various methods described above with reference to method 700, method 900, method 1100, and method 1400. For brevity, these details are not repeated below.

[00410] In accordance with some embodiments, FIG. 17 shows an exemplary functional block diagram of an electronic device 1700 configured in accordance with the principles of the various described embodiments. In accordance with some embodiments, the functional blocks of electronic device 1700 are configured to perform the techniques described above. The functional blocks of the device 1700 are, optionally, implemented by hardware, software, or a combination of hardware and software to carry out the principles of the various described examples. It is understood by persons of skill in the art that the functional blocks described in FIG. 17 are, optionally, combined or separated into sub-blocks to implement the principles of the various described examples. Therefore, the description herein optionally supports any possible combination or separation or further definition of the functional blocks described herein.

[00411] As shown in FIG. 17, an electronic device 1700 includes an (optional) display unit 1702 configured to display a graphic user interface, a physical input mechanism unit 1704 that includes an integrated biometric sensor unit 1706 configured to detect fingerprints, a short-range communication radio unit 1708, and a processing unit 1710 coupled to the (optional) display unit 1702, the physical input mechanism unit 1704 that includes the integrated biometric sensor unit 1706 configured to detect fingerprints, and the short-range communication radio unit 1708. In some embodiments, the processing unit 1710 includes a detecting unit 1712, a determining unit

1714, a transitioning unit 1716, an unlocking unit 1718, a display enabling unit 1720, an enabling unit 1722, and a providing unit 1724.

[00412] The processing unit 1710 is configured to: detect (e.g., using detecting unit 1712) activation of the physical input mechanism unit 1704; detect (e.g., using detecting unit 1712) a fingerprint using the integrated biometric sensor unit 1706; determine (e.g., using determining unit 1714) whether the fingerprint is consistent with an enrolled fingerprint; determine (e.g., using determining unit 1714) whether a set of one or more criteria is met, wherein the set of one or more criteria includes a criterion that is met when the physical input mechanism unit 1704 is reactivated within a predetermined period of time after the activation of the physical input mechanism unit 1704; in accordance with a determination that the fingerprint is consistent with the enrolled fingerprint and a determination that the set of one or more criteria is met, transition (e.g., using transitioning unit 1716) to a second short-range communication radio payment mode different from the first short-range communication radio payment mode (e.g., using short-range communication radio unit 1708); and in accordance with a determination that the fingerprint is consistent with the enrolled fingerprint and a determination that the set of one or more criteria is not met, unlock (e.g., using unlocking unit 1719) the electronic device.

[00413] In accordance with some embodiments, the processing unit 1710 is further configured to: in accordance with the determination that the fingerprint is consistent with the enrolled fingerprint and the determination that the set of one or more criteria is met, forgo unlocking (e.g., using the unlocking unit 1718) the device.

[00414] In accordance with some embodiments, the processing unit 1710 is further configured to: in accordance with a determination that the fingerprint is consistent with the enrolled fingerprint and a determination that the set of one or more criteria is not met, forgo transitioning (e.g., using transitioning unit 1716) to the second short-range communication radio payment mode.

[00415] In accordance with some embodiments, the first short-range communication radio payment mode is a mode in which the device is not enabled to participate in payment transactions via the short-range communication radio unit 1708 and the second short-range

communication radio payment mode is a mode in which the device is enabled to participate in payment transactions via the short-range communication radio unit 1708.

[00416] In accordance with some embodiments, wherein the set of one or more criteria includes a criterion that is met when at least one payment account is linked to the electronic device for use in payment transactions using the short-range communication radio unit 1708.

[00417] In accordance with some embodiments, the processing unit 1710 is further configured to: in response to detecting (e.g., using detecting unit 1712) activation of the physical input mechanism unit 1704, enable (e.g. using enabling unit 1722) the integrated biometric sensor unit 1706 to detect fingerprints.

[00418] In accordance with some embodiments, the processing unit 1710 is further configured to: in response to detecting (e.g., using detecting unit 1712) activation of the physical input mechanism unit 1704, turning on (e.g., using display enabling unit 1720) the display unit 1702 of the electronic device.

[00419] In accordance with some embodiments, unlocking (e.g., using unlocking unit 1718) the electronic device does not enable (e.g., using enabling unit 1722) the device to participate in payment transactions via the short-range communication radio unit 1708.

[00420] In accordance with some embodiments, enabling (e.g., using enabling unit 1722) the device to participate in payment transactions via the short-range communication radio unit 1708 does not unlock (e.g., using unlocking unit 1718) the device.

[00421] In accordance with some embodiments, determining (e.g., using determining unit 1714) whether the fingerprint is consistent with an enrolled fingerprint occurs subsequent to determining (e.g., using determining unit 1714) whether the set of one or more criteria is met.

[00422] In accordance with some embodiments, the processing unit 1710 is further configured to: in accordance with a determination that the fingerprint is not consistent with the enrolled fingerprint, forgo transitioning (e.g., using transitioning unit 1716) to the second short-range communication radio payment mode and forgoing unlocking (e.g., using unlocking unit 1718) the electronic device.

2016102031 24 Nov 2016

[00423] In accordance with some embodiments, to unlock the device, the processing unit 1710 is further configured to: provide (e.g., using providing unit 1724) fingerprint sensor information of the integrated biometric sensor unit 1706 to a first application of the electronic device, wherein the first application configured to unlock (e.g., using unlocking unit 1718) the device.

[00424] In accordance with some embodiments, the processing unit 1710 is further configured to: in accordance with the determination that the fingerprint is consistent with the enrolled fingerprint and the determination that the set of one or more criteria is not met, transition (e.g., using transitioning unit 1716) the integrated biometric sensor unit 1706 from a first sensor mode to a second sensor mode; and in accordance with the determination that the fingerprint is consistent with the enrolled fingerprint and the determination that the set of one or more criteria is not met, transitioning (e.g., using transitioning unit 1716) the integrated biometric sensor unit 1706 from the first sensor mode to a third sensor mode.

[00425] The operations described above with reference to FIG. 14 are, optionally, implemented by components depicted in FIGS. 1A-1B or FIG. 17. For example, detecting operation 1404, determining operation 1406, and transitioning operation 1412 may be implemented by event sorter 170, event recognizer 180, and event handler 190. Event monitor 171 in event sorter 170 detects a contact on touch-sensitive display 112, and event dispatcher module 174 delivers the event information to application 136-1. A respective event recognizer 180 of application 136-1 compares the event information to respective event definitions 186, and determines whether a first contact at a first location on the touch-sensitive surface corresponds to a predefined event or sub event, such as activation of an affordance on a user interface. When a respective predefined event or sub-event is detected, event recognizer 180 activates an event handler 190 associated with the detection of the event or sub-event. Event handler 190 may utilize or call data updater 176 or object updater 177 to update the application internal state 192. In some embodiments, event handler 190 accesses a respective GUI updater 178 to update what is displayed by the application. Similarly, it would be clear to a person having ordinary skill in the art how other processes can be implemented based on the components depicted in FIGS. 1A-1B.

[00426] In accordance with some embodiments, FIG. 18 shows an exemplary functional block diagram of an electronic device 1800 configured in accordance with the principles of the various described embodiments. In accordance with some embodiments, the functional blocks of electronic device 1800 are configured to perform the techniques described above. The functional blocks of the device 1800 are, optionally, implemented by hardware, software, or a combination of hardware and software to carry out the principles of the various described examples. It is understood by persons of skill in the art that the functional blocks described in FIG. 18 are, optionally, combined or separated into sub-blocks to implement the principles of the various described examples. Therefore, the description herein optionally supports any possible combination or separation or further definition of the functional blocks described herein.

[00427] As shown in FIG. 18, an electronic device 1800 includes an (optional) display unit 1802 configured to display a graphic user interface, a physical input mechanism unit 1804 that includes an integrated biometric sensor unit 1806 configured to detect fingerprints, a short-range communication radio unit 1808, and a processing unit 1810 coupled to the (optional) display unit 1804, the physical input mechanism unit 1804 that includes the integrated biometric sensor unit 1806 configured to detect fingerprints, and the short-range communication radio unit 1808. In some embodiments, the processing unit 1810 includes a detecting unit 1812, a determining unit 1814, a transitioning unit 1816, an unlocking unit 1818, an enabling unit 1820, and a providing unit 1822.

[00428] The processing unit 1810 is configured to: detect (e.g., using detecting unit 1812) a fingerprint using the integrated biometric sensor unit 1806; determine (e.g., using determining unit 1814) whether the fingerprint is consistent with an enrolled fingerprint; determine (e.g., using determining unit 1814) whether a set of one or more criteria is met, wherein the set of one or more criteria includes a criterion that is met when the physical input mechanism unit 1804 is activated within a first predetermined period of time after detecting the fingerprint using the biometric sensor unit 1806; in accordance with a determination that the fingerprint is consistent with an enrolled fingerprint and a determination that the set of one or more criteria is not met, unlock (e.g., using unlocking unit 1818) the electronic device; and in accordance with a determination that the set of one or more criteria is met: determine (e.g., using determining unit 1814) whether the physical input mechanism unit 1804 is reactivated within a second

predetermined period of time after the activation of the physical input mechanism unit 1804; in accordance with a determination that the physical input mechanism unit 1804 is not reactivated within the second predetermined period of time and a determination that the fingerprint is consistent with an enrolled fingerprint, unlock (e.g., using unlocking unit 1818) the electronic device; and in accordance with a determination that the physical input mechanism is reactivated within the second predetermined period of time and in accordance with a determination that the fingerprint is consistent with an enrolled fingerprint, transition (e.g., using transitioning unit 1816) to a second short-range communication radio payment mode different from the first short-range communication radio payment mode (e.g., using short-range communication radio unit 1808).

[00429] In accordance with some embodiments, the processing unit 1810 is further configured to: in accordance with the determination that the fingerprint is consistent with the enrolled fingerprint and the determination that the set of one or more criteria is met, forgo unlocking (e.g., using unlocking unit 1818) the device.

[00430] In accordance with some embodiments, the processing unit 1810 is further configured to: in accordance with a determination that the fingerprint is consistent with the enrolled fingerprint and a determination that the set of one or more criteria is not met, forgo transitioning (e.g., using transitioning unit 1816) to the second short-range communication radio payment mode.

[00431] In accordance with some embodiments, the first short-range communication radio payment mode is a mode in which the device is not enabled to participate in payment transactions via the short-range communication radio unit 1808 and the second short-range communication radio payment mode is a mode in which the device is enabled to participate in payment transactions via the short-range communication radio unit 1808.

[00432] In accordance with some embodiments, the set of one or more criteria includes a criterion that is met when at least one payment account is linked to the device for use in payment transactions using the short-range communication radio unit 1808.

[00433] In accordance with some embodiments, unlocking (e.g., using unlocking unit 1818) the device does not enable (e.g., using enabling unit 1820) the device to participate in payment transactions via the short-range communication radio unit 1808.

[00434] In accordance with some embodiments, enabling (e.g., using the enabling unit 1820) the device to participate in payment transactions via the short-range communication radio unit 1808 does not unlock (e.g., using unlocking unit 1818) the device.

[00435] In accordance with some embodiments, determining (e.g., using determining unit 1814) whether the fingerprint is consistent with an enrolled fingerprint occurs subsequent to determining (e.g., using determining unit 1814) whether the set of one or more criteria is met.

[00436] In accordance with some embodiments, the processing unit 1810 is further configured to: in accordance with a determination that the fingerprint is not consistent with the enrolled fingerprint, forgo transitioning (e.g., using transitioning unit 1816) to the second short-range communication radio payment mode and forgo unlocking (e.g., using unlocking unit 1818) the device.

[00437] In accordance with some embodiments, the display unit 1802 is on while detecting (e.g., using detecting unit 1812) the fingerprint using the integrated biometric sensor unit 1806.

[00438] In accordance with some embodiments, to unlock the device, the processing unit 1810 is further configured to: provide (e.g., using providing unit 1822) fingerprint sensor information of the integrated biometric sensor unit 1806 to a first application of the electronic device, the first application configured to unlock (e.g., using unlocking unit 1818) the electronic device.

[00439] In accordance with some embodiments, the processing unit 1810 is further configured to: in accordance with the determination that the fingerprint is consistent with an enrolled fingerprint and the determination that the set of one or more criteria is not met, transition (e.g., using transitioning unit 1816) the integrated biometric sensor unit 1806 from a first sensor mode to a second sensor mode; and in accordance with the determination that the set of one or more criteria is met: in accordance with the determination that the physical input mechanism is not reactivated within the second predetermined period of time and the determination that the fingerprint is consistent with an enrolled fingerprint, transition (e.g., using transitioning unit

2016102031 24 Nov 2016

1816) the integrated biometric sensor unit 1806 from the first sensor mode to a second sensor mode; and in accordance with the determination that the physical input mechanism is reactivated within the second predetermined period of time and the determination that the fingerprint is consistent with an enrolled fingerprint, transition (e.g., using transitioning unit 1816) the integrated biometric sensor unit 1806 from the first sensor mode to a third sensor mode.

[00440] The operations described above with reference to FIG. 16 are, optionally, implemented by components depicted in FIGS. 1A-1B or FIG. 18. For example, detecting operation 1604, determining operation 1606, and unlocking operation 1610 may be implemented by event sorter 170, event recognizer 180, and event handler 190. Event monitor 171 in event sorter 170 detects a contact on touch-sensitive display 112, and event dispatcher module 174 delivers the event information to application 136-1. A respective event recognizer 180 of application 136-1 compares the event information to respective event definitions 186, and determines whether a first contact at a first location on the touch-sensitive surface corresponds to a predefined event or sub event, such as activation of an affordance on a user interface. When a respective predefined event or sub-event is detected, event recognizer 180 activates an event handler 190 associated with the detection of the event or sub-event. Event handler 190 may utilize or call data updater 176 or object updater 177 to update the application internal state 192. In some embodiments, event handler 190 accesses a respective GUI updater 178 to update what is displayed by the application. Similarly, it would be clear to a person having ordinary skill in the art how other processes can be implemented based on the components depicted in FIGS. 1A-1B.

[00441] The foregoing description, for purpose of explanation, has been described with reference to specific embodiments. However, the illustrative discussions above are not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many modifications and variations are possible in view of the above teachings. The embodiments were chosen and described in order to best explain the principles of the techniques and their practical applications. Others skilled in the art are thereby enabled to best utilize the techniques and various embodiments with various modifications as are suited to the particular use contemplated.

[00442] Although the disclosure and examples have been fully described with reference to the accompanying drawings, it is to be noted that various changes and modifications will become apparent to those skilled in the art. Such changes and modifications are to be understood as being included within the scope of the disclosure and examples as defined by the claims.

[00443] As described above, one aspect of the present technology is the gathering and use of data available from various sources to improve the delivery to users of invitational content or any other content that may be of interest to them. The present disclosure contemplates that in some instances, this gathered data may include personal information data that uniquely identifies or can be used to contact or locate a specific person. Such personal information data can include demographic data, location-based data, telephone numbers, email addresses, home addresses, or any other identifying information.

[00444] The present disclosure recognizes that the use of such personal information data, in the present technology, can be used to the benefit of users. For example, the personal information data can be used to deliver targeted content that is of greater interest to the user. Accordingly, use of such personal information data enables calculated control of the delivered content. Further, other uses for personal information data that benefit the user are also contemplated by the present disclosure.

[00445] The present disclosure further contemplates that the entities responsible for the collection, analysis, disclosure, transfer, storage, or other use of such personal information data will comply with well-established privacy policies and/or privacy practices. In particular, such entities should implement and consistently use privacy policies and practices that are generally recognized as meeting or exceeding industry or governmental requirements for maintaining personal information data private and secure. For example, personal information from users should be collected for legitimate and reasonable uses of the entity and not shared or sold outside of those legitimate uses. Further, such collection should occur only after receiving the informed consent of the users. Additionally, such entities would take any needed steps for safeguarding and securing access to such personal information data and ensuring that others with access to the personal information data adhere to their privacy policies and procedures. Further, such entities

can subject themselves to evaluation by third parties to certify their adherence to widely accepted privacy policies and practices.

[00446] Despite the foregoing, the present disclosure also contemplates embodiments in which users selectively block the use of, or access to, personal information data. That is, the present disclosure contemplates that hardware and/or software elements can be provided to prevent or block access to such personal information data. For example, in the case of advertisement delivery services, the present technology can be configured to allow users to select to “opt in” or “opt out” of participation in the collection of personal information data during registration for services. In another example, users can select not to provide location information for targeted content delivery services. In yet another example, users can select to not provide precise location information, but permit the transfer of location zone information.

[00447] Therefore, although the present disclosure broadly covers use of personal information data to implement one or more various disclosed embodiments, the present disclosure also contemplates that the various embodiments can also be implemented without the need for accessing such personal information data. That is, the various embodiments of the present technology are not rendered inoperable due to the lack of all or a portion of such personal information data. For example, content can be selected and delivered to users by inferring preferences based on non-personal information data or a bare minimum amount of personal information, such as the content being requested by the device associated with a user, other non-personal information available to the content delivery services, or publically available information.

CLAIMS

What is claimed is:

1. A method, comprising:
at an electronic device with a display and a camera sensor:
displaying, on the display, a user interface comprising:
a credit card input affordance for receiving, at the electronic device, at least partial credit card information;
receiving selection of the credit card input affordance;
in response to receiving the selection of the credit card input affordance,
concurrently displaying, on the display:
a live preview of images obtained via the camera sensor; and
a manual credit card entry affordance that, when selected, triggers display of one or more text entry fields and a character entry control that includes a plurality of character keys for entering characters into a text entry field of the one or more text entry fields; and
while concurrently displaying the live preview of images obtained via the camera sensor and the manual credit card entry affordance:
in accordance with detection of at least partial credit card information of a credit card in a field of view of the camera sensor, ceasing to display the manual credit card entry affordance and displaying the detected at least partial credit card information of the credit card on the display once the at least partial credit card information has been detected in the field of view of the camera sensor.
2. The method of claim 1, wherein the live preview is displayed on the display immediately in response to receiving the selection of the credit card input affordance, and without displaying an intervening user interface on the display.
3. The method of any of claims 1-2, wherein the at least partial credit card information of the credit card includes a portion of an account number of the credit card, and further comprising:
determining, based on the portion of the account number of the credit card, whether the credit card is of a first type;

in accordance with a determination that the credit card is not of the first type, displaying an expiration date of the credit card in a first entry field and a security code of the credit card in a second entry field; and

in accordance with a determination that the credit card is of the first type, forgoing displaying the expiration date of the credit card in the first entry field and forgoing displaying the security code of the credit card in the second entry field.

4. The method of any of claims 1-3 further comprising:
displaying two or more input fields associated with the credit card; and
wherein the quantity of the two or more input fields is based on an image obtained via the camera sensor.

5. A computer-readable storage medium comprising one or more programs for execution by one or more processors of an electronic device with a display and a camera sensor, the one or more programs including instructions for performing the method of any of claims 1-4.

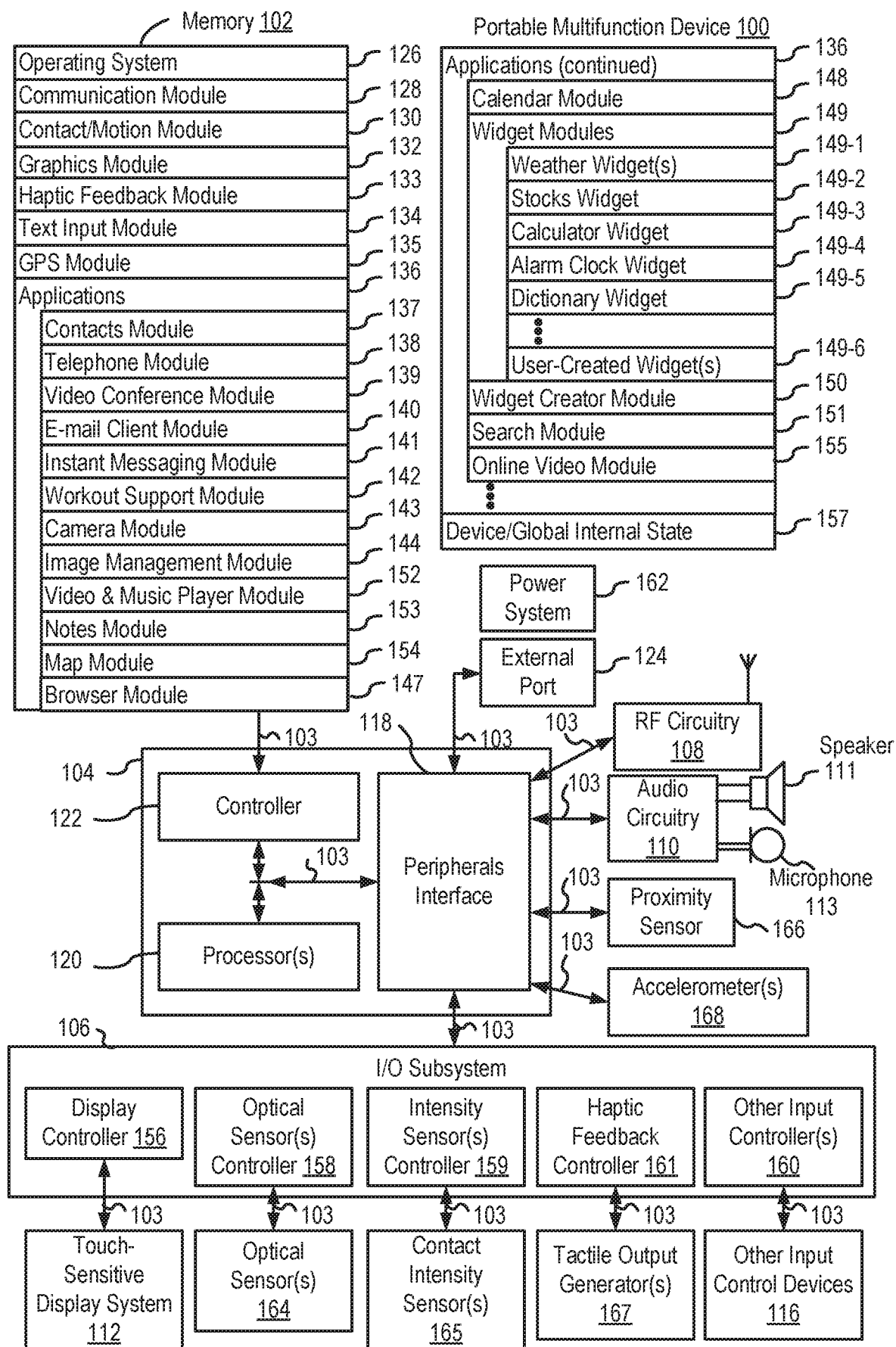


FIG. 1A

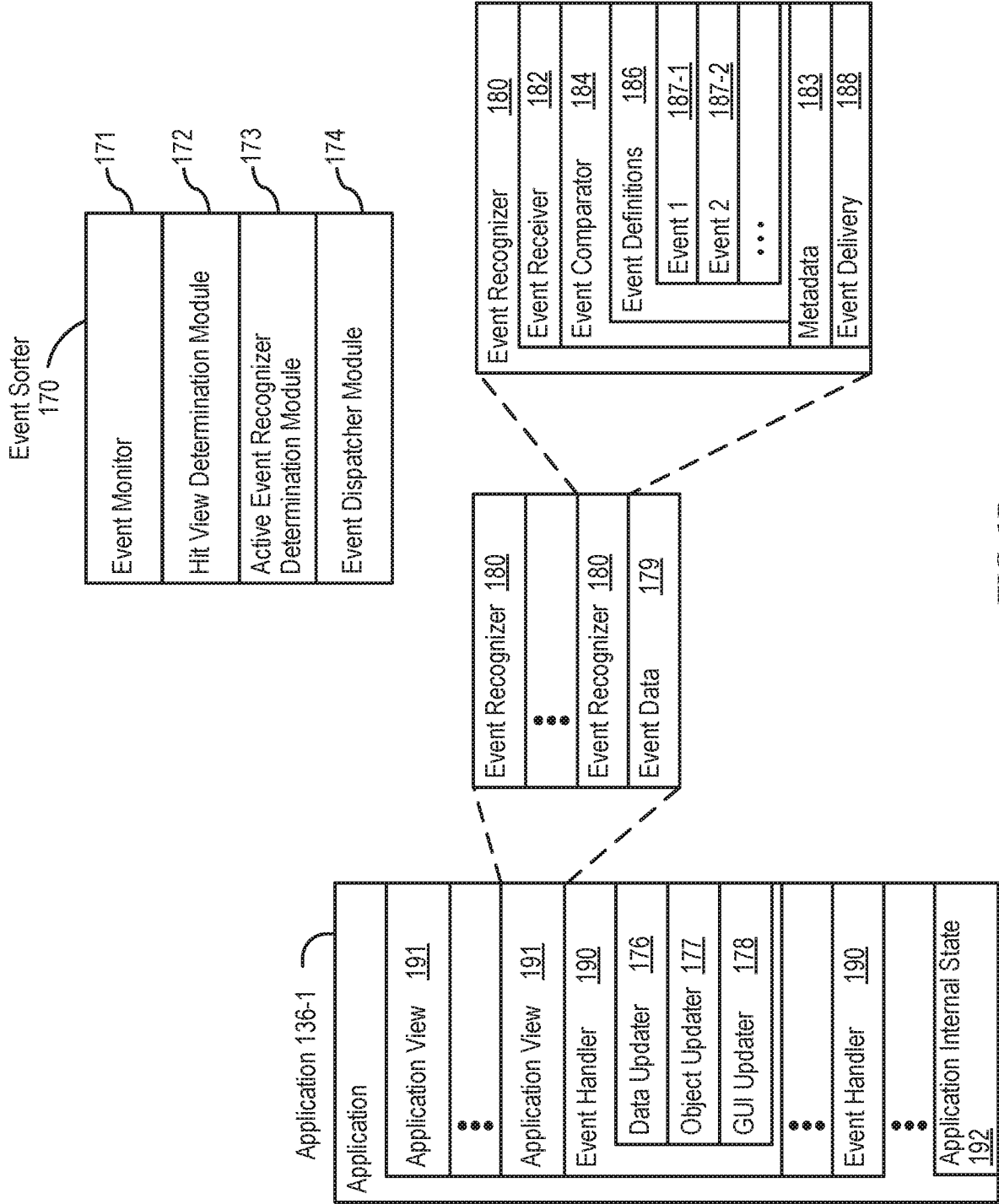


FIG. 1B

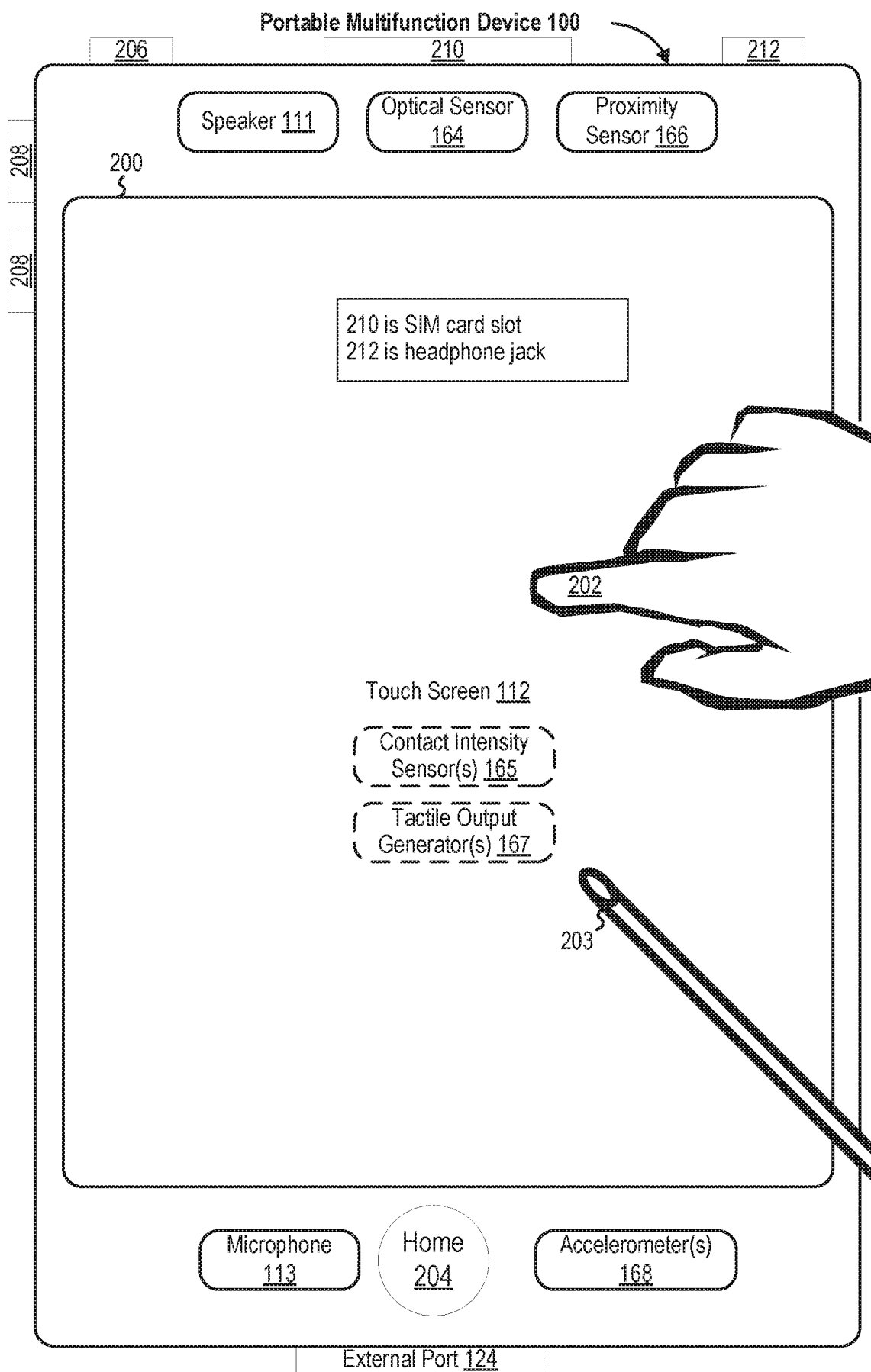


FIG. 2

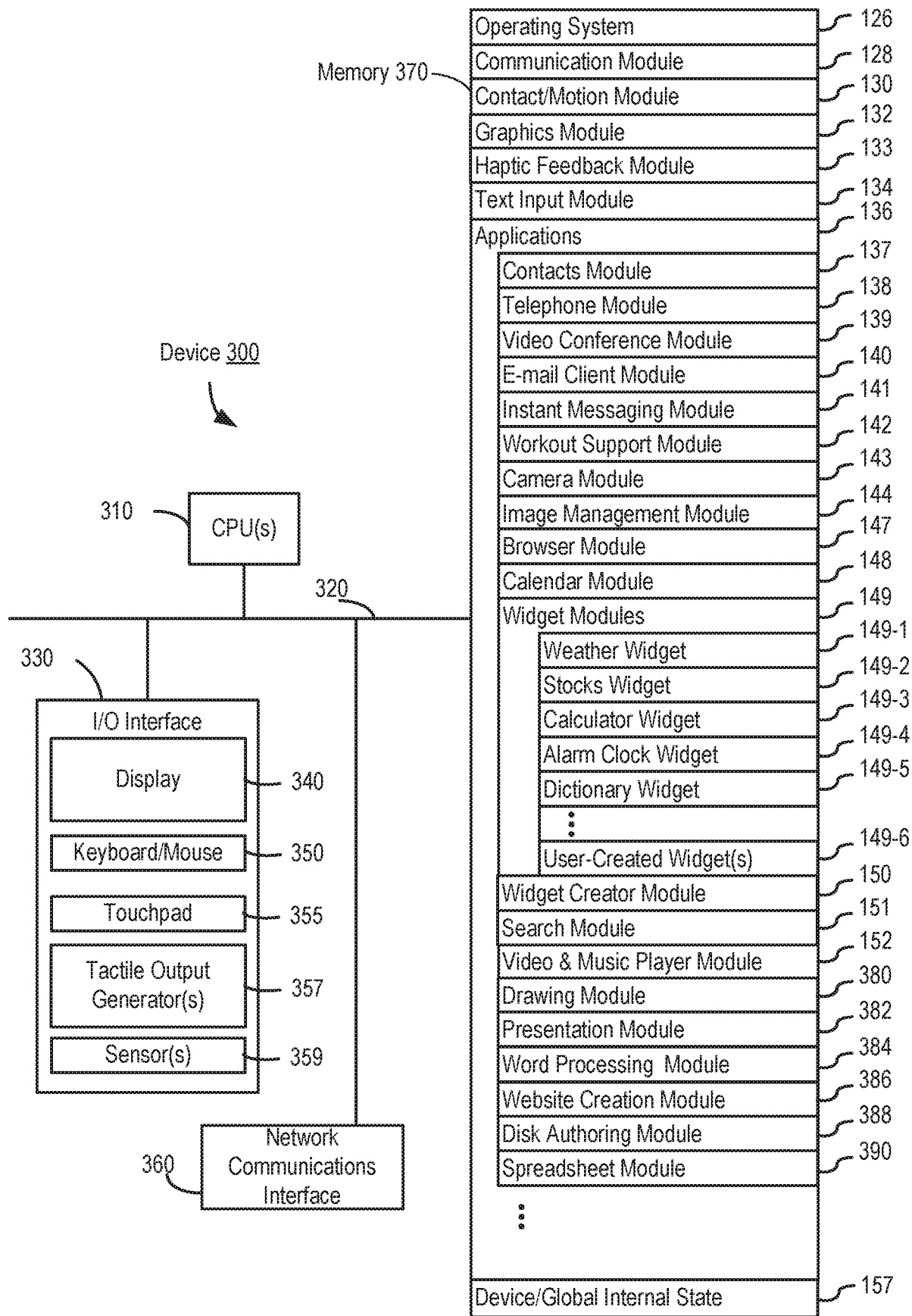


FIG. 3

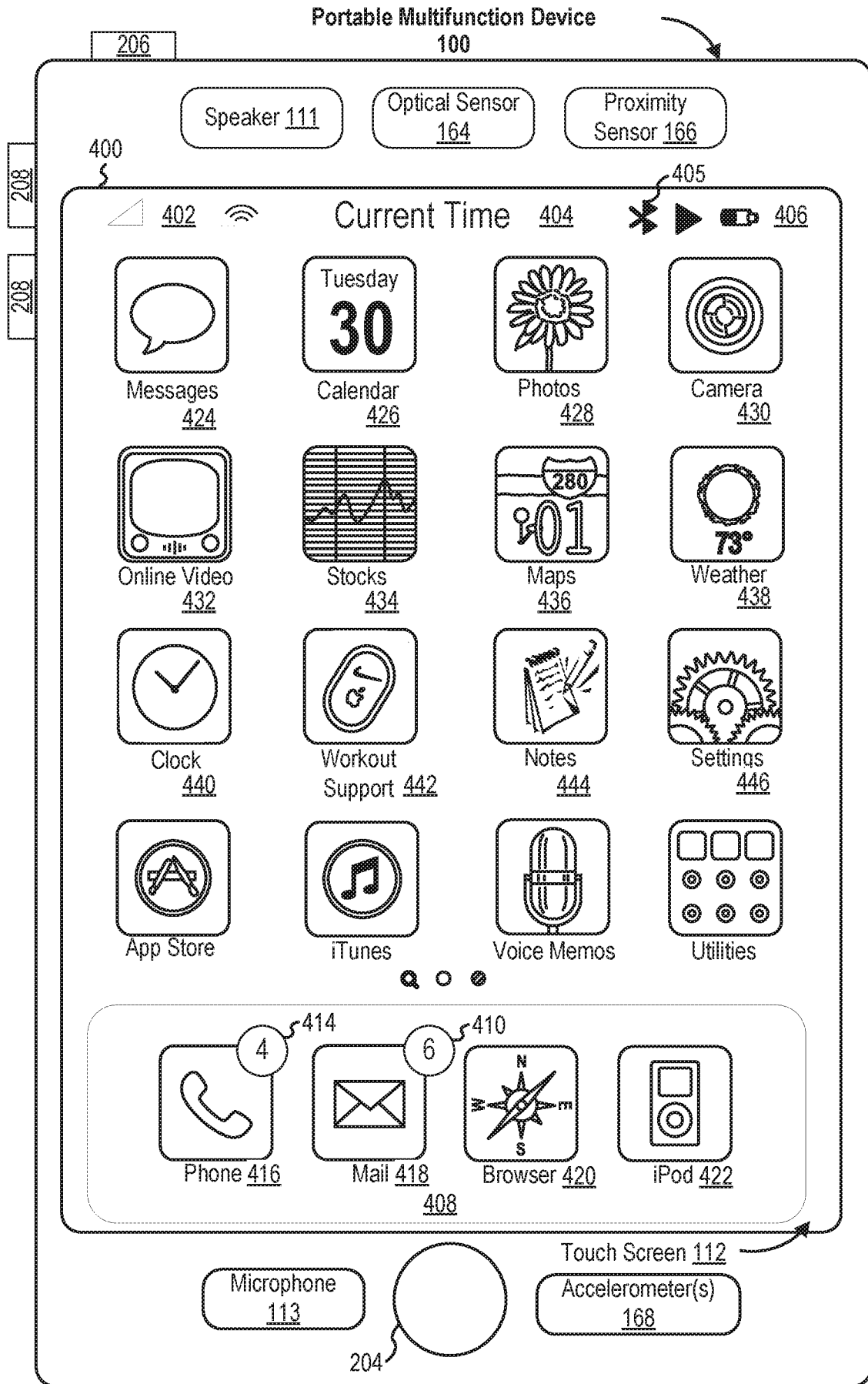


FIG. 4A

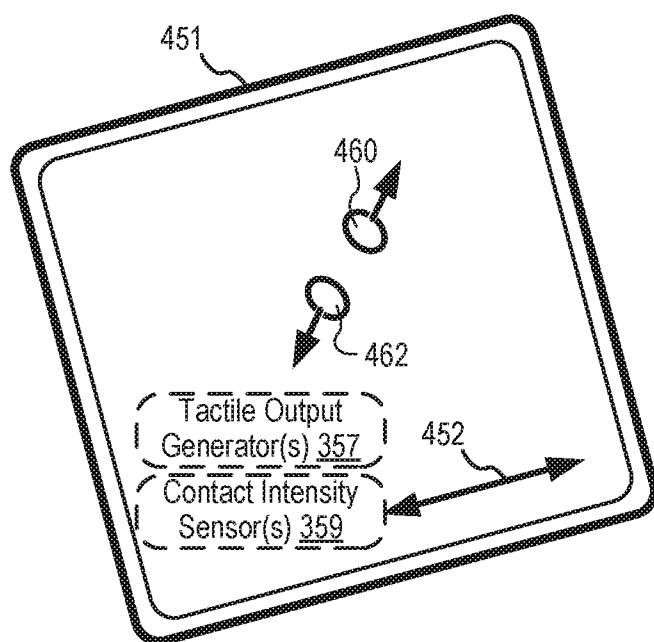
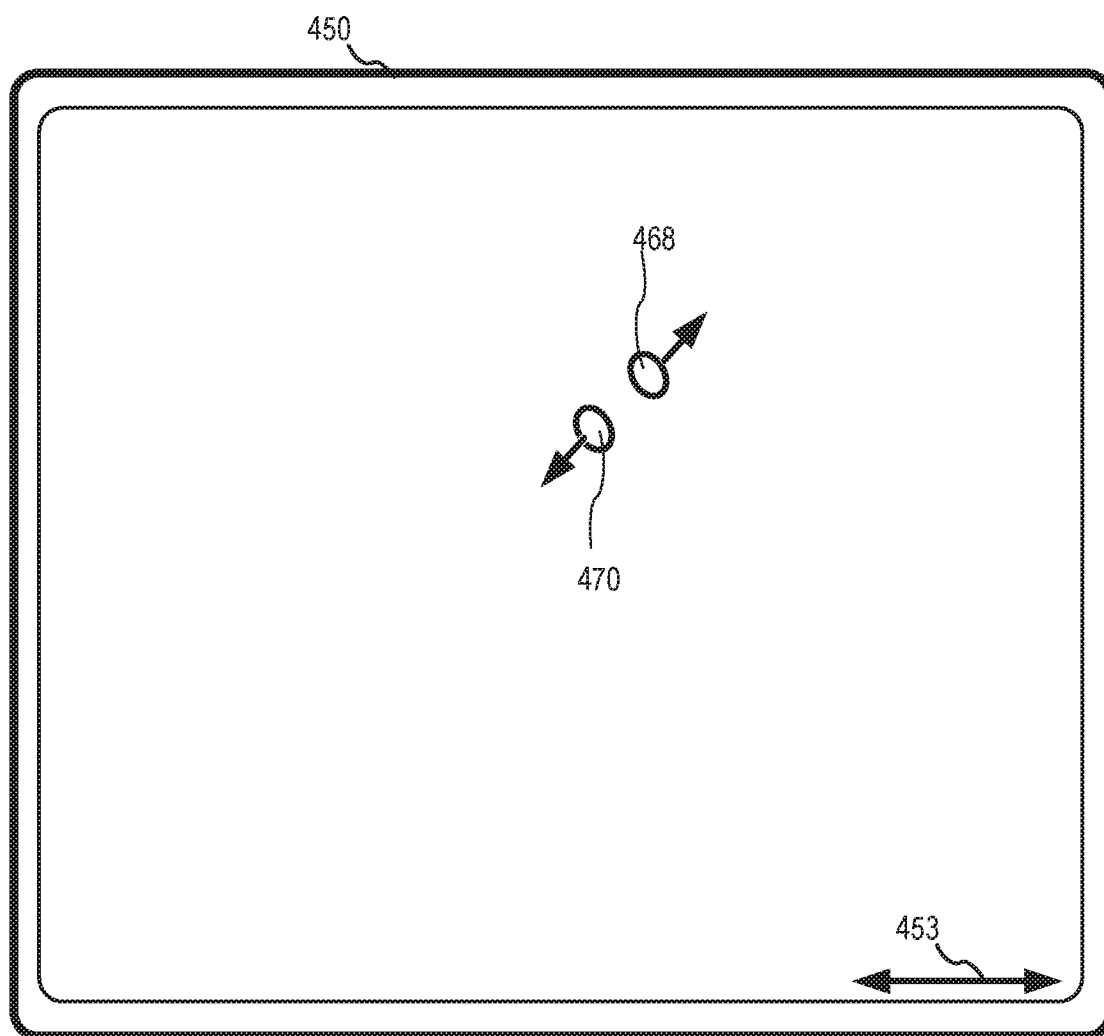
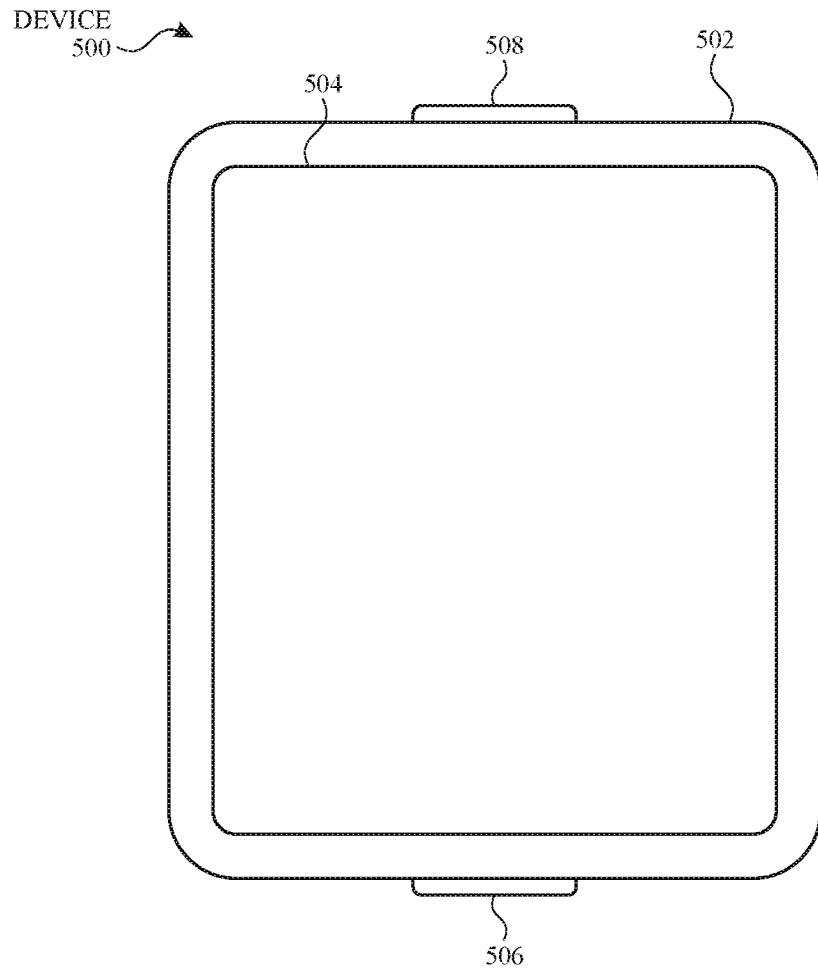


FIG. 4B

*FIG. 5A*

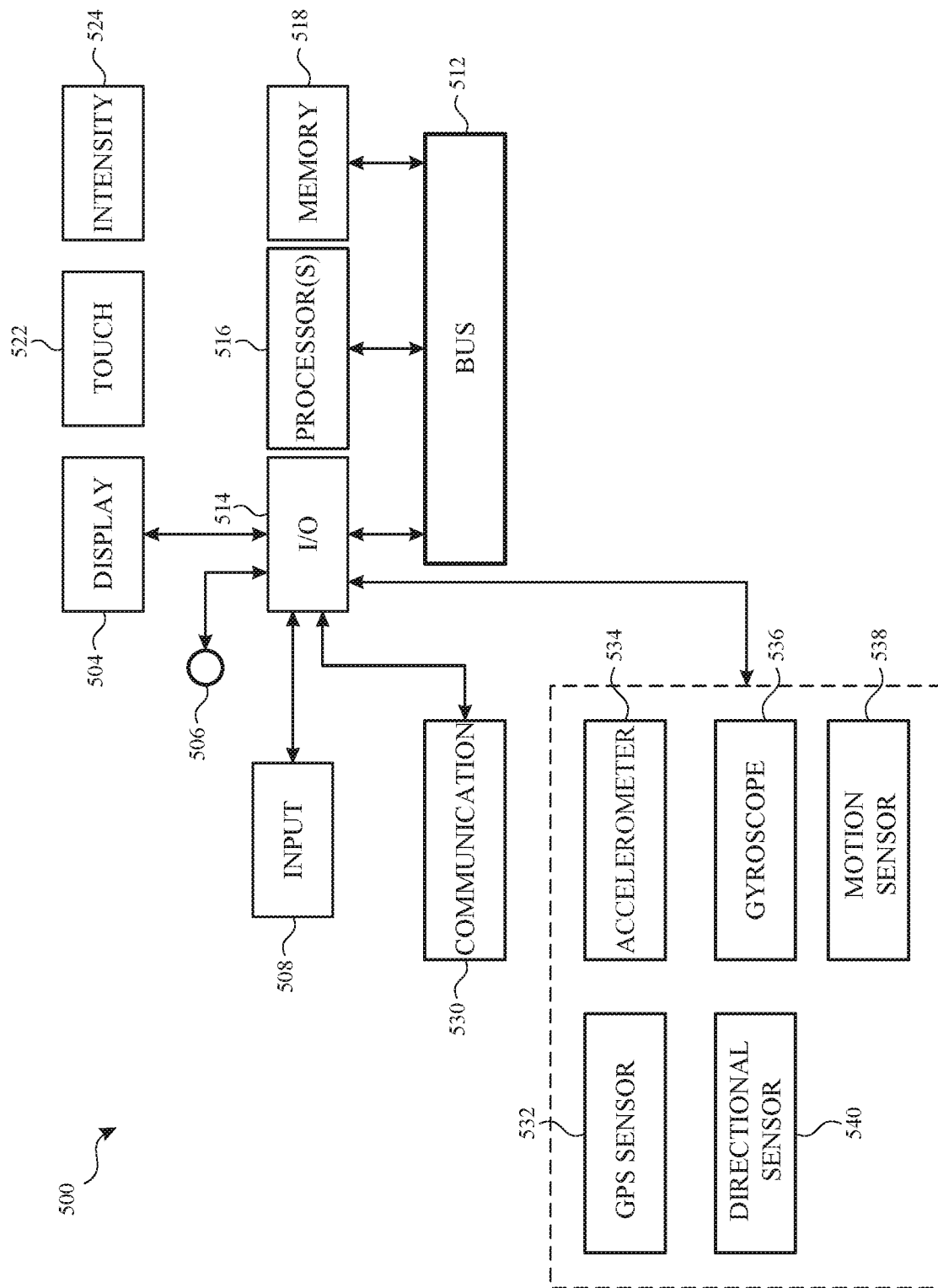


FIG. 5B

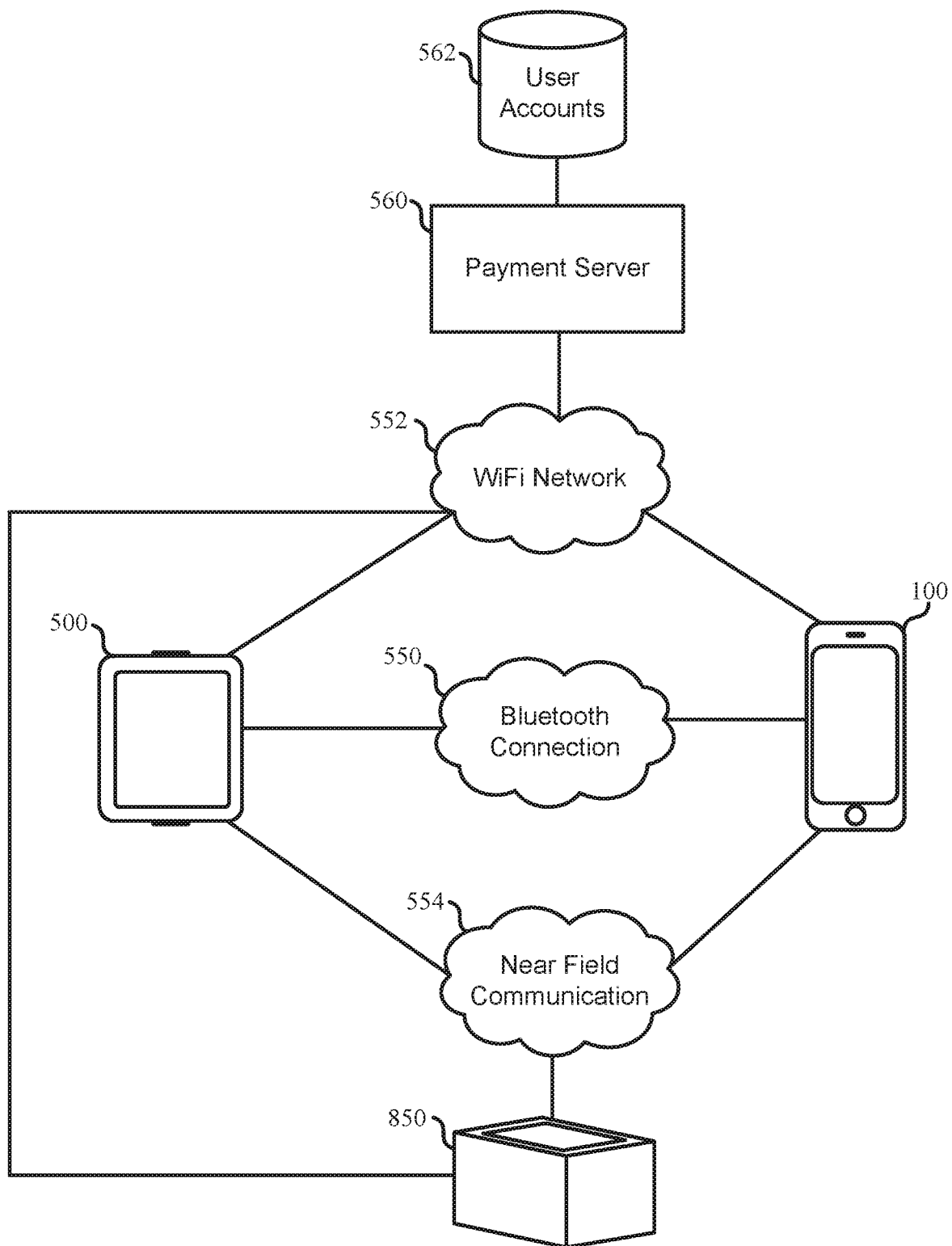


FIG. 5C

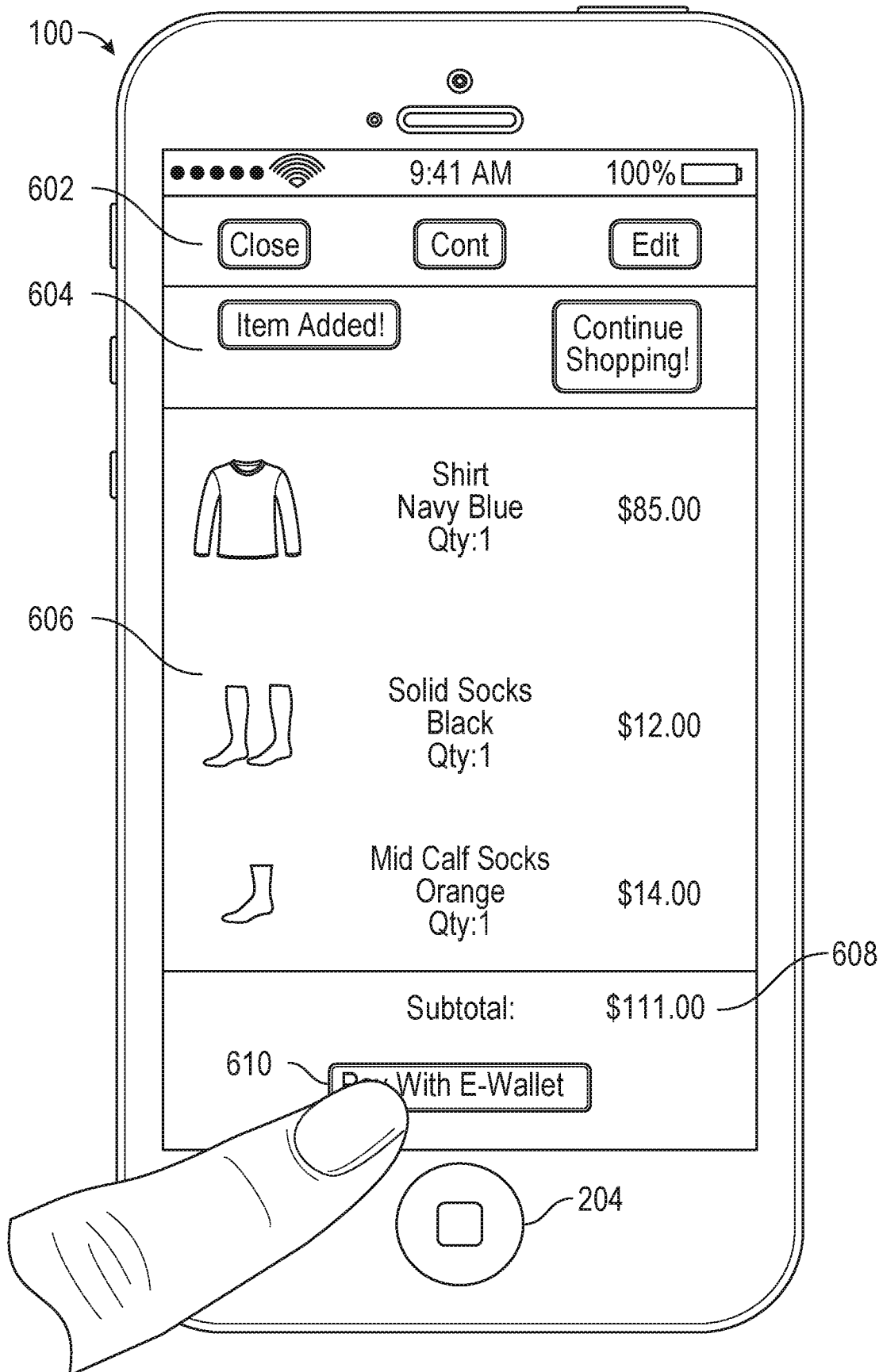


FIG. 6A

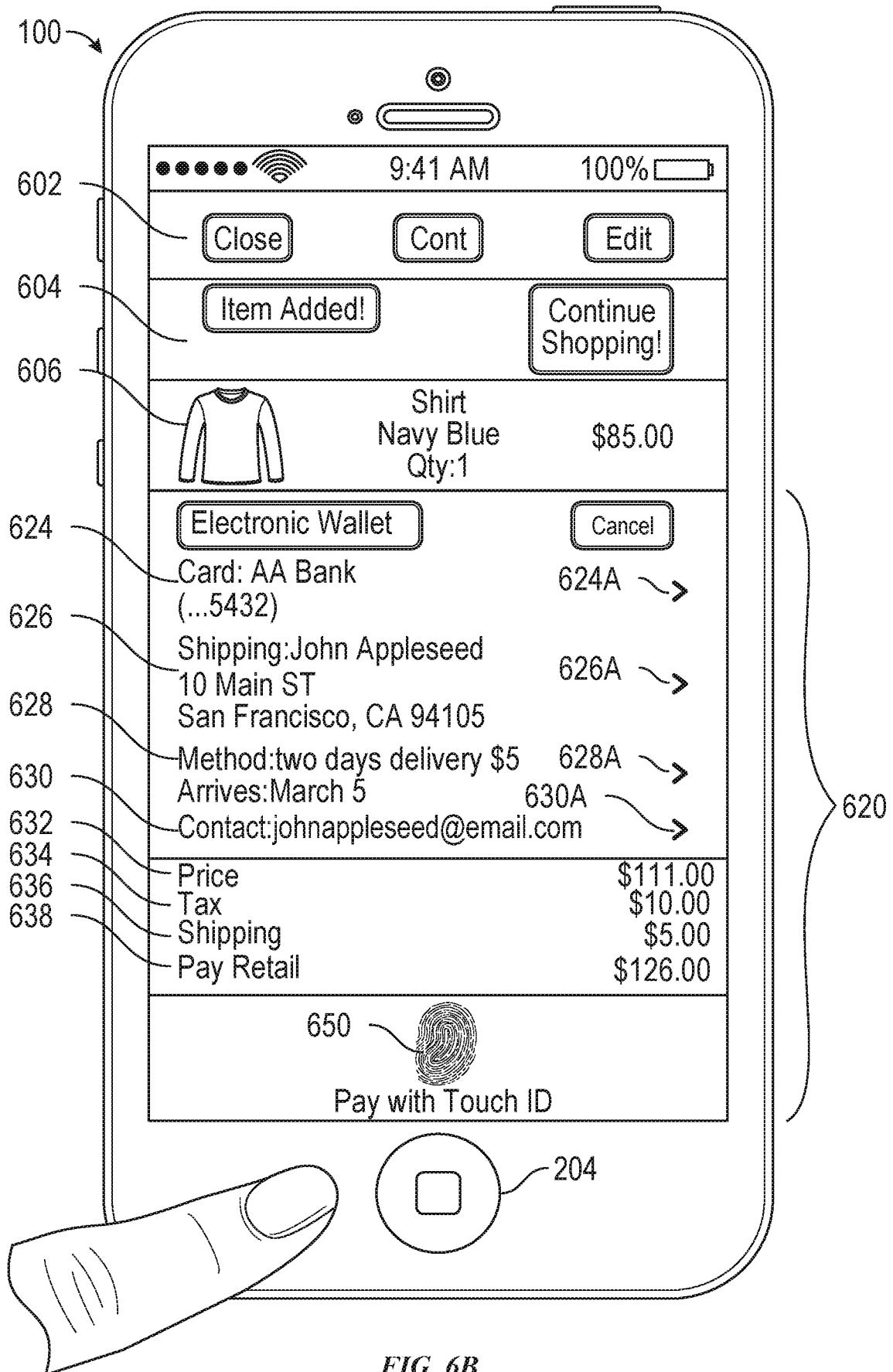


FIG. 6B

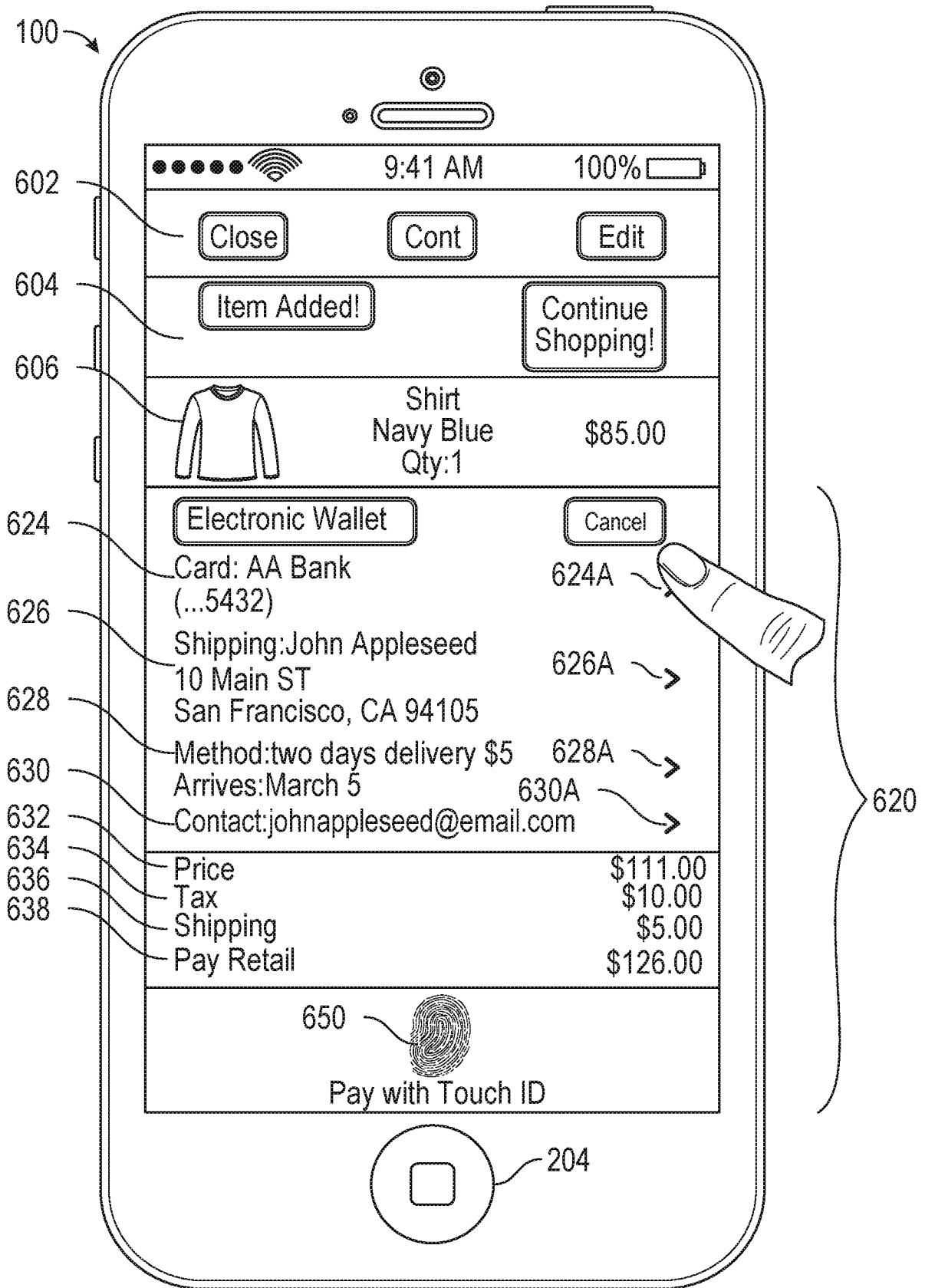


FIG. 6C

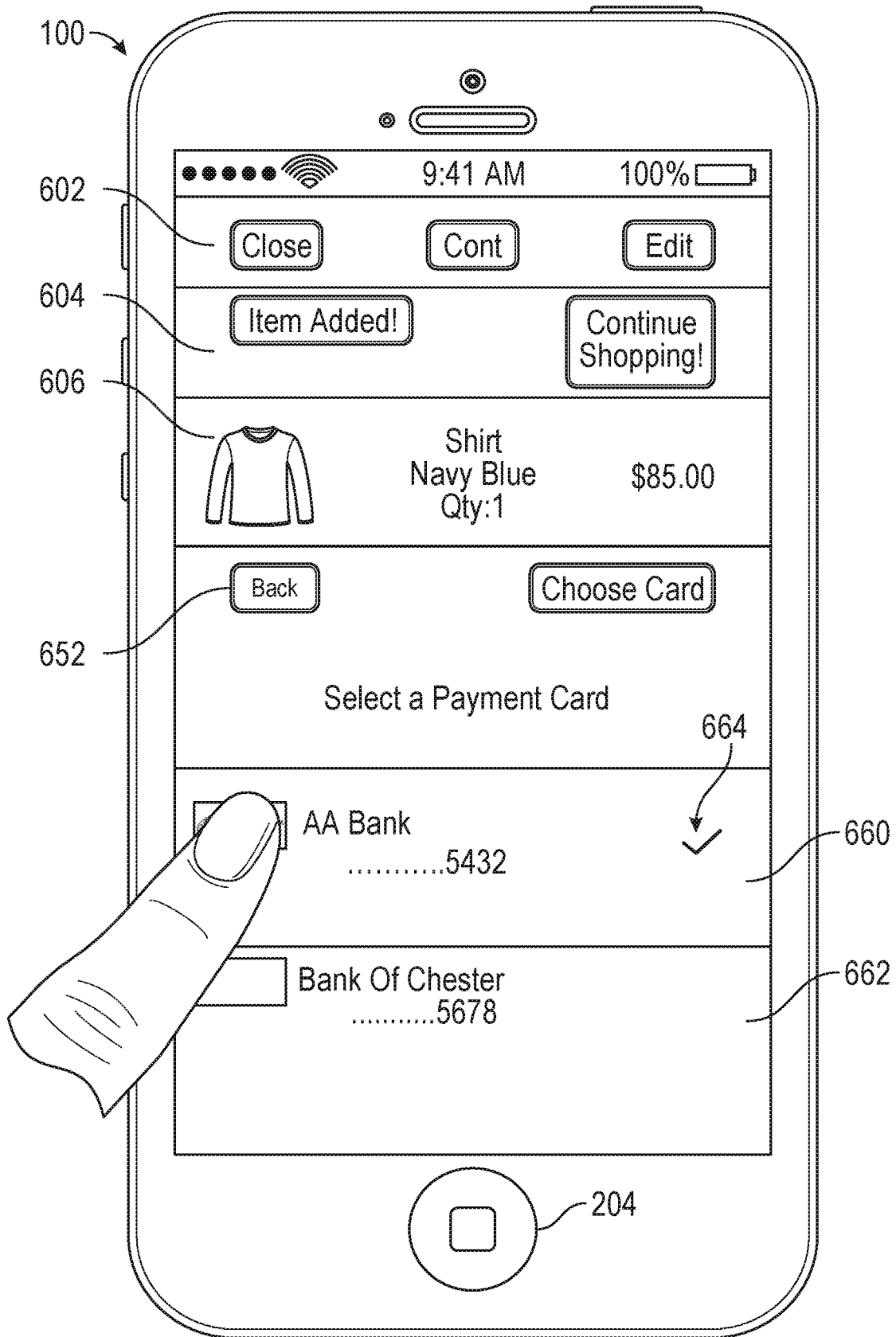


FIG. 6D

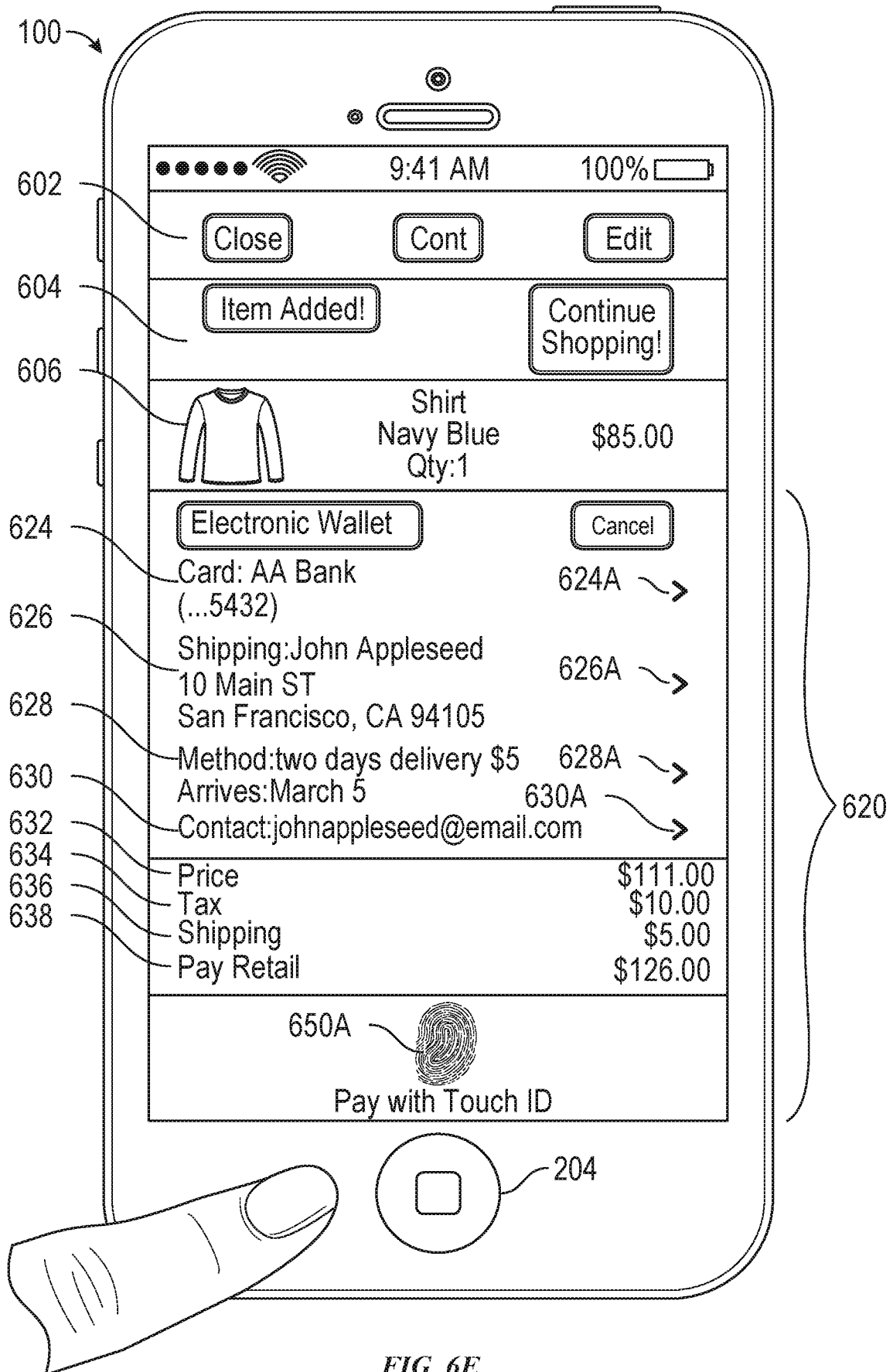


FIG. 6E

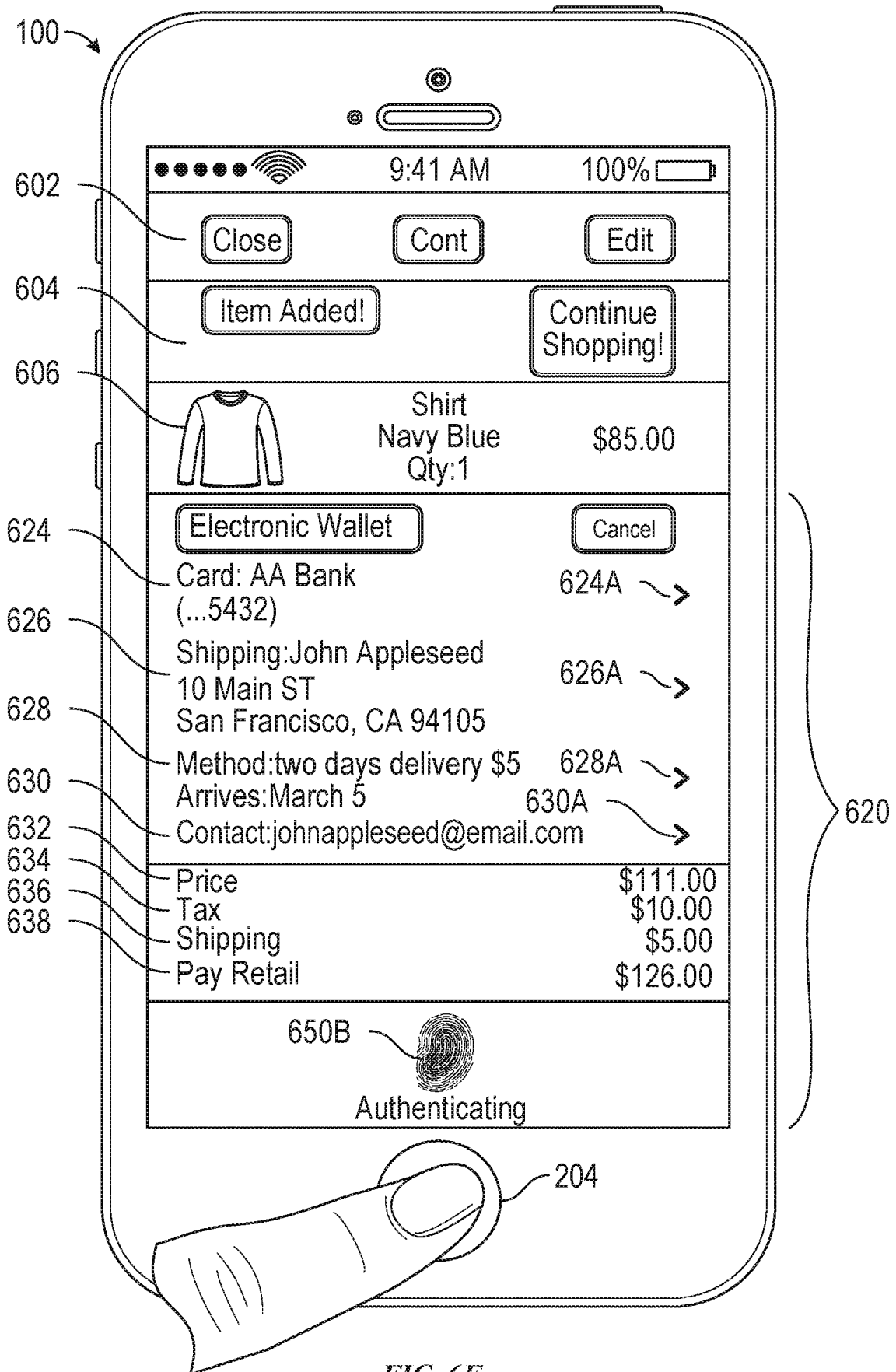


FIG. 6F

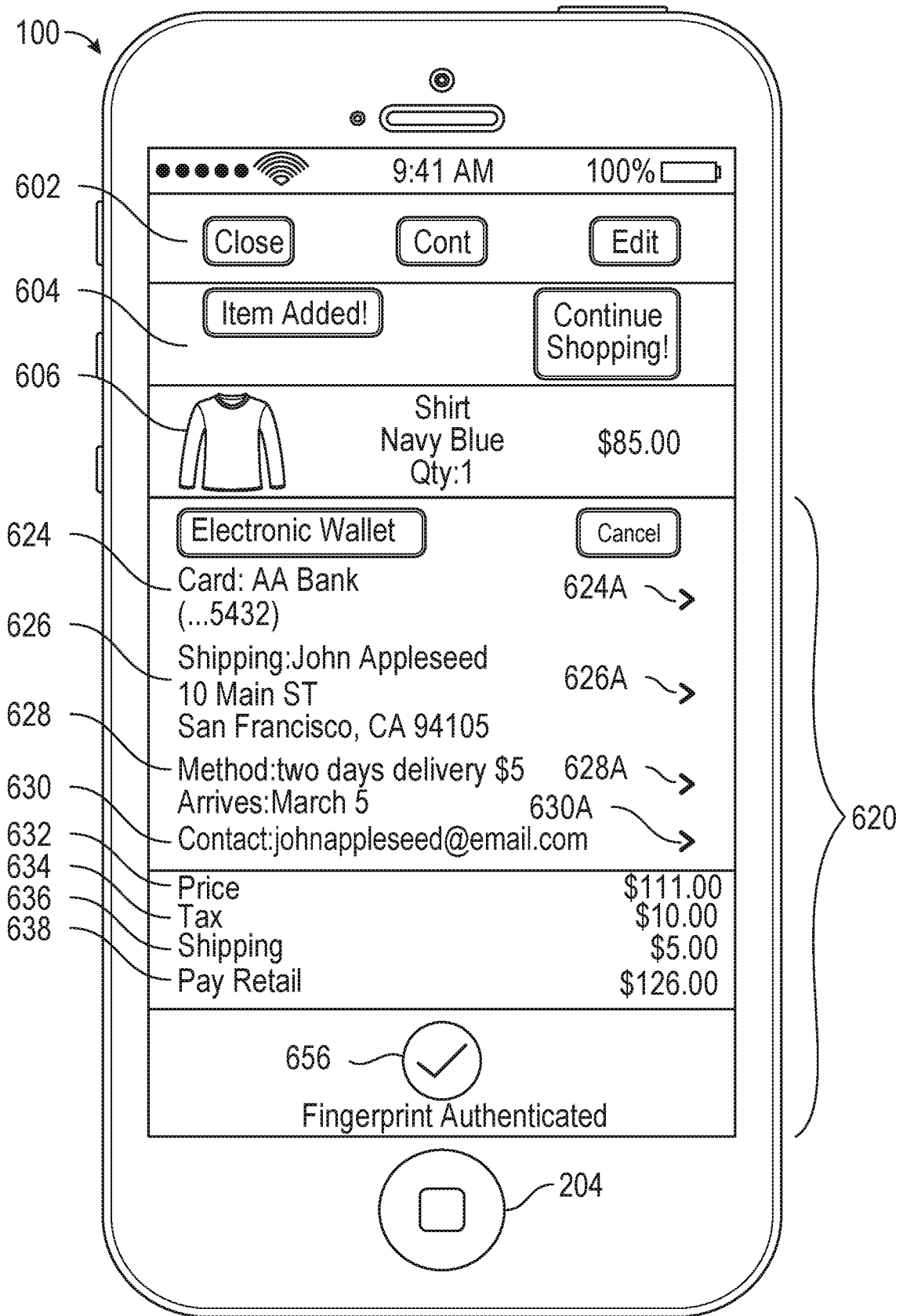


FIG. 6G

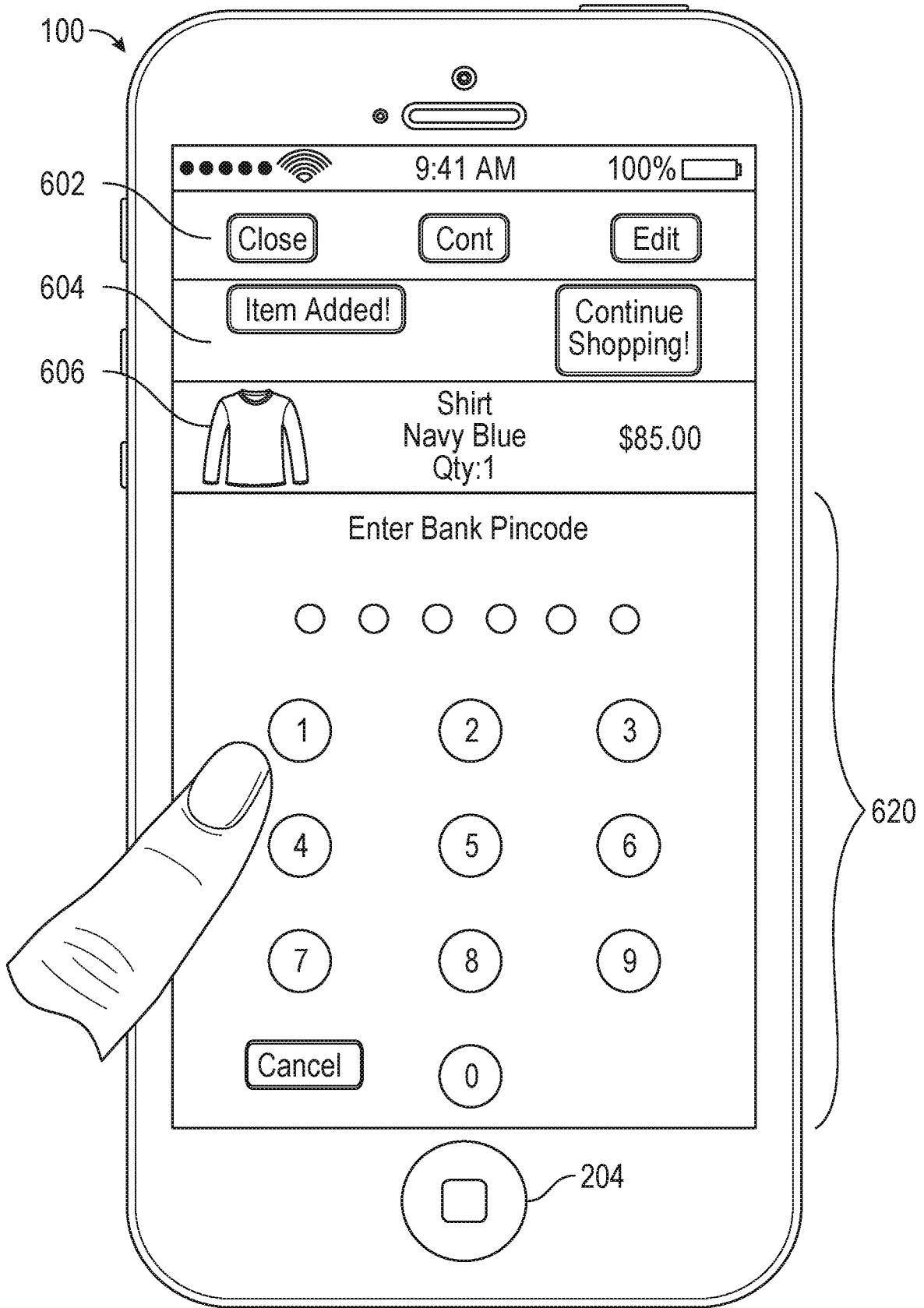


FIG. 6H

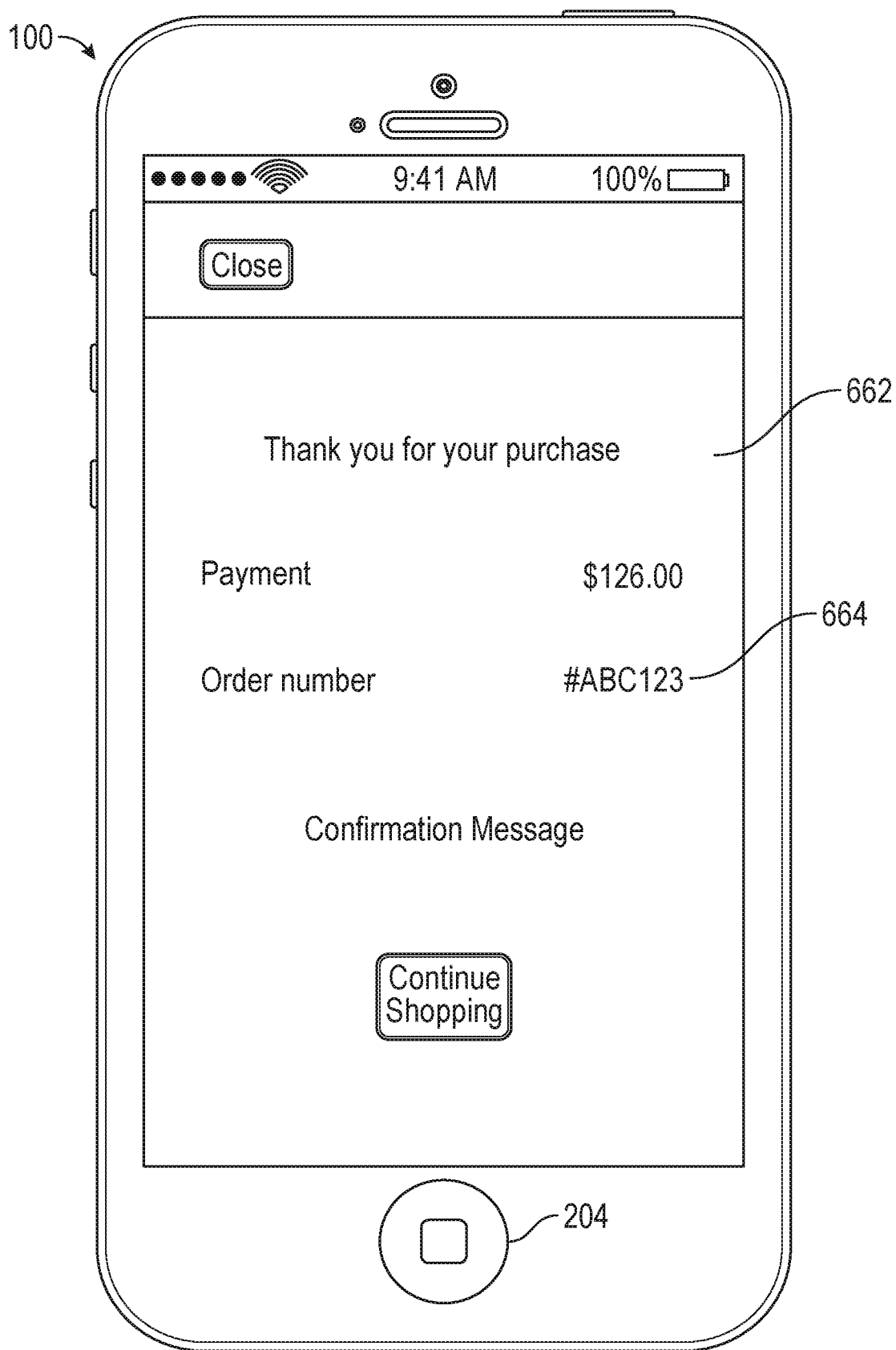


FIG. 6I

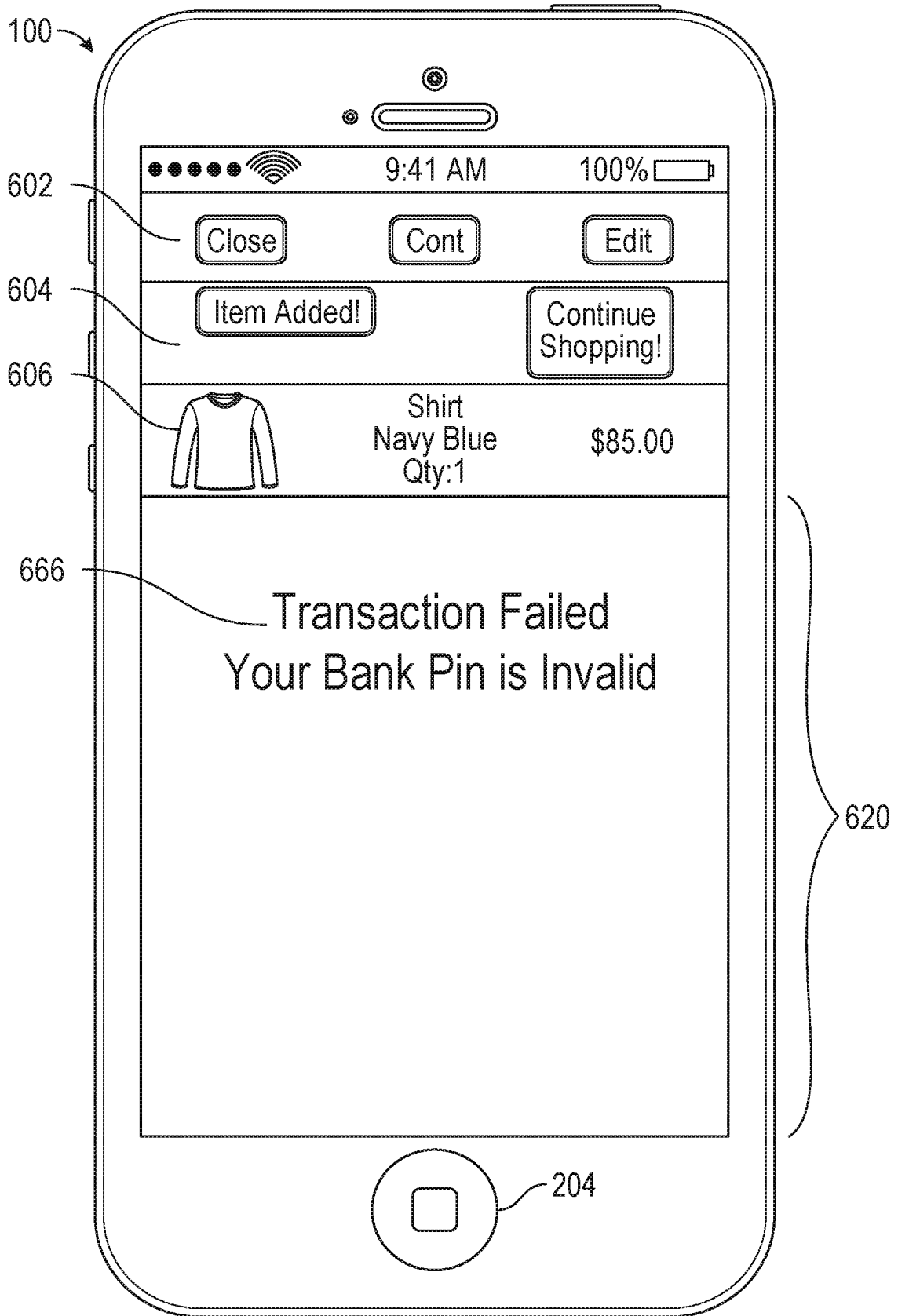


FIG. 6J



FIG. 6K

2016102031 24 Nov 2016

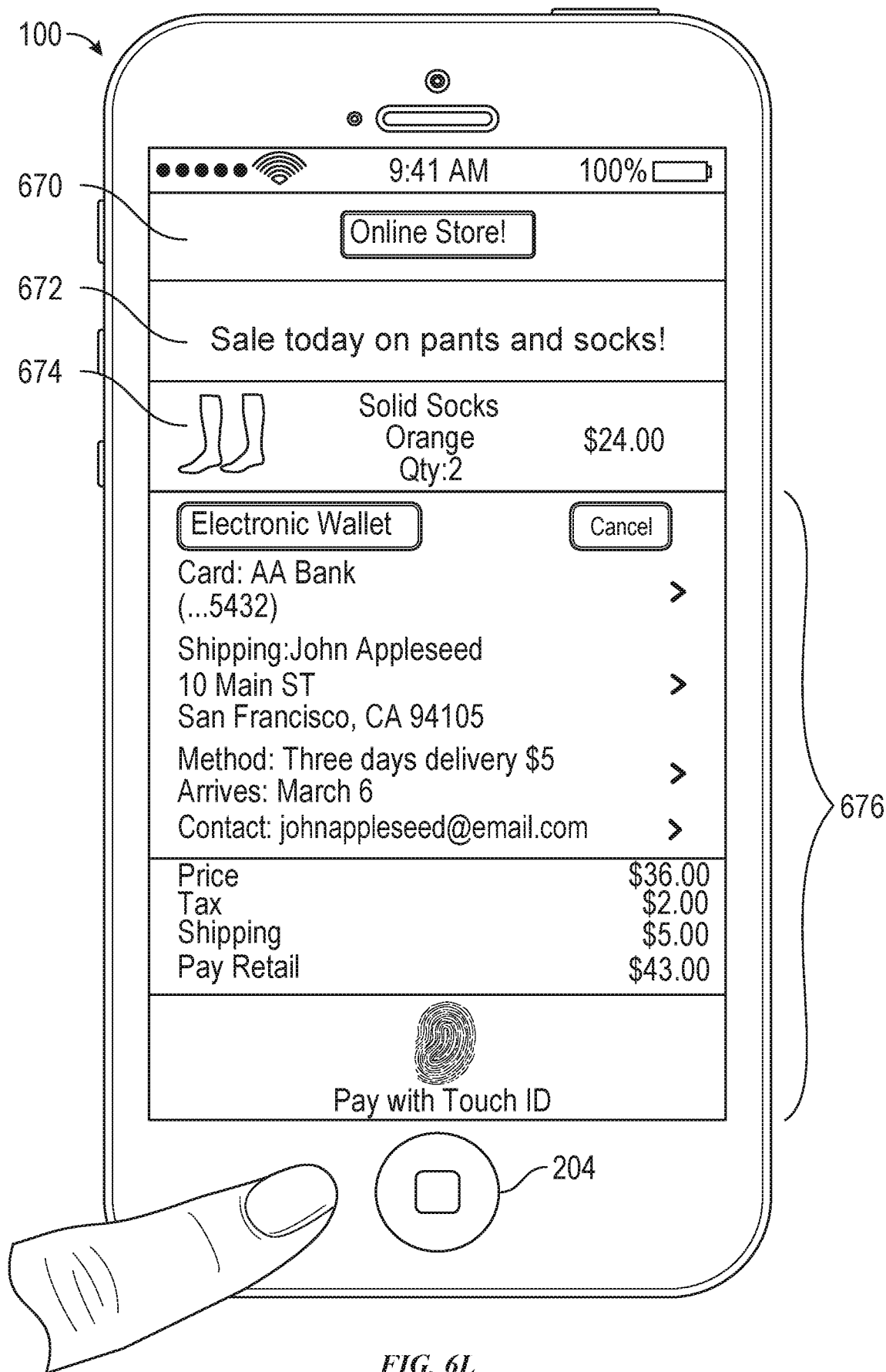


FIG. 6L

2016102031 24 Nov 2016



FIG. 6M

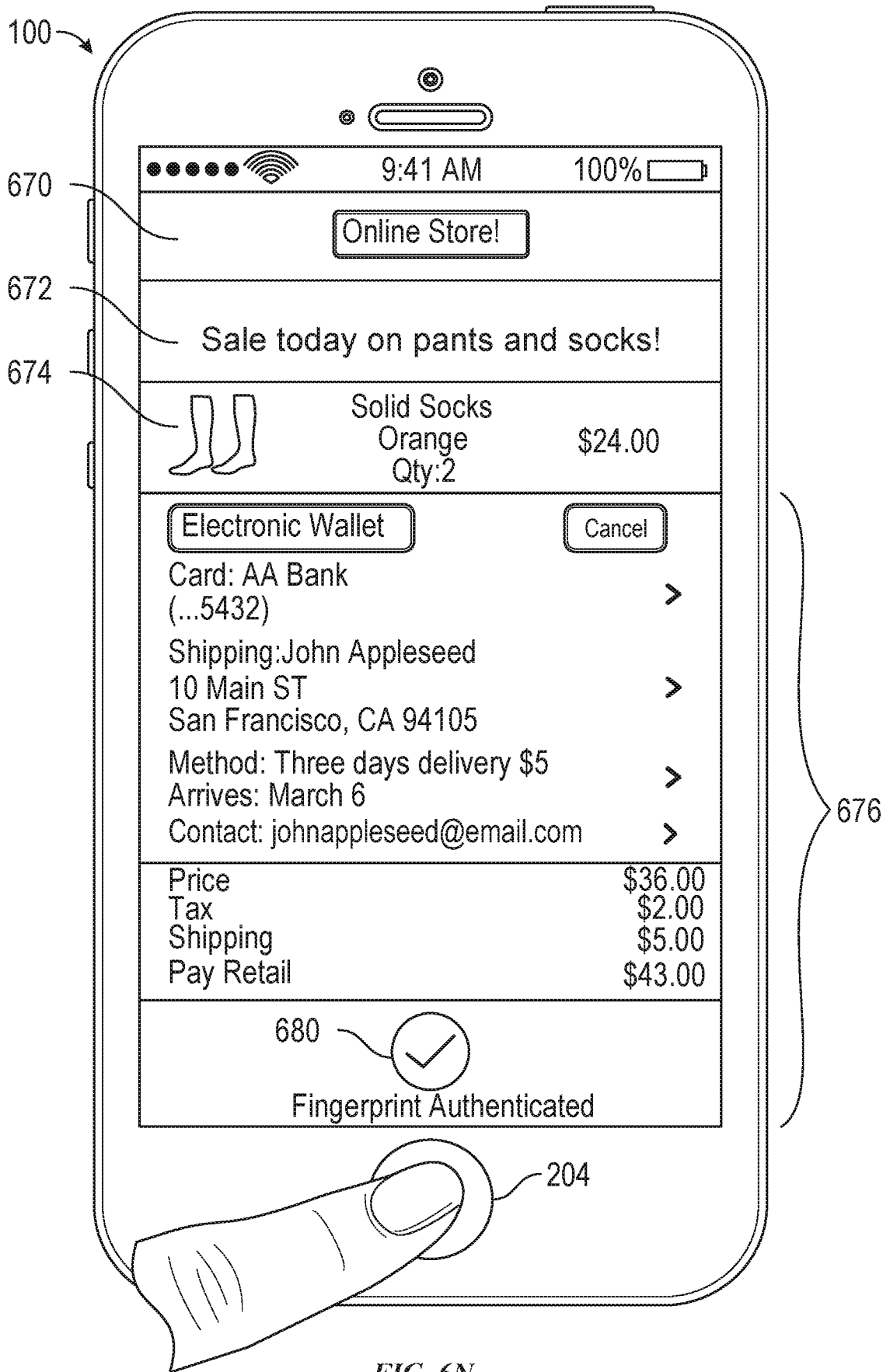


FIG. 6N

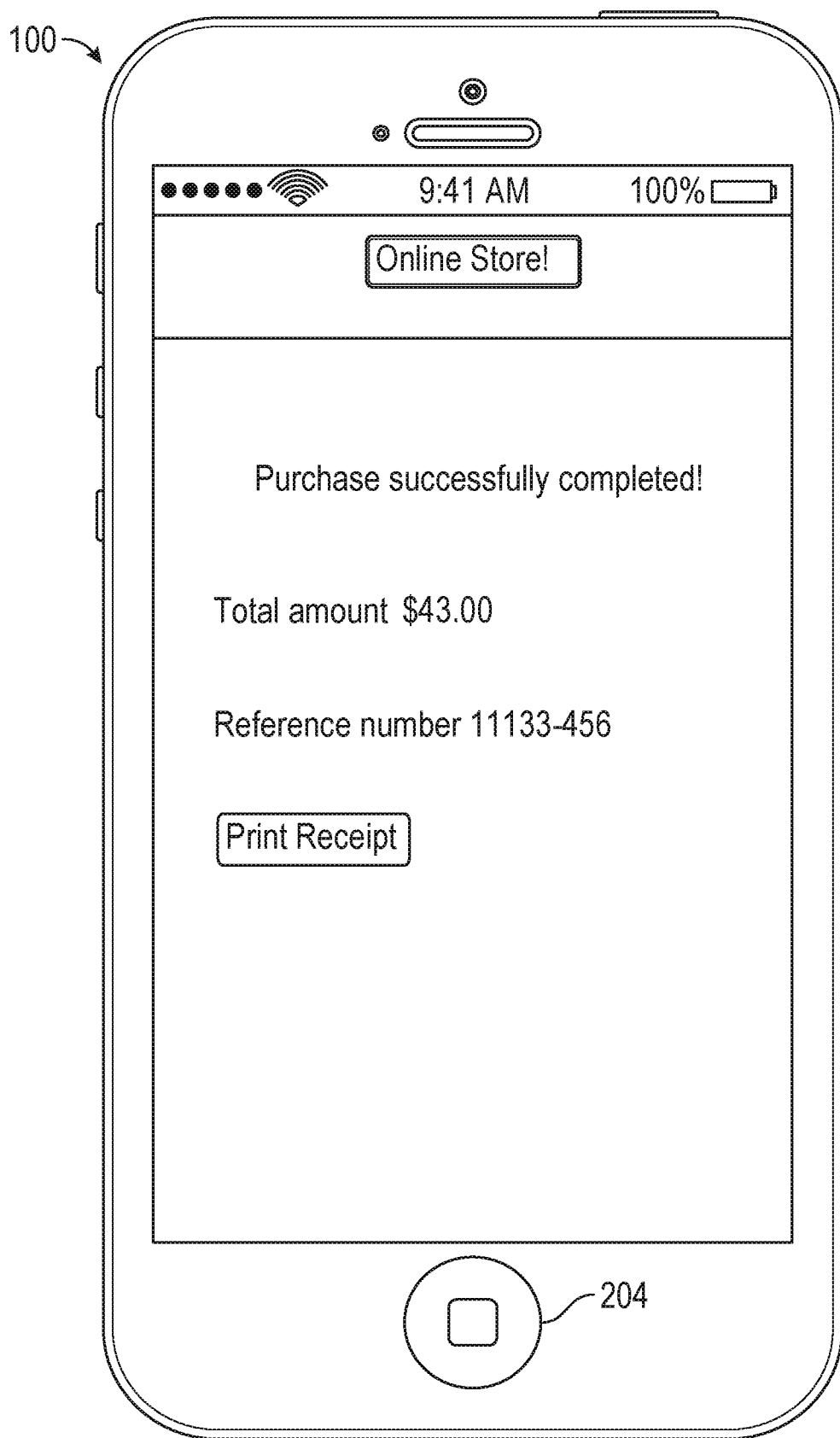
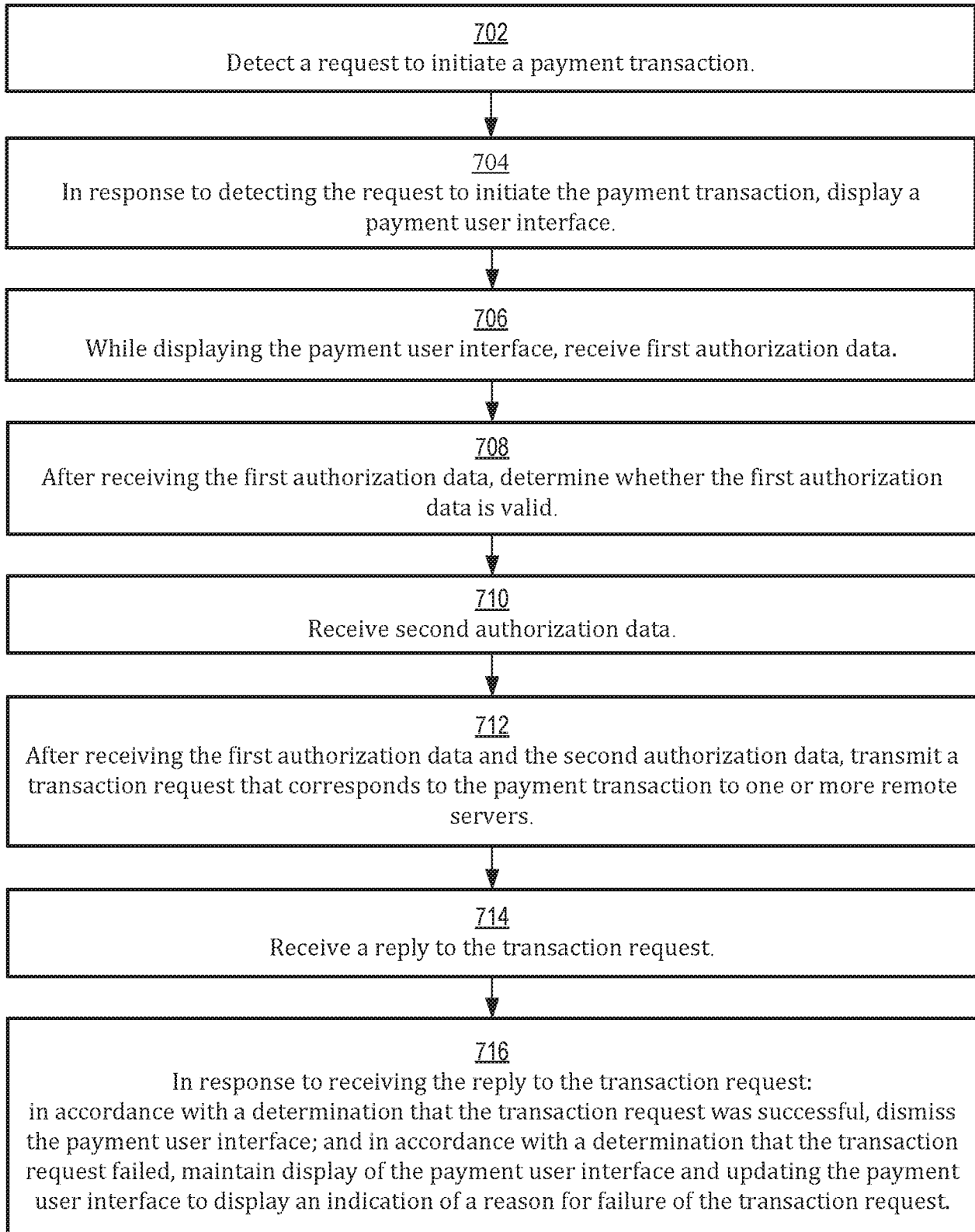


FIG. 60

700*FIG. 7*

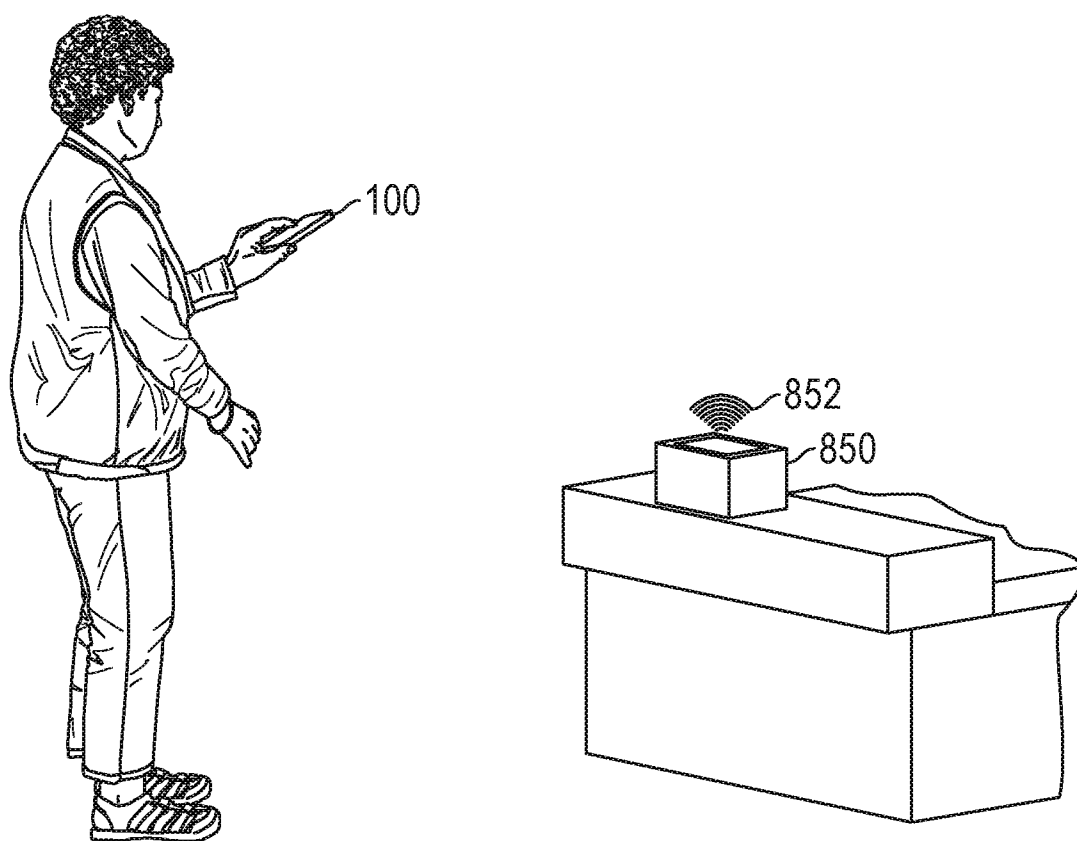


FIG. 8A

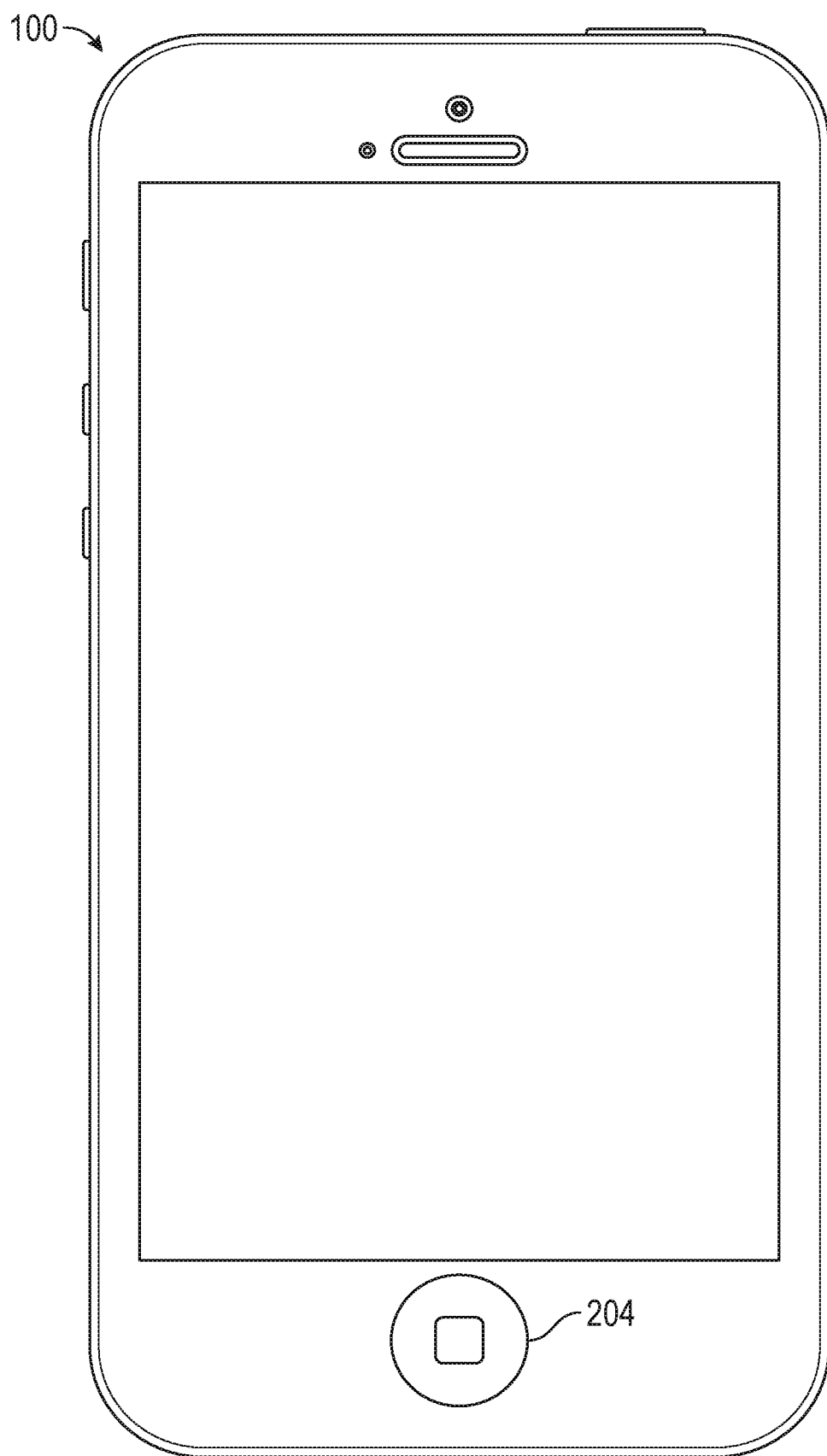
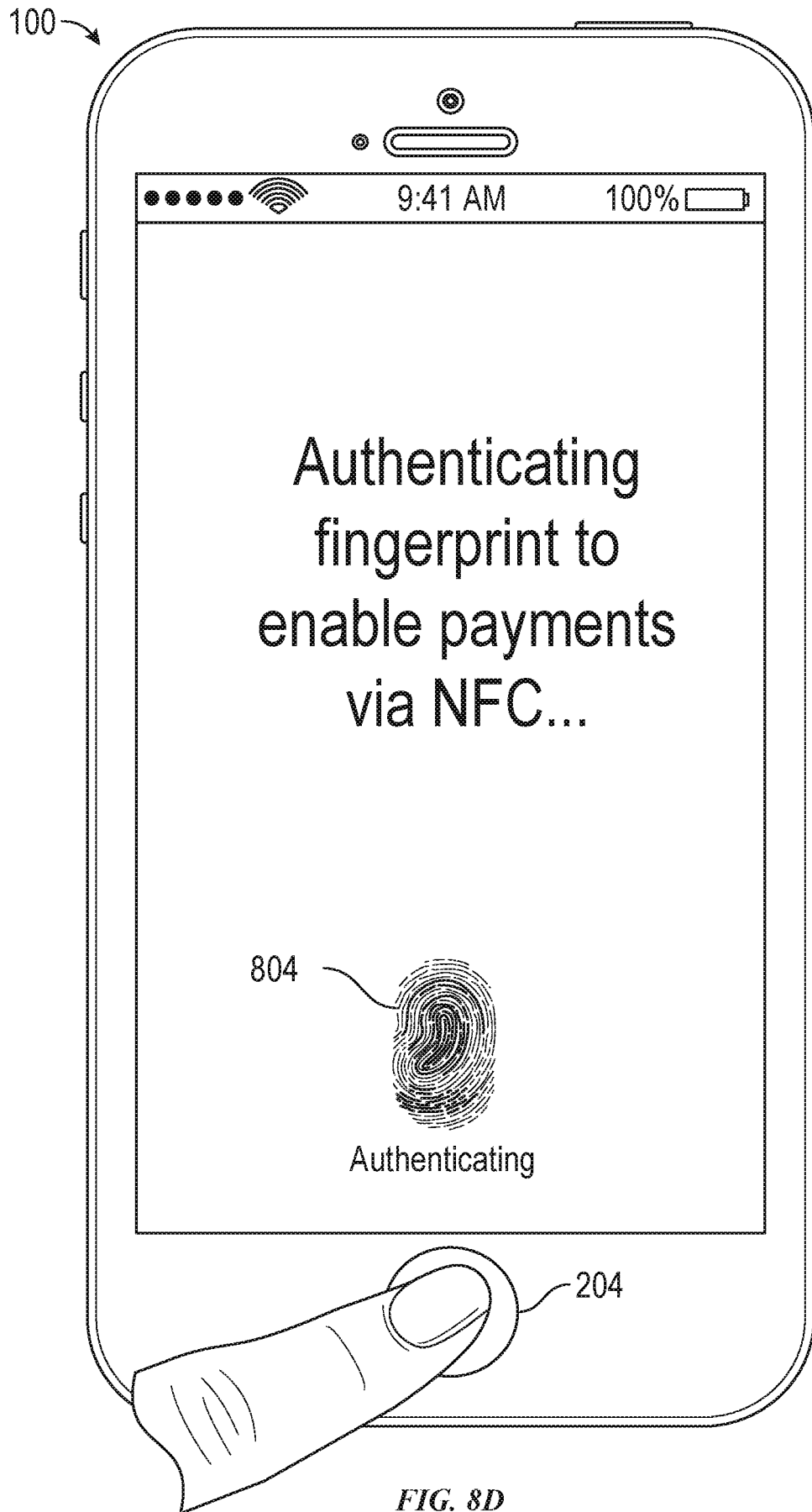


FIG. 8B



FIG. 8C



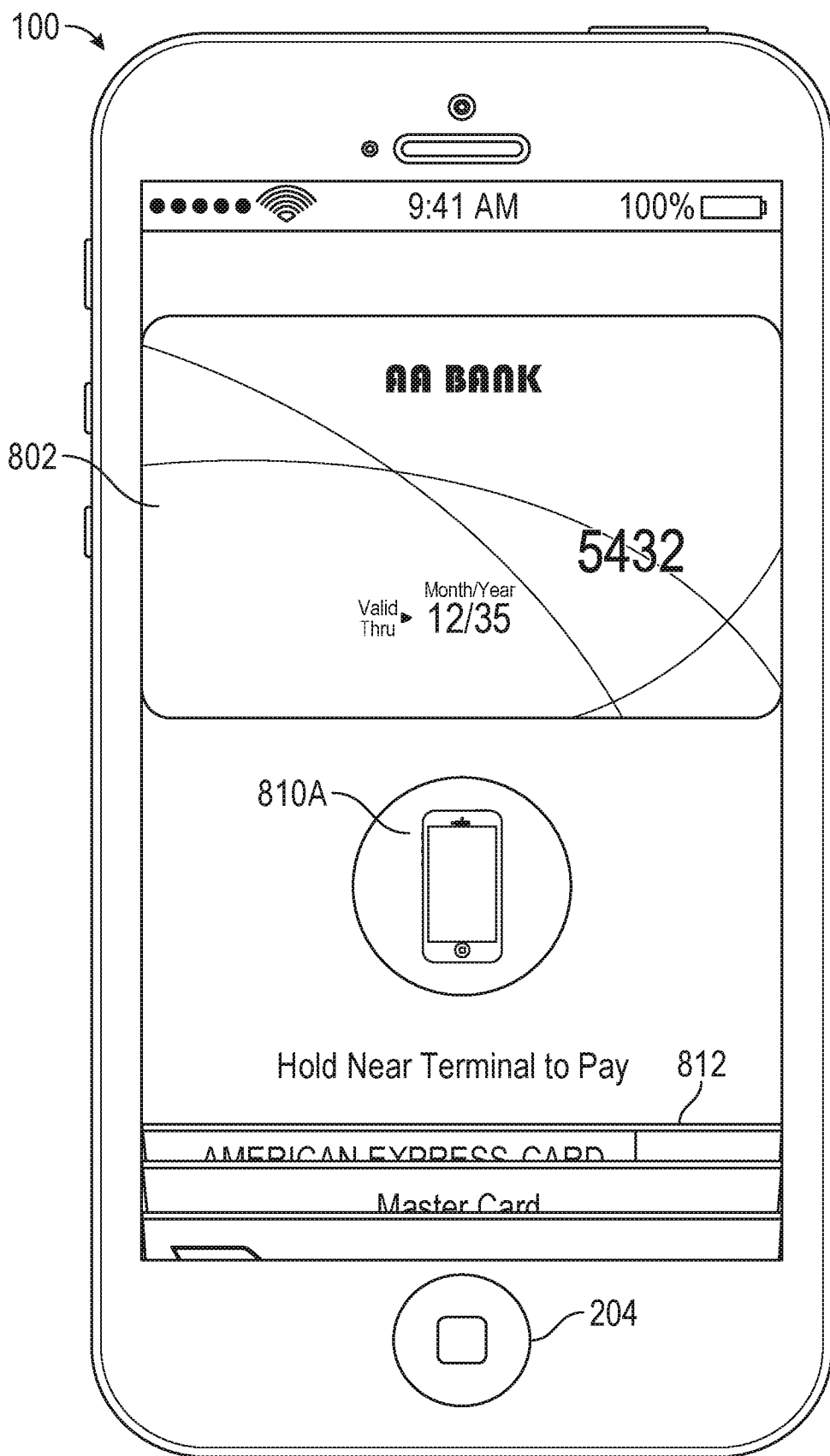


FIG. 8E

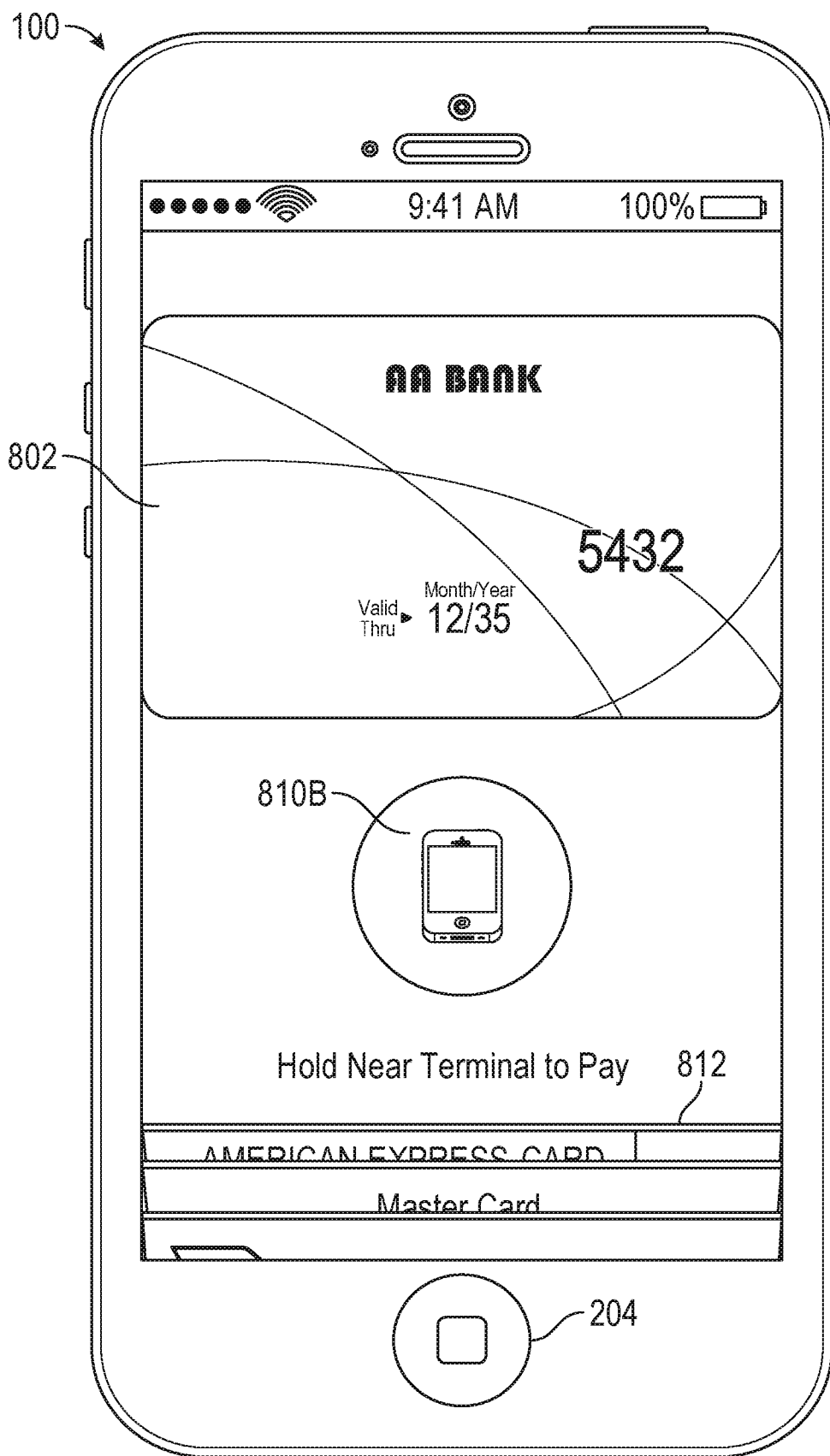


FIG. 8F

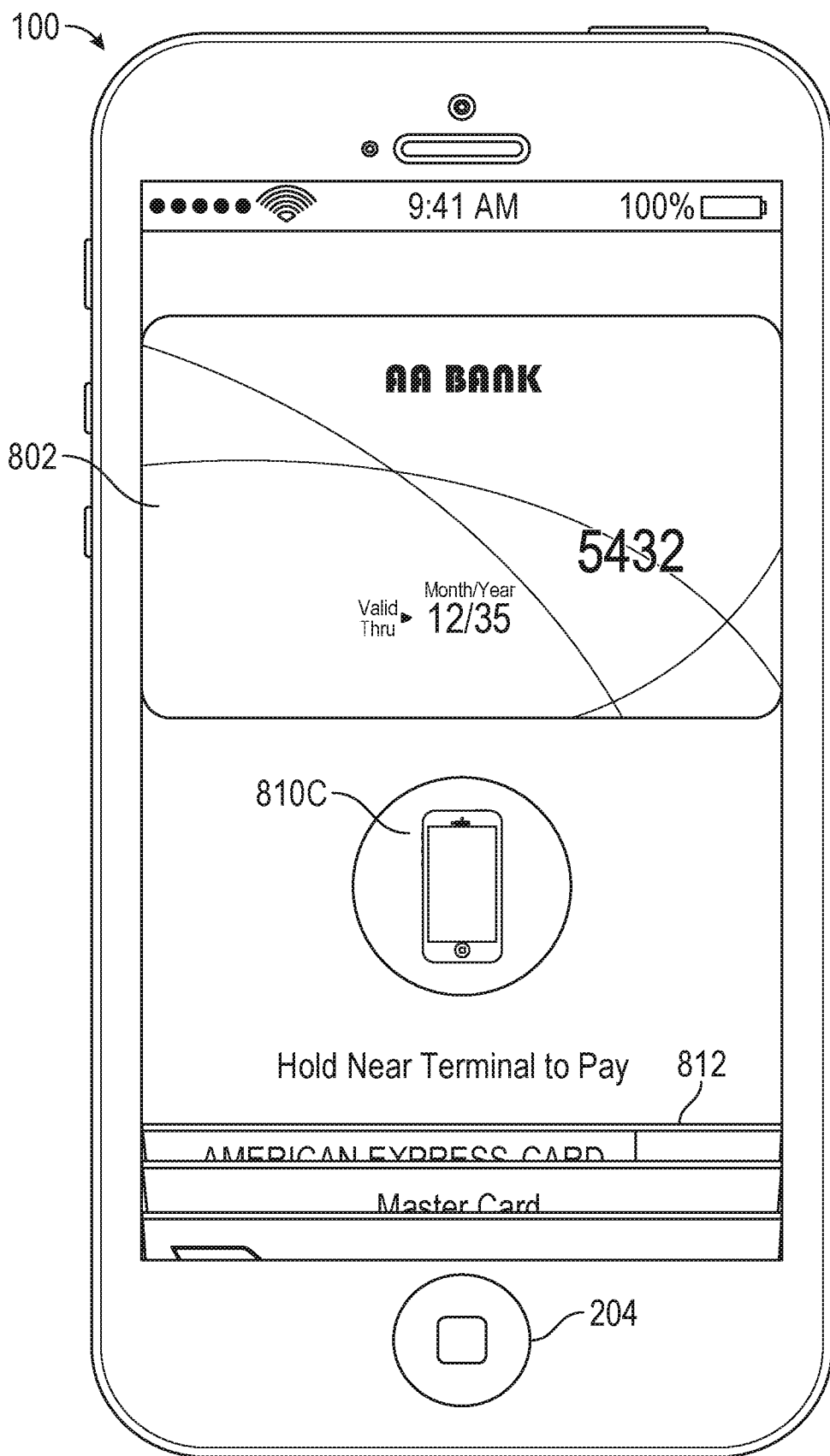


FIG. 8G

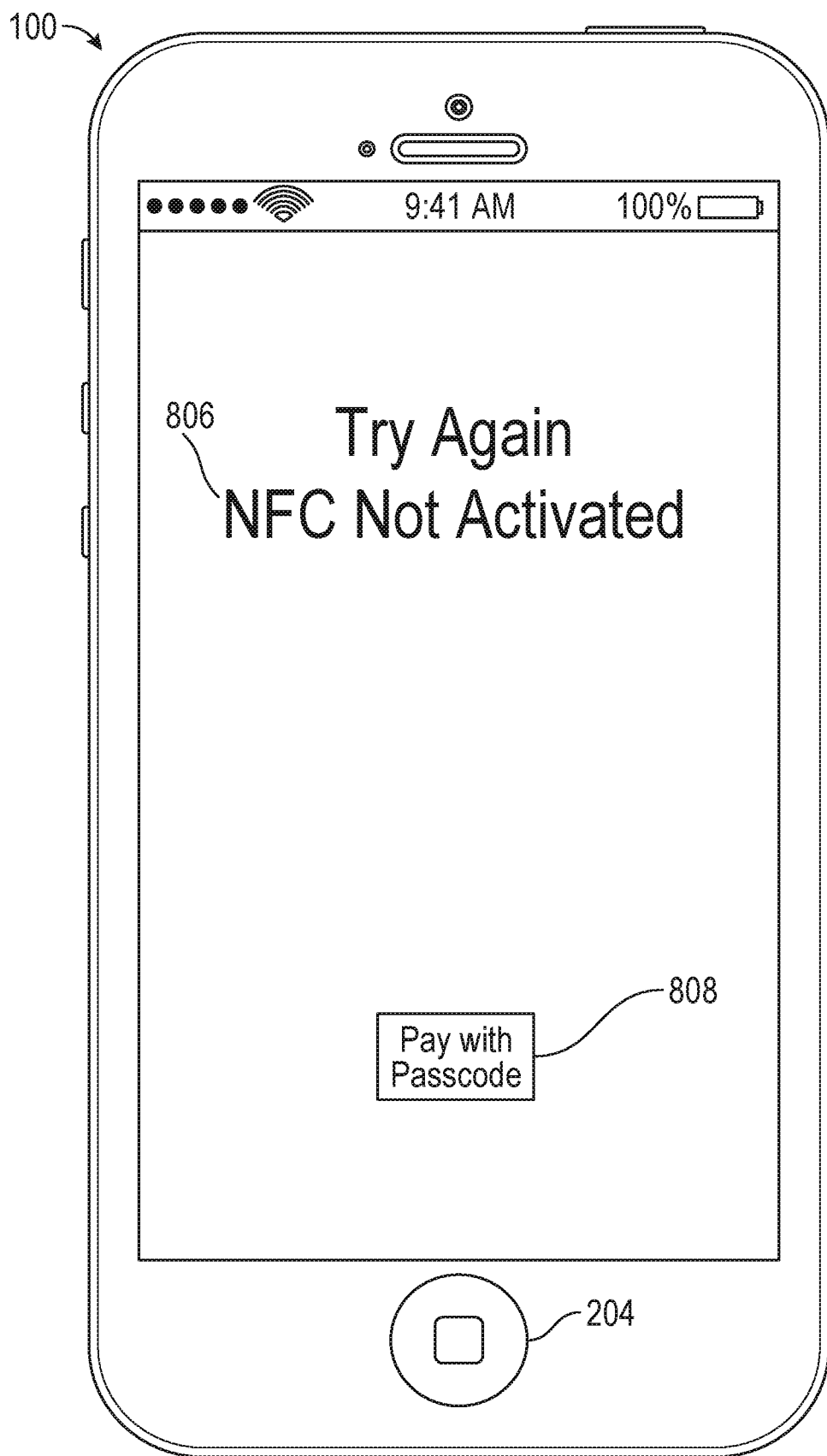


FIG. 8H

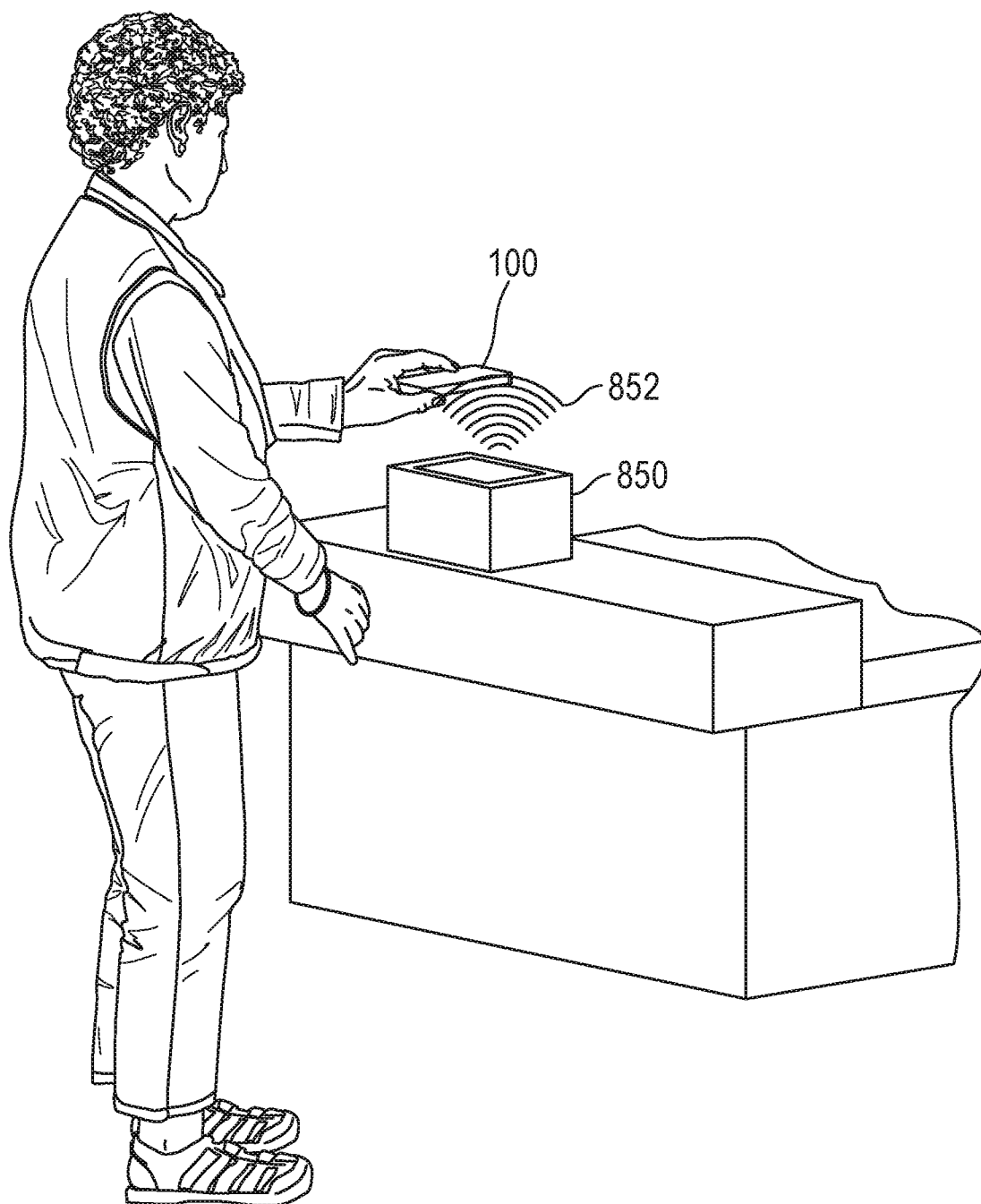


FIG. 8I

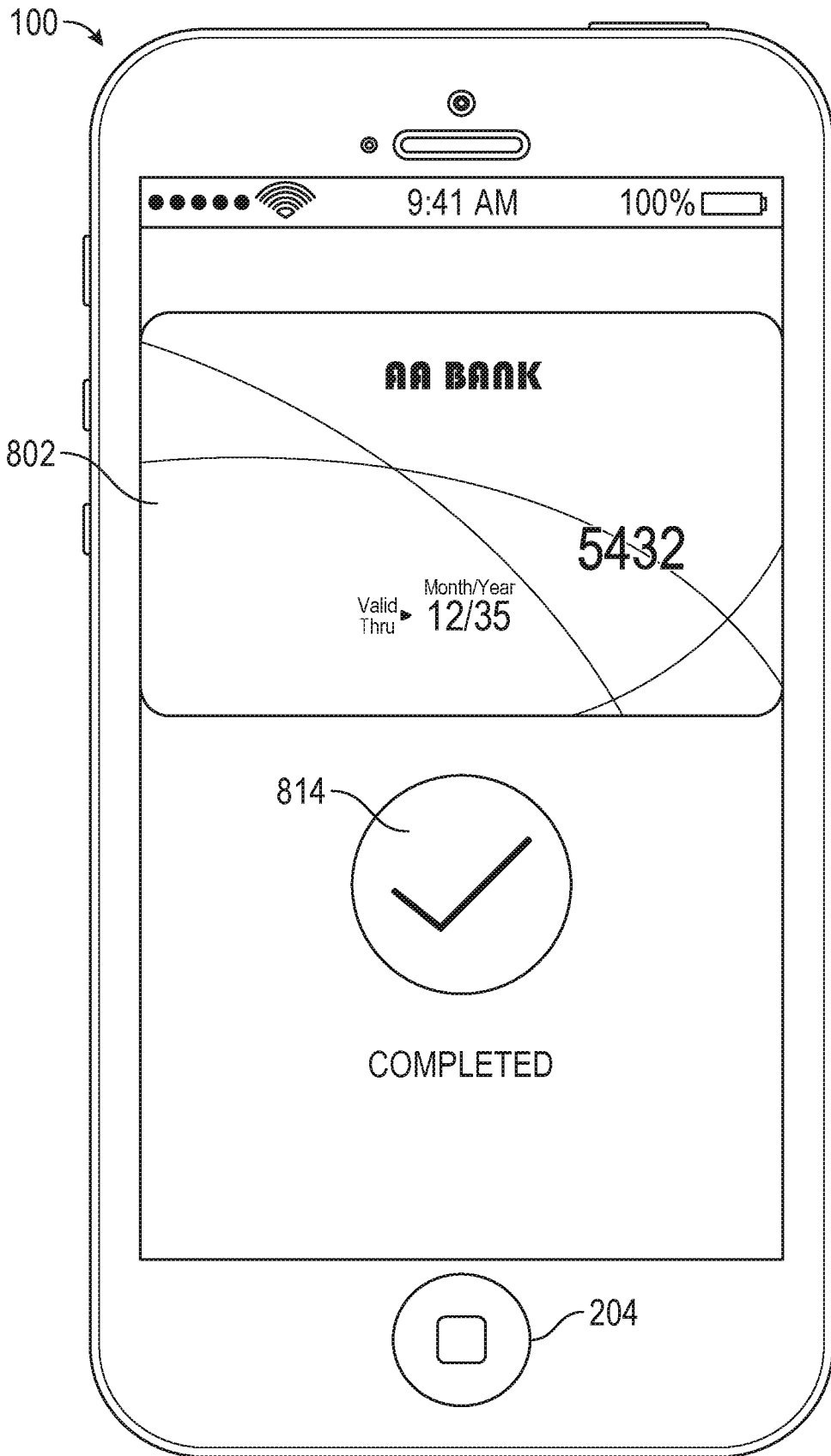


FIG. 8J

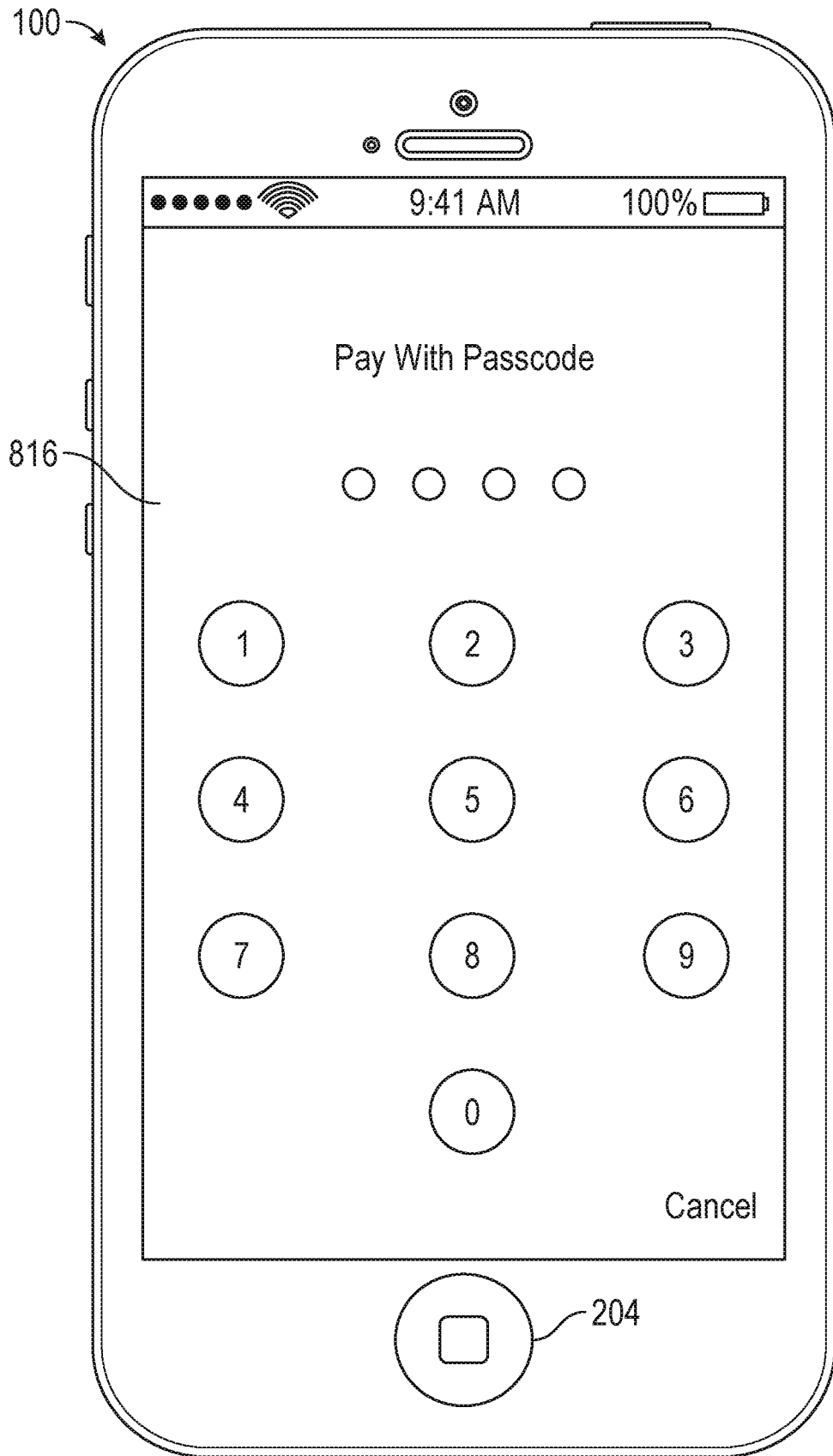


FIG. 8K

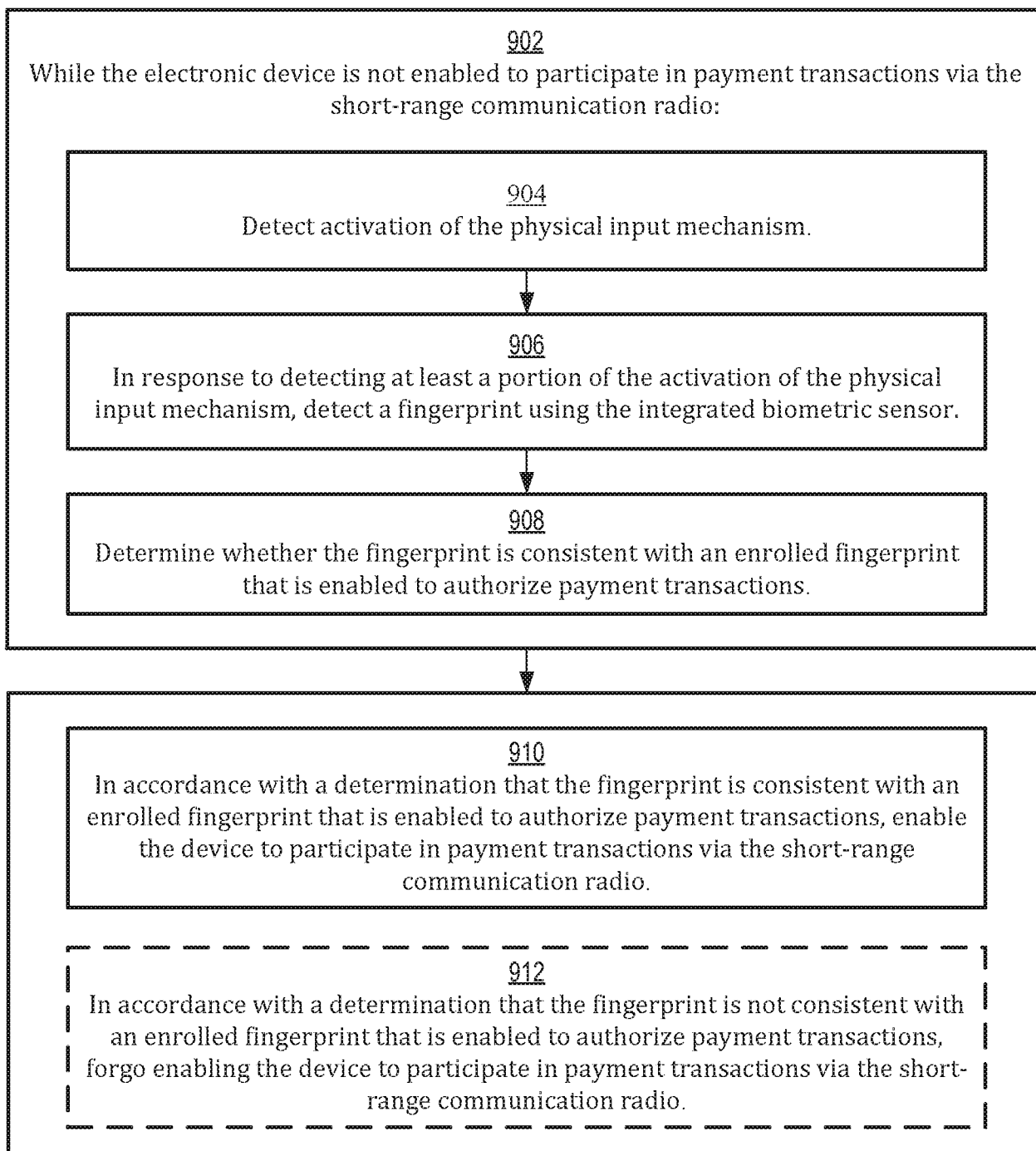


FIG. 9

2016102031 24 Nov 2016

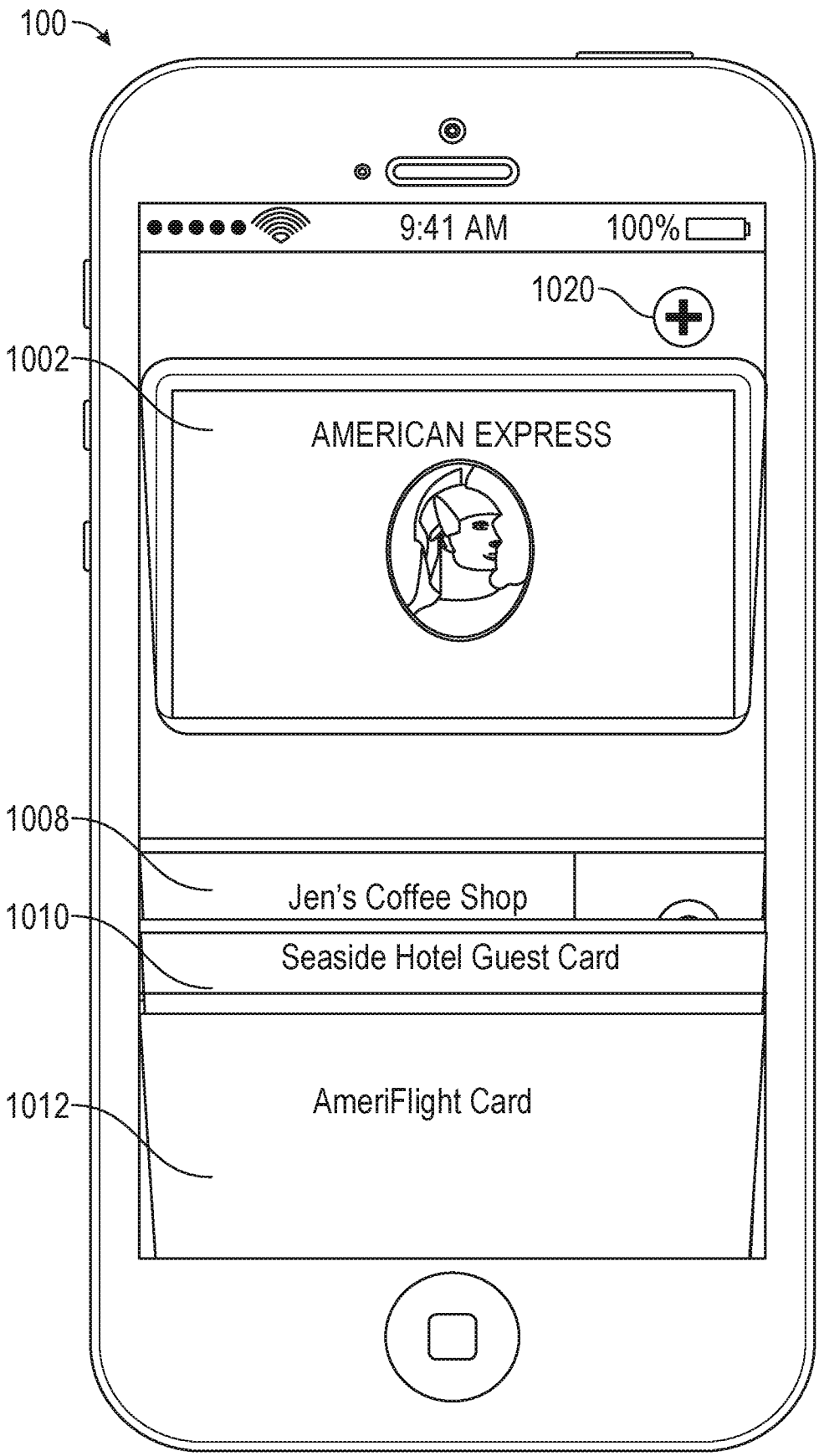


FIG. 10A

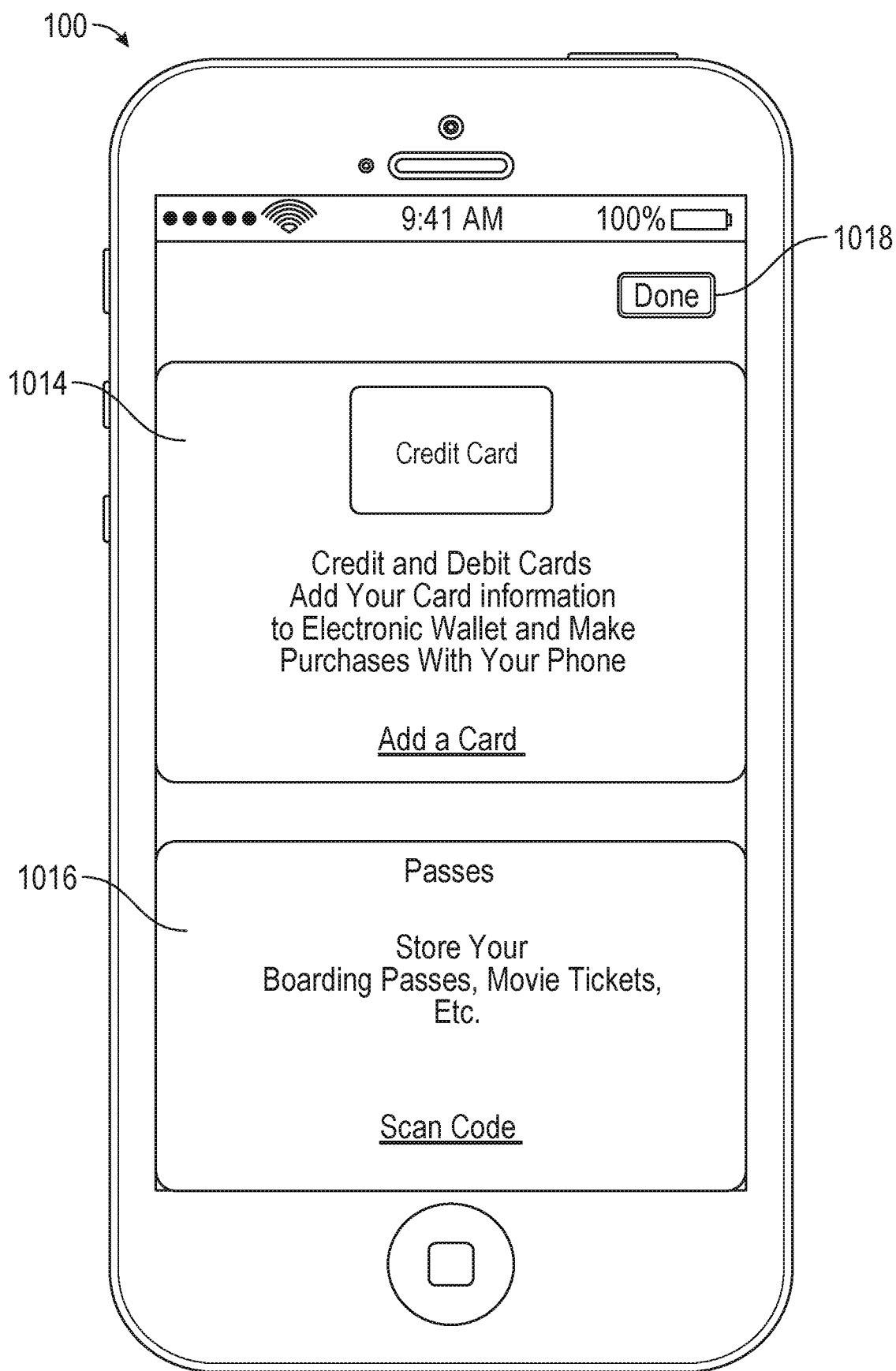


FIG. 10B

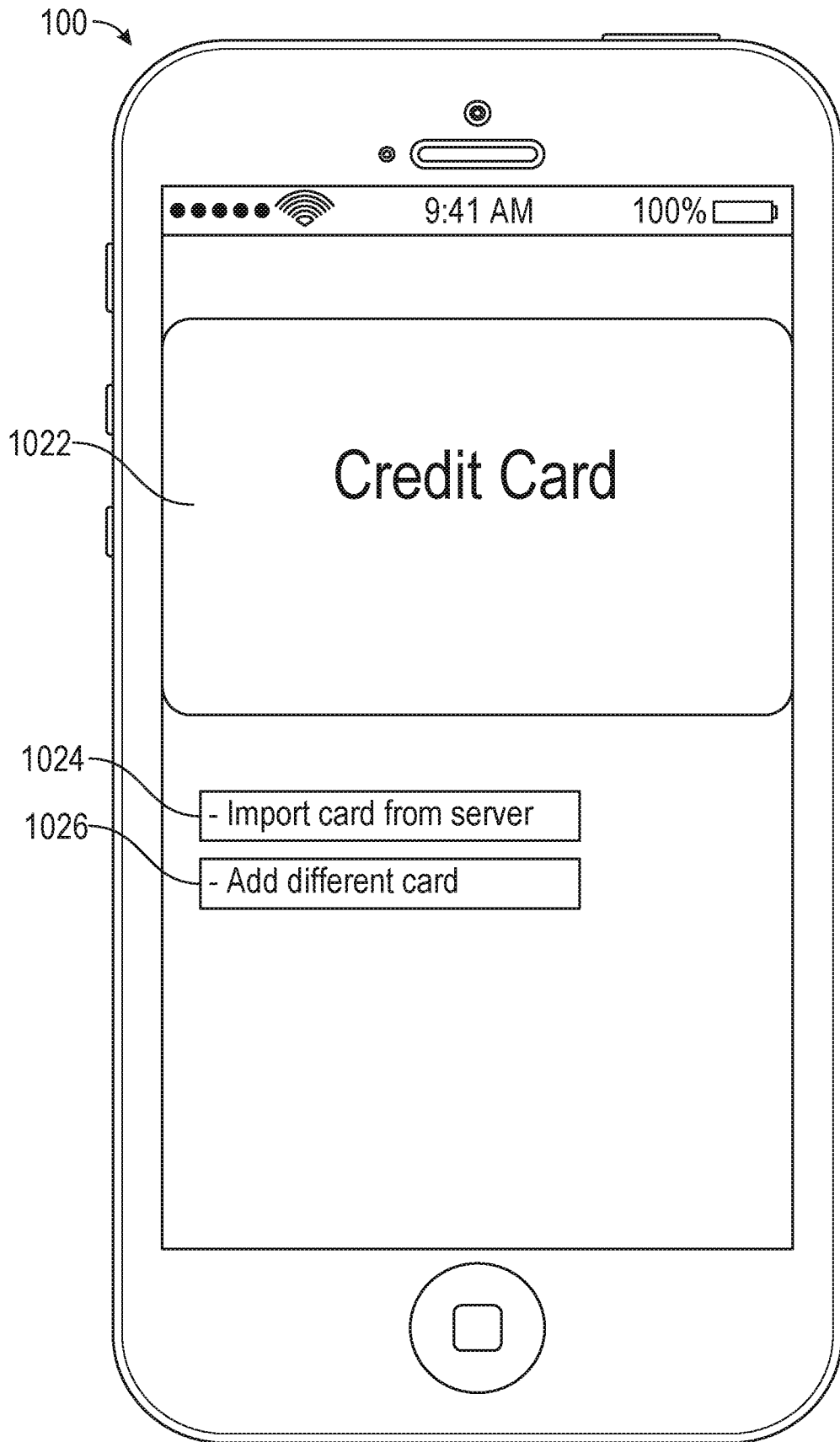


FIG. 10C

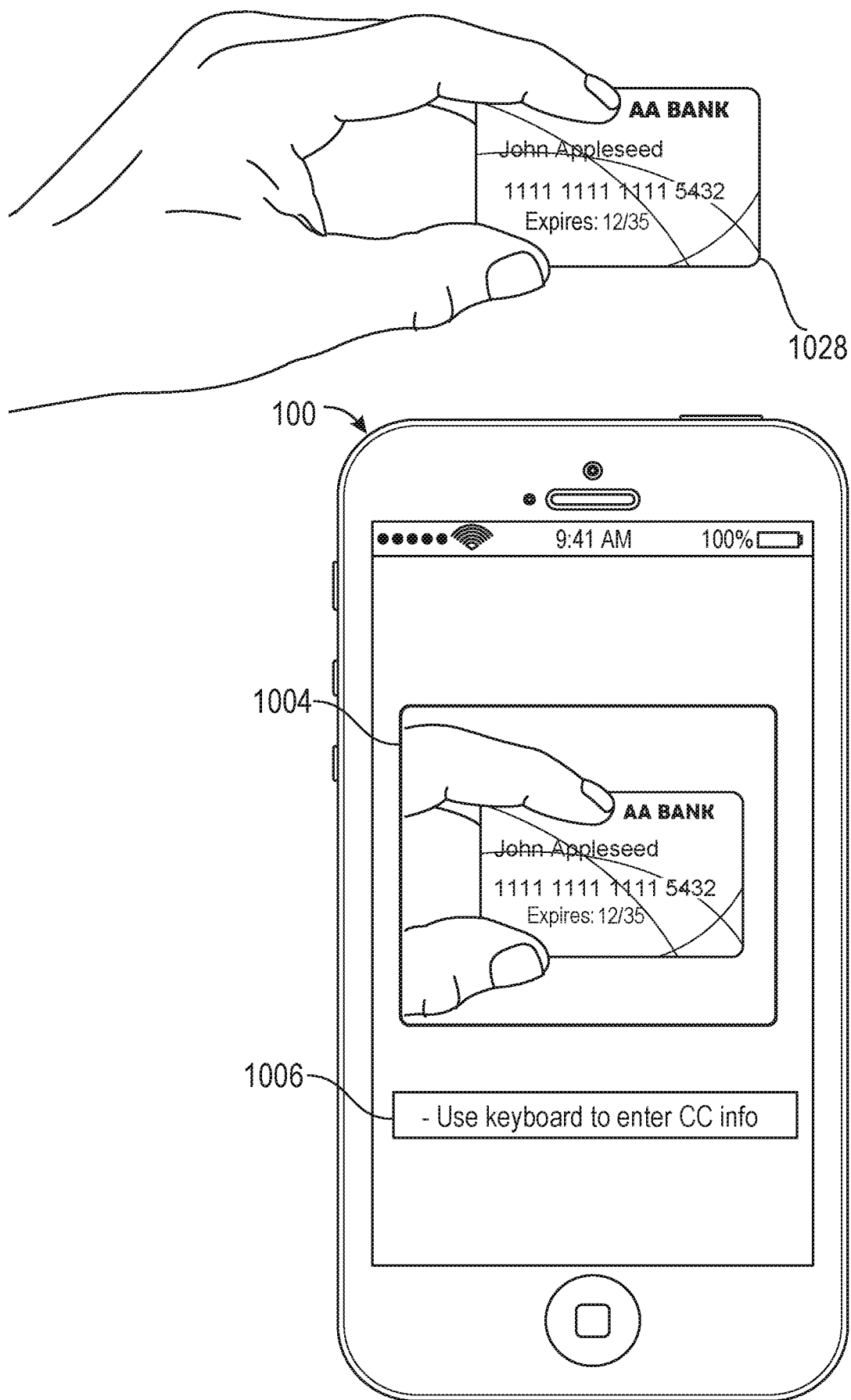


FIG. 10D

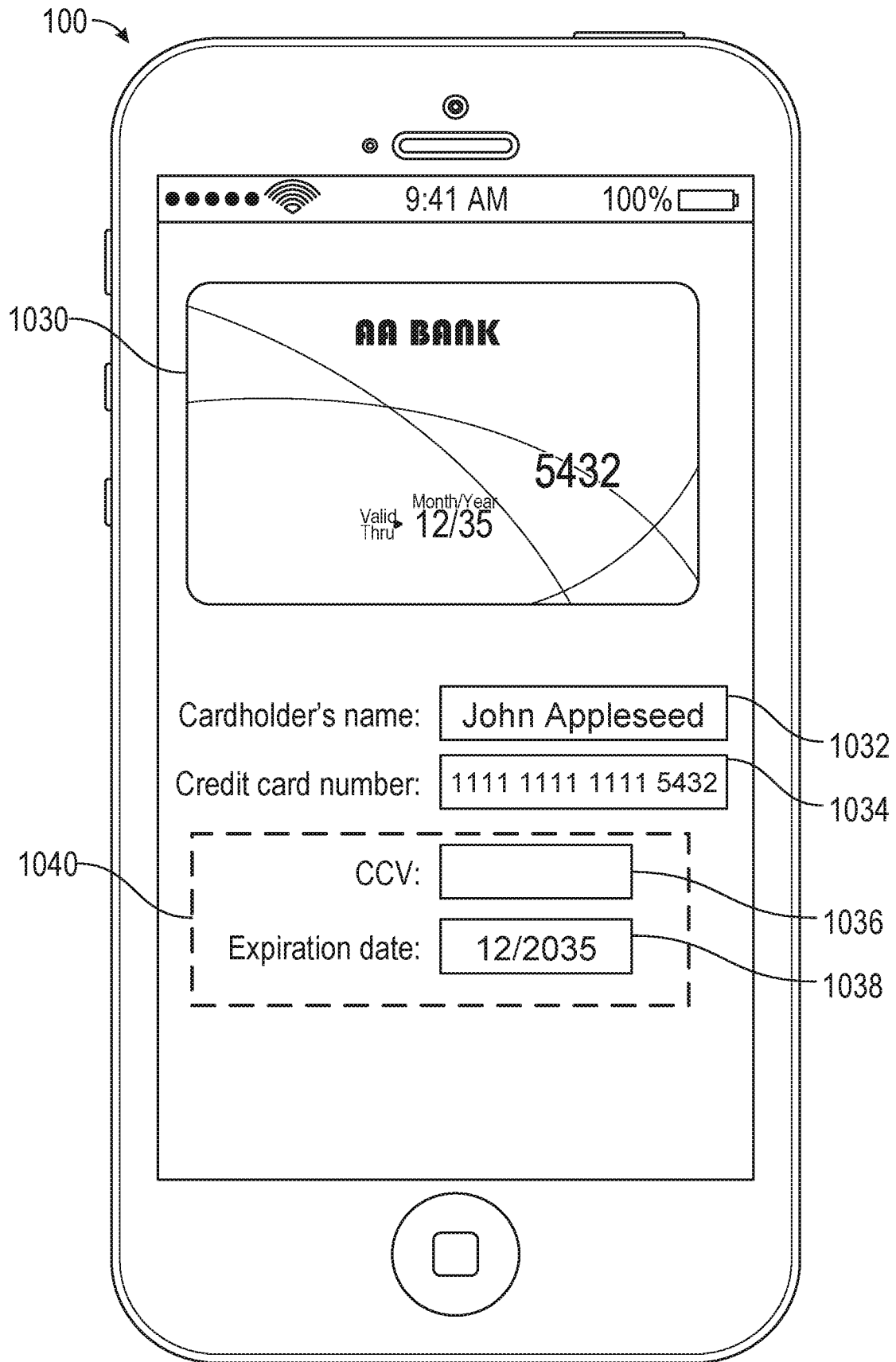


FIG. 10E

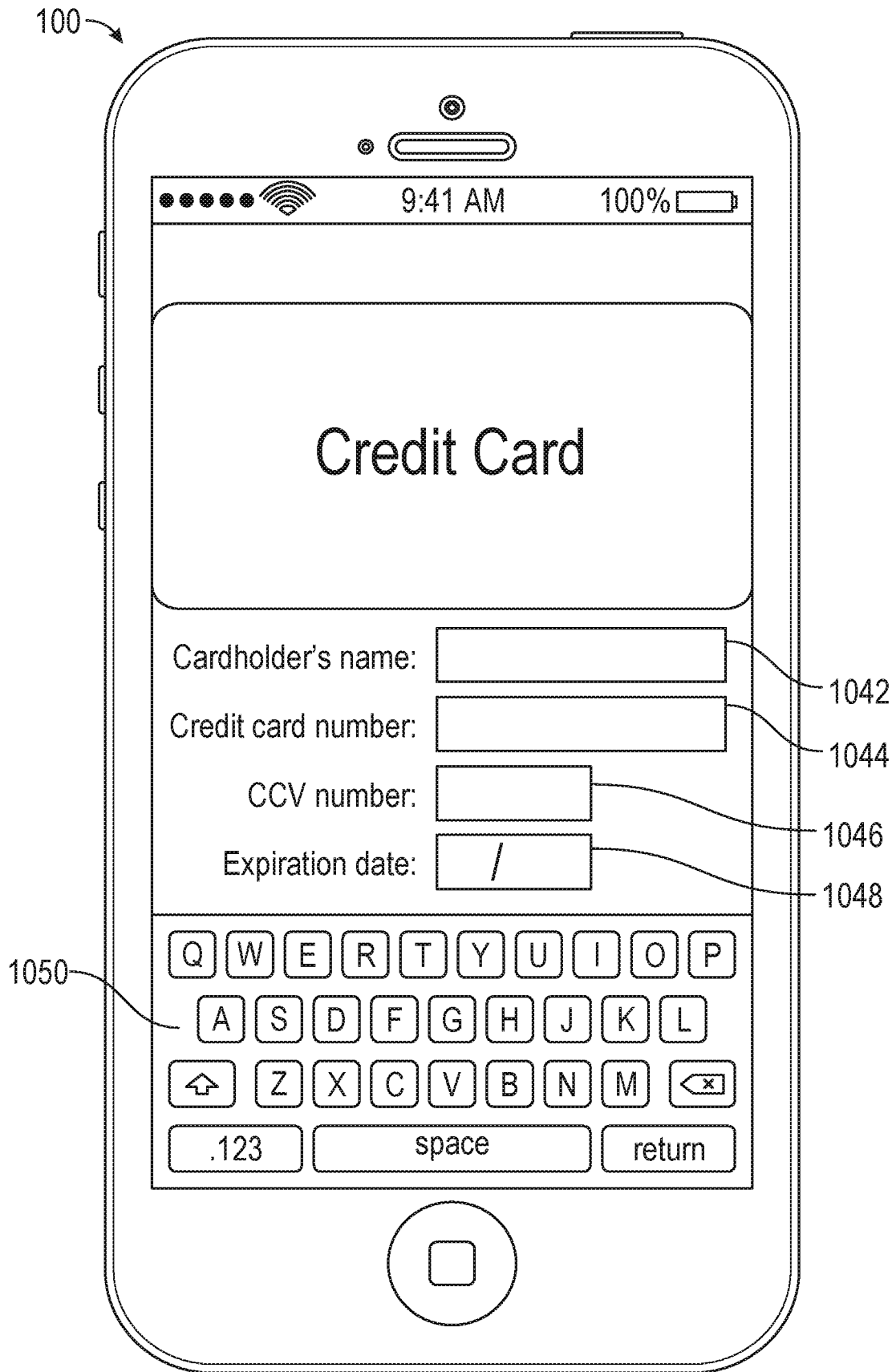


FIG. 10F

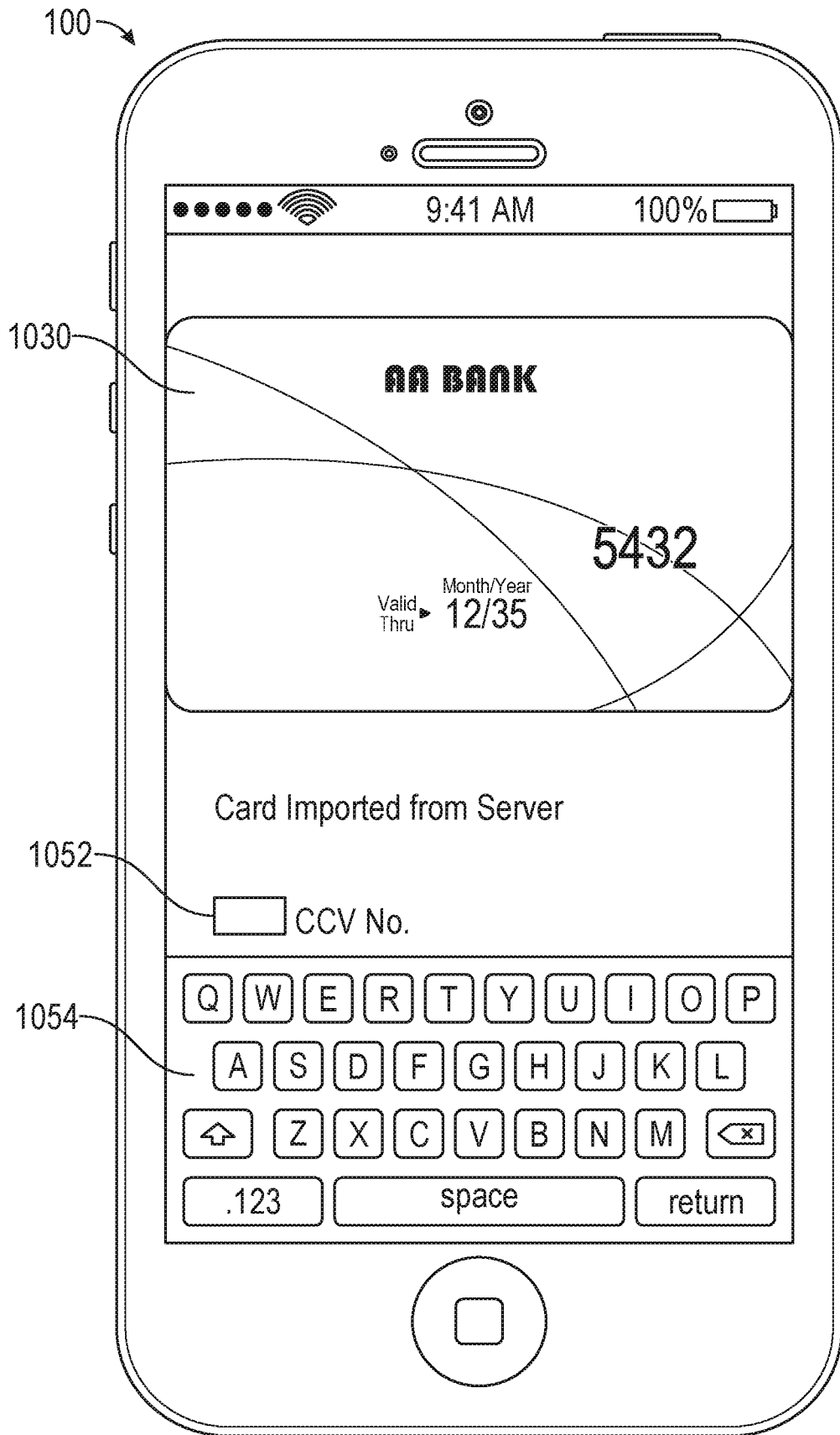


FIG. 10G

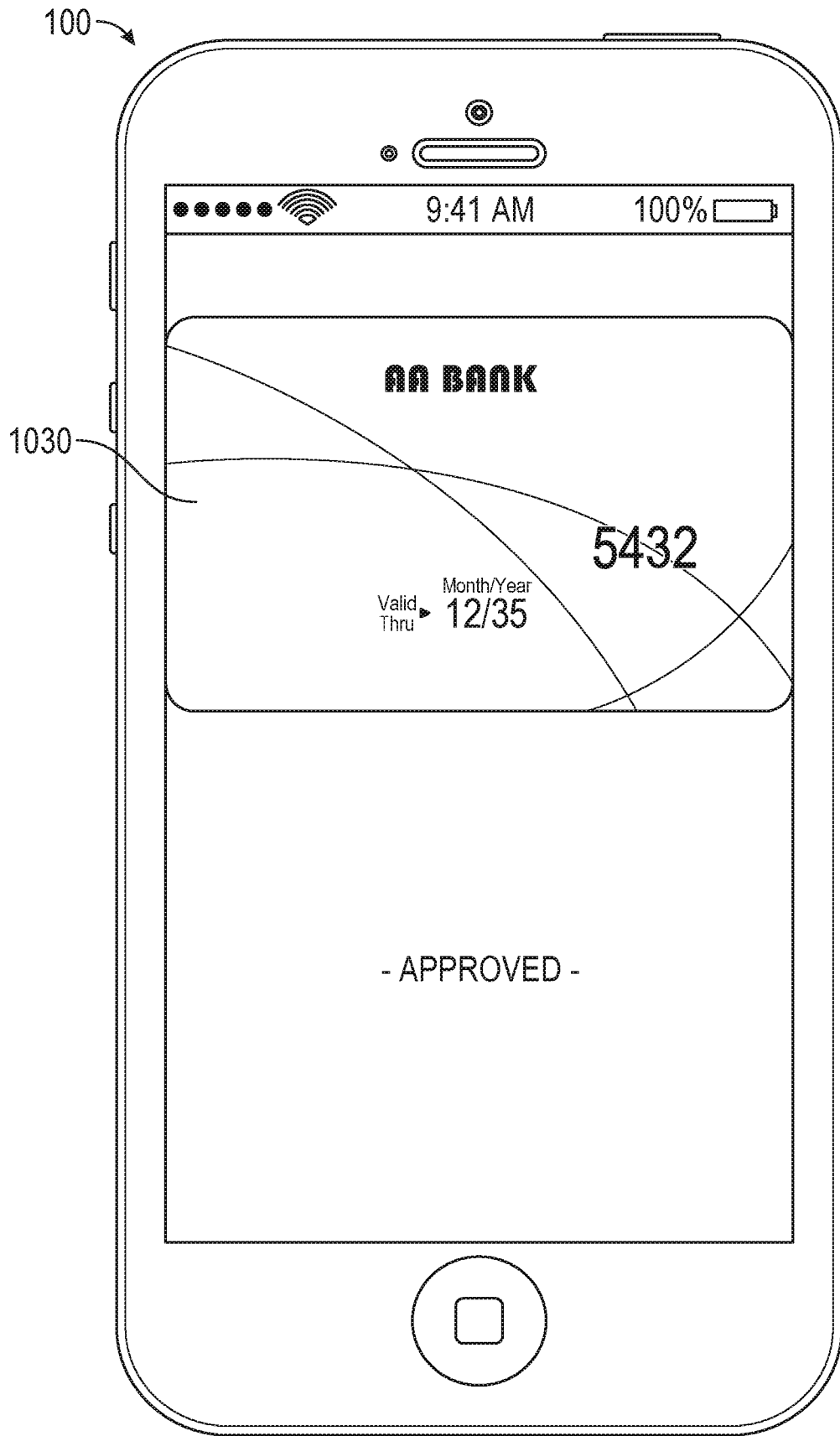


FIG. 10H

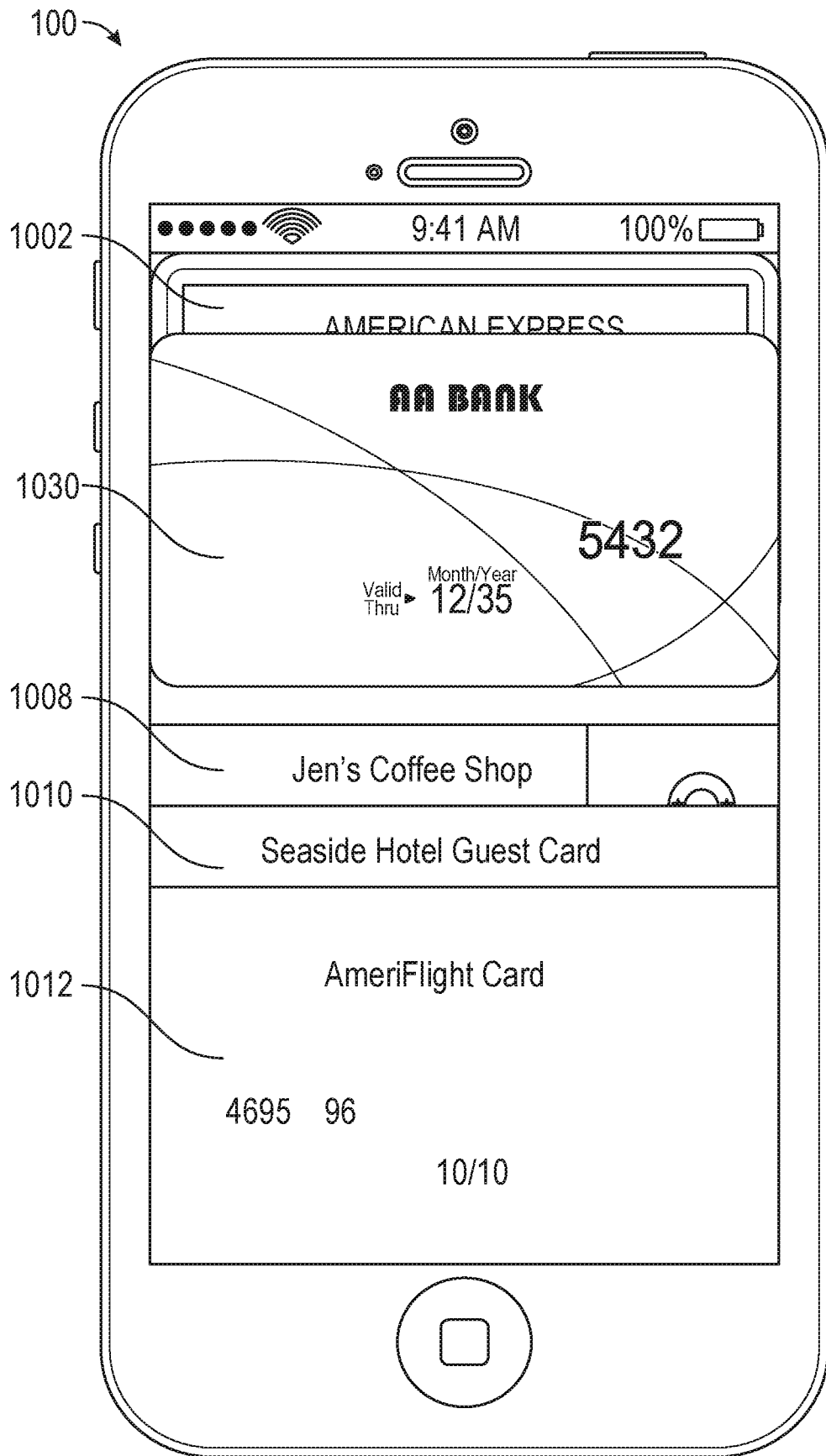
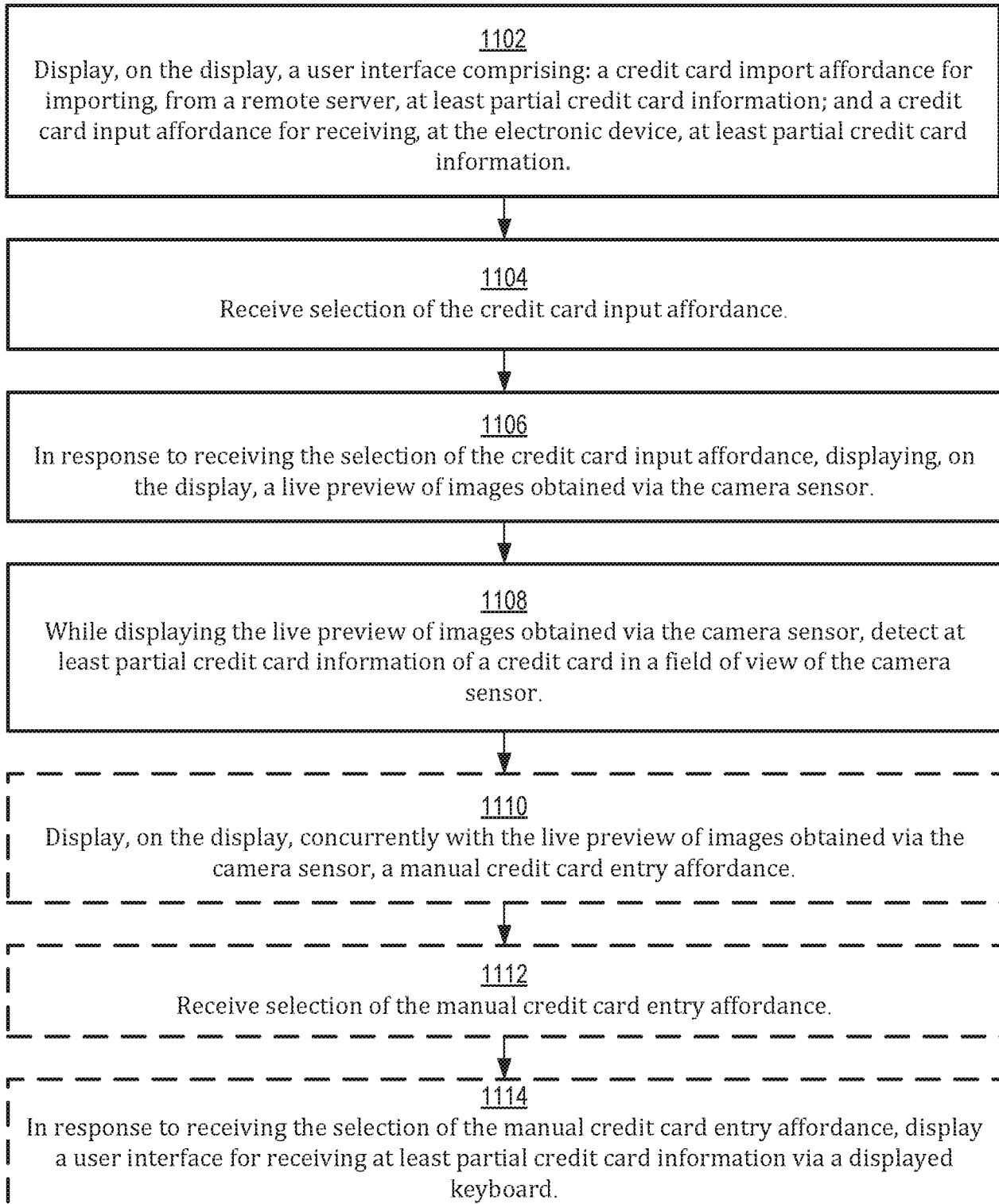


FIG. 101

1100*FIG. 11*

2016102031 24 Nov 2016

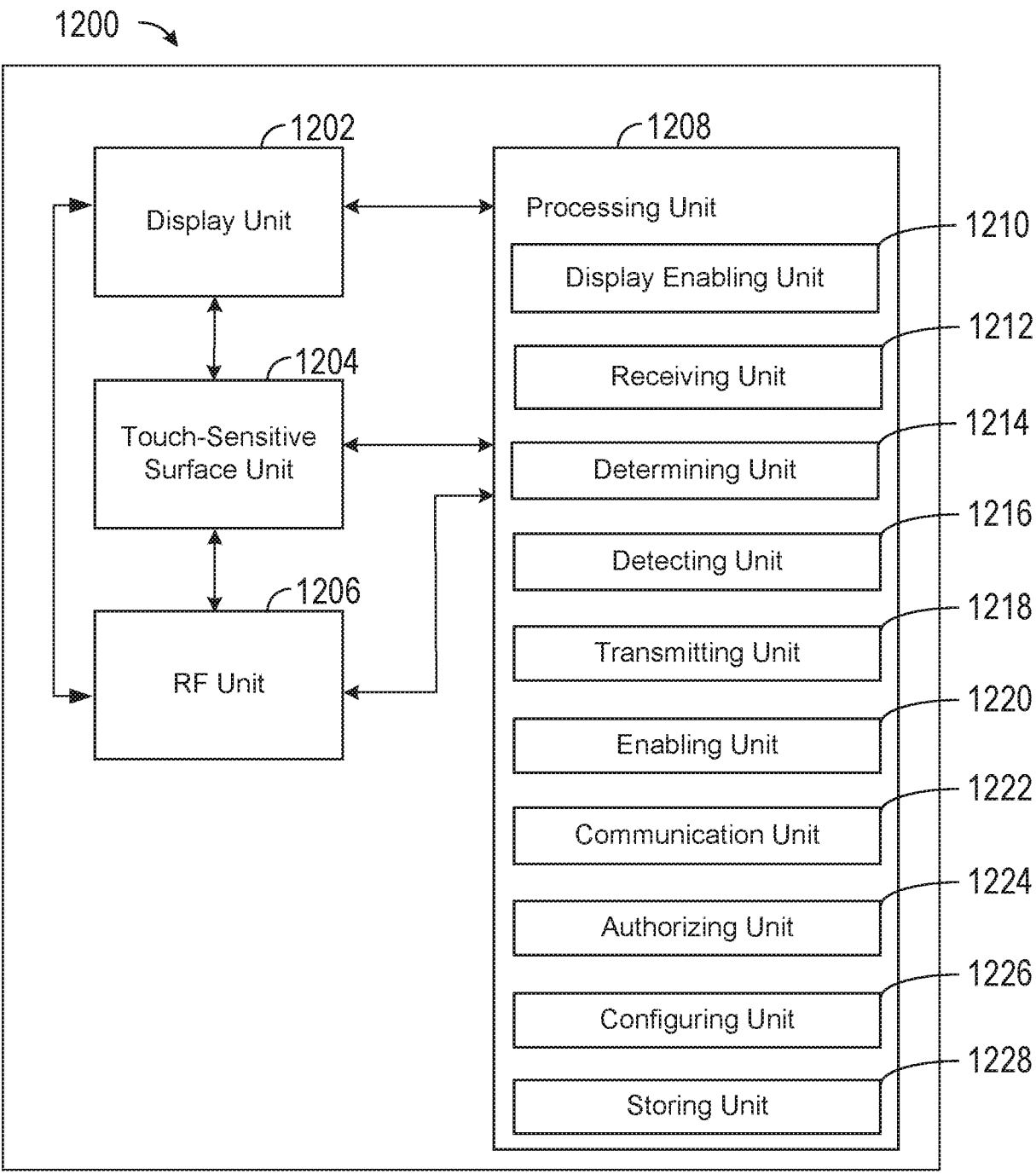


FIG. 12

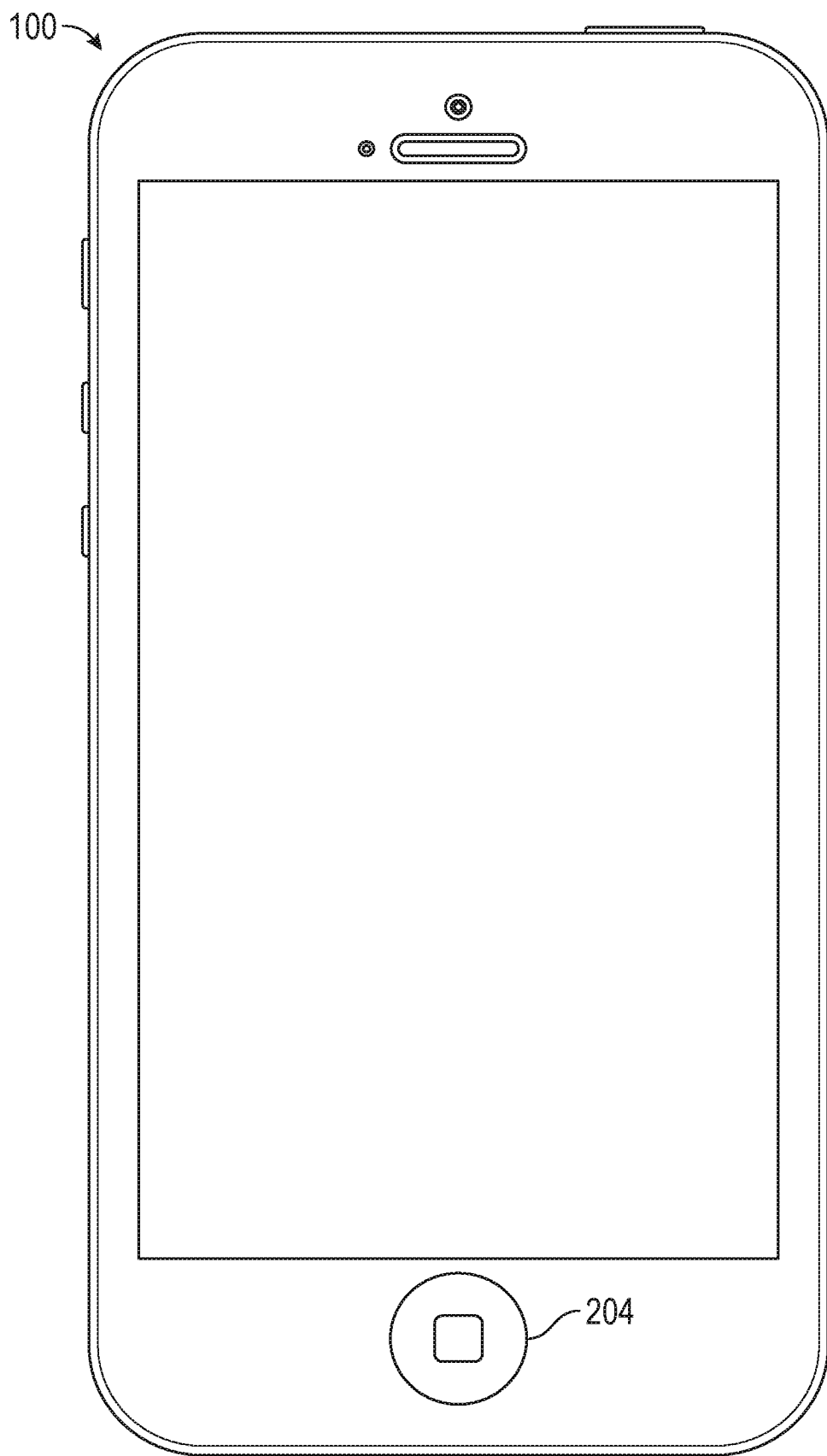


FIG. 13A

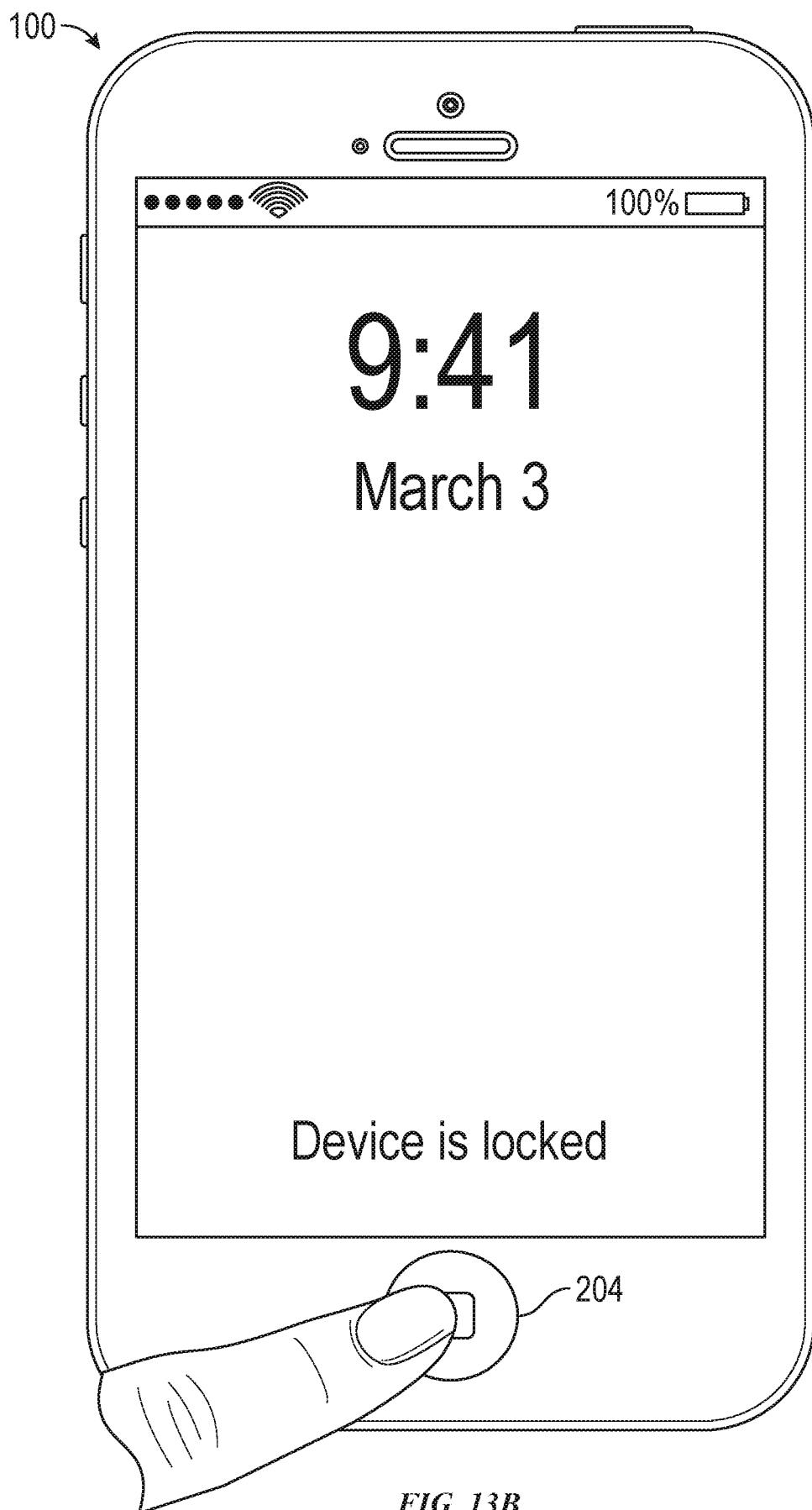


FIG. 13B

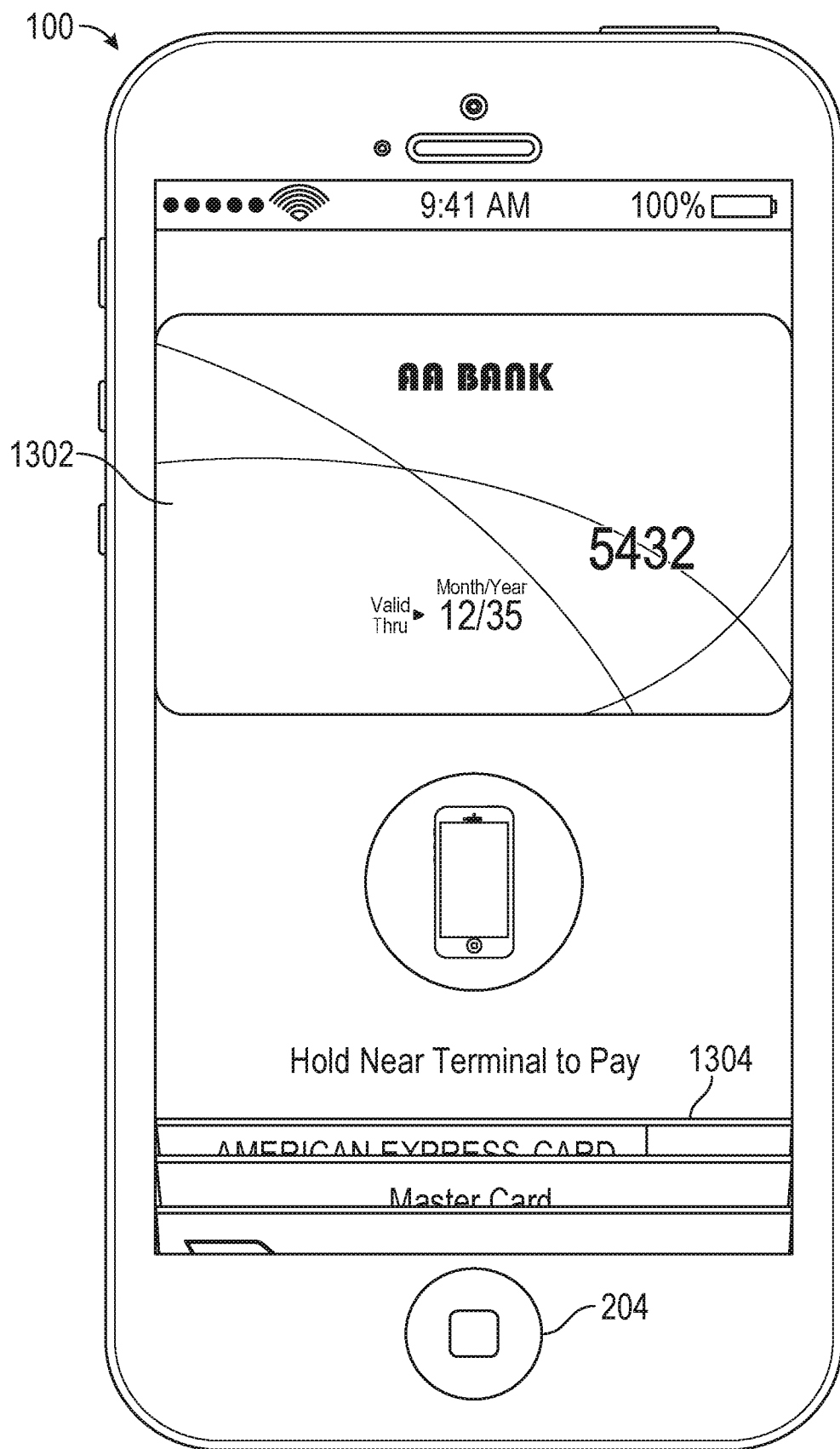


FIG. 13C

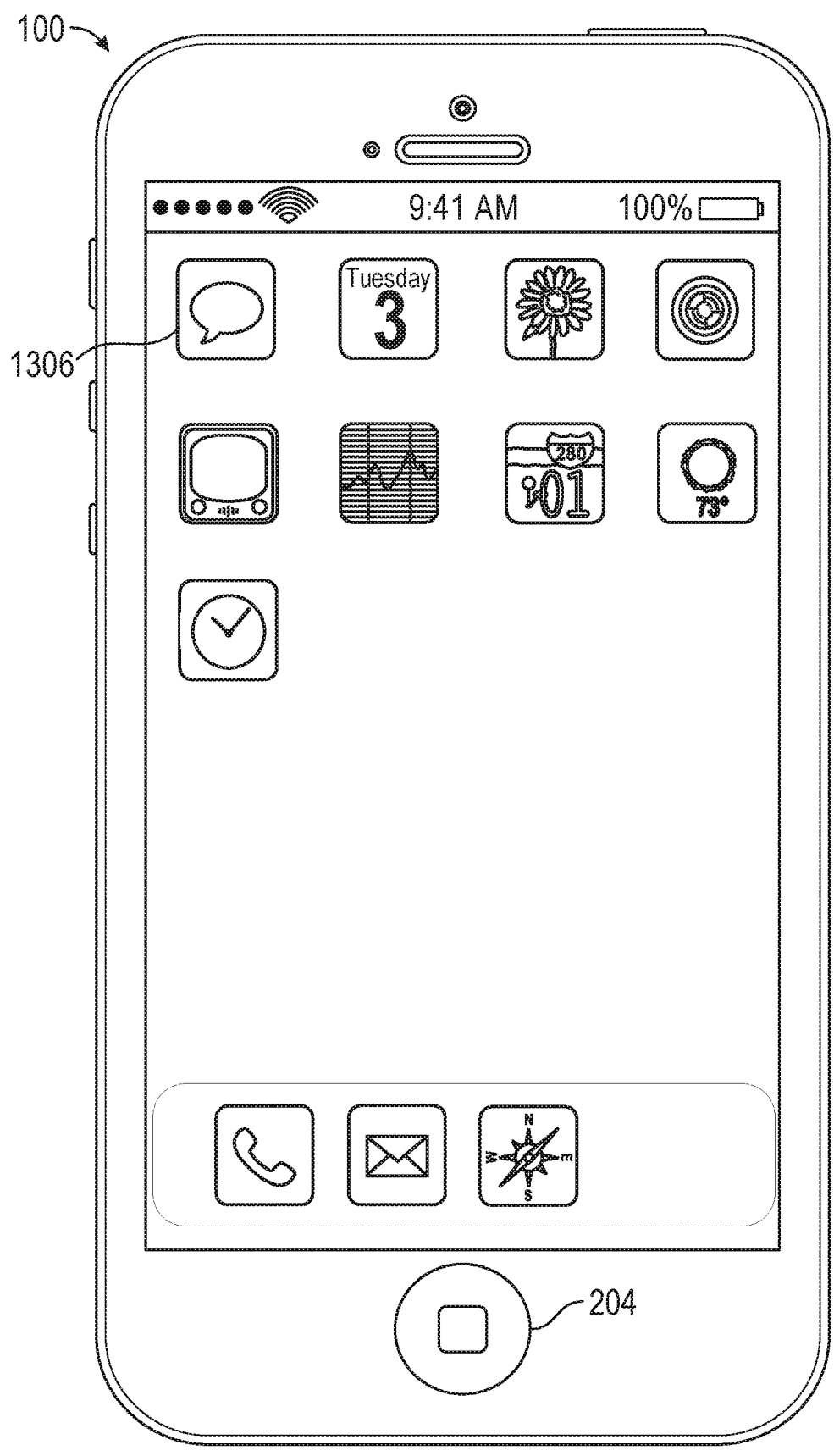


FIG. 13D

2016102031 24 Nov 2016

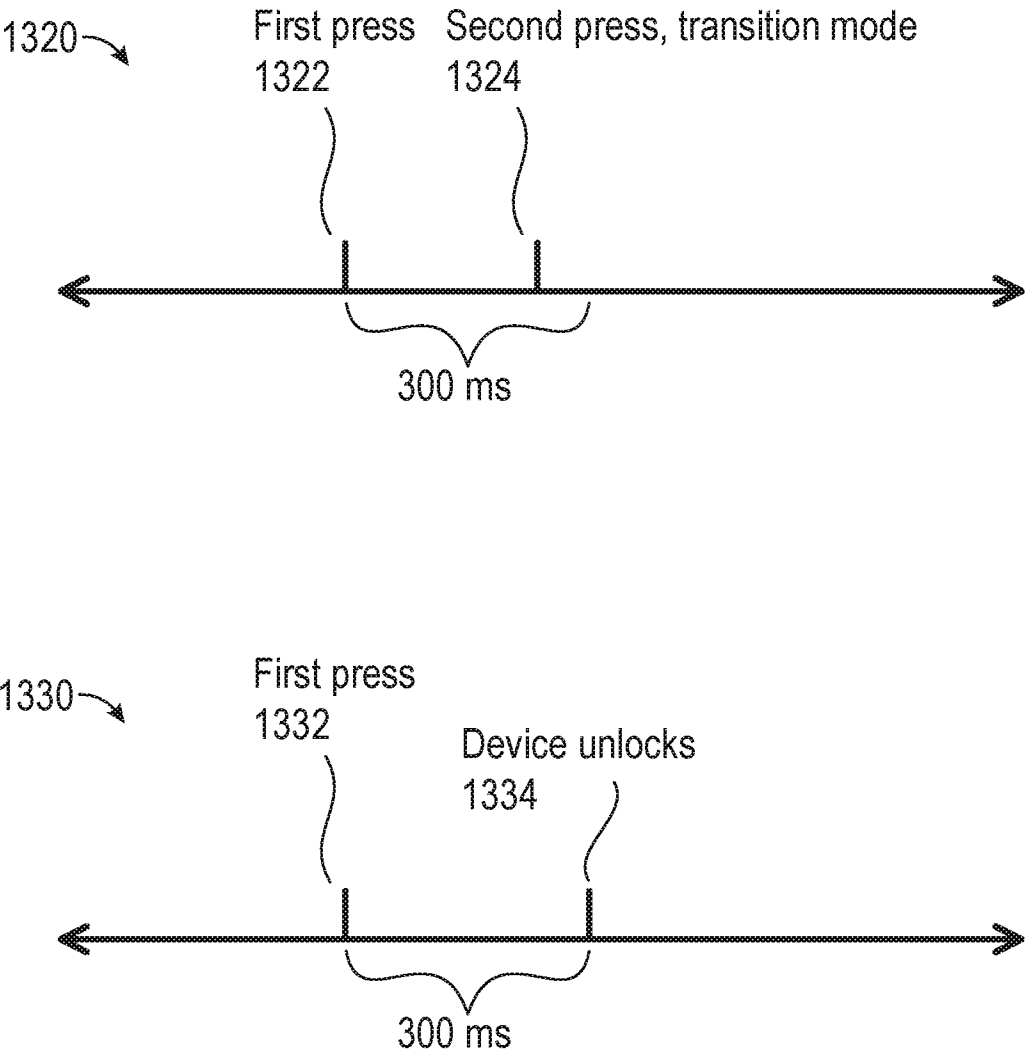
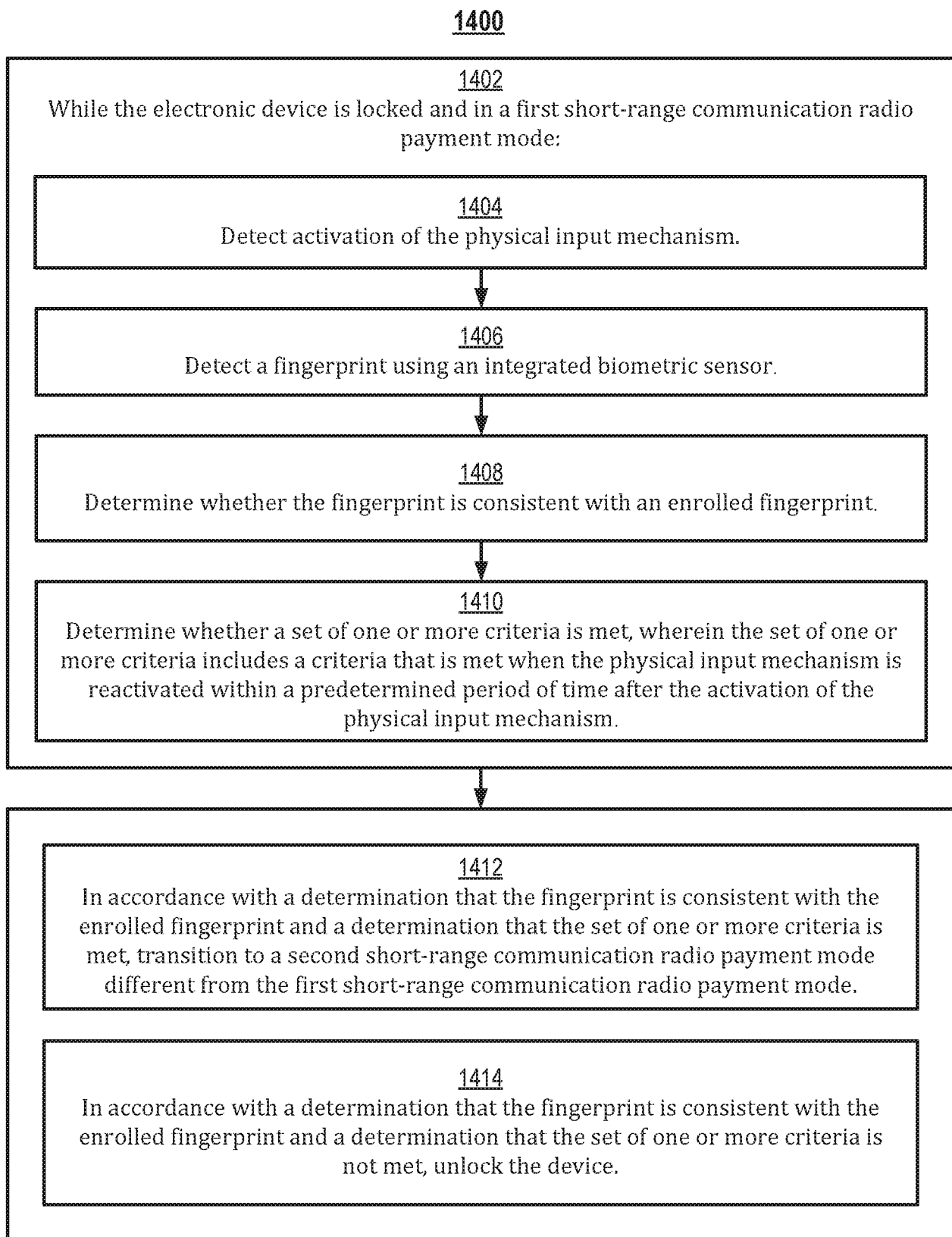


FIG. 13E

*FIG. 14*

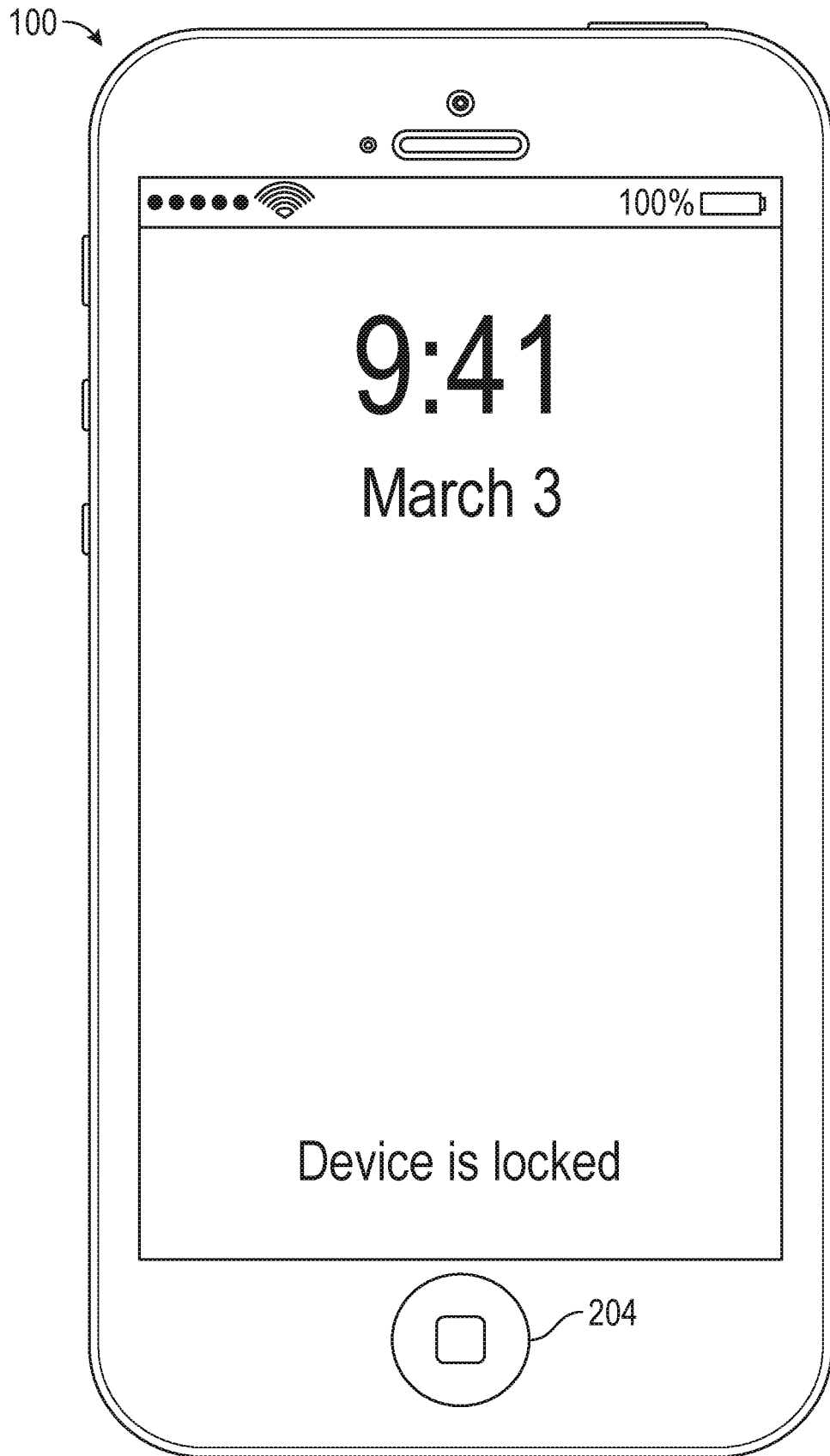


FIG. 15A

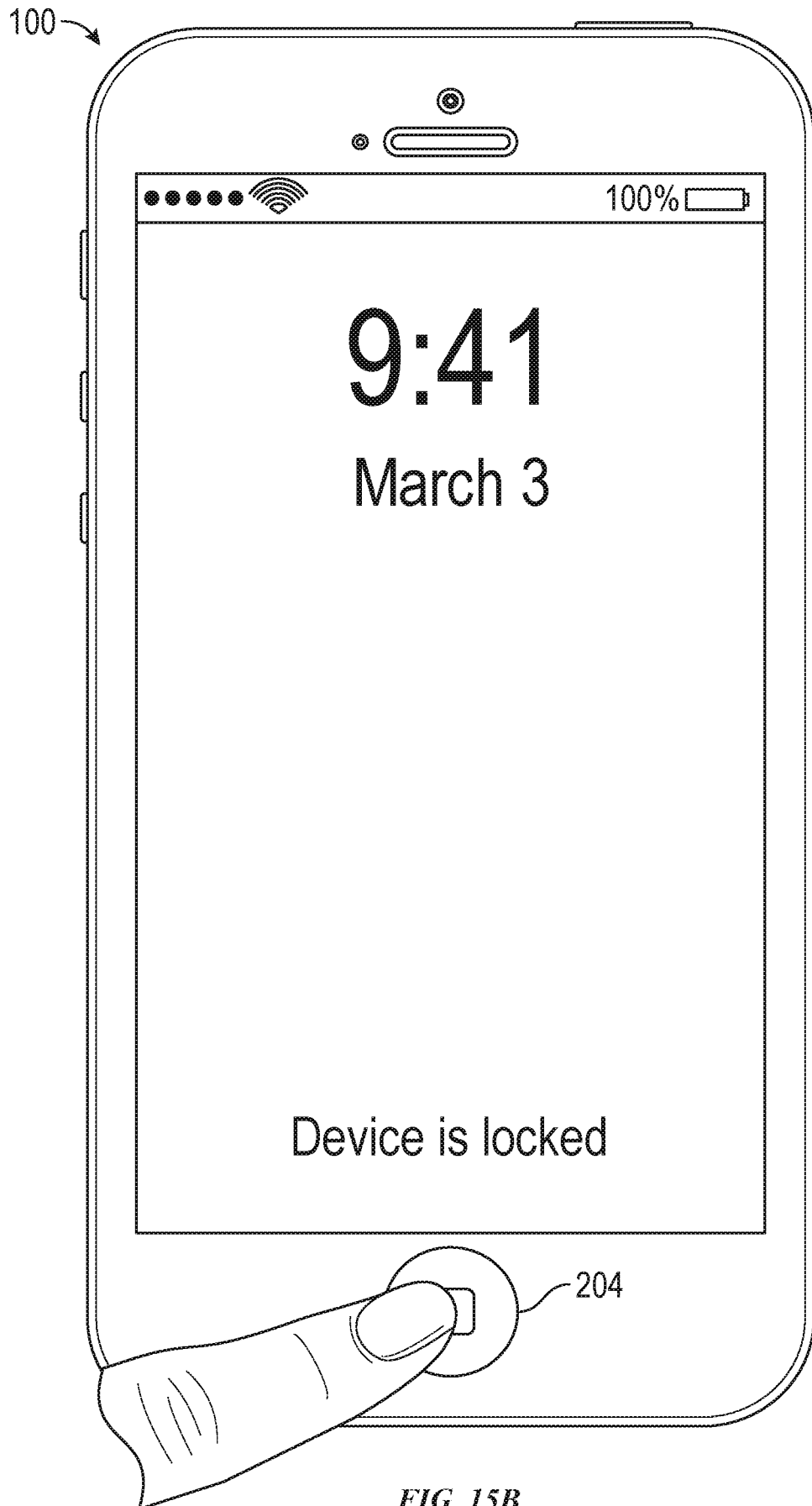


FIG. 15B

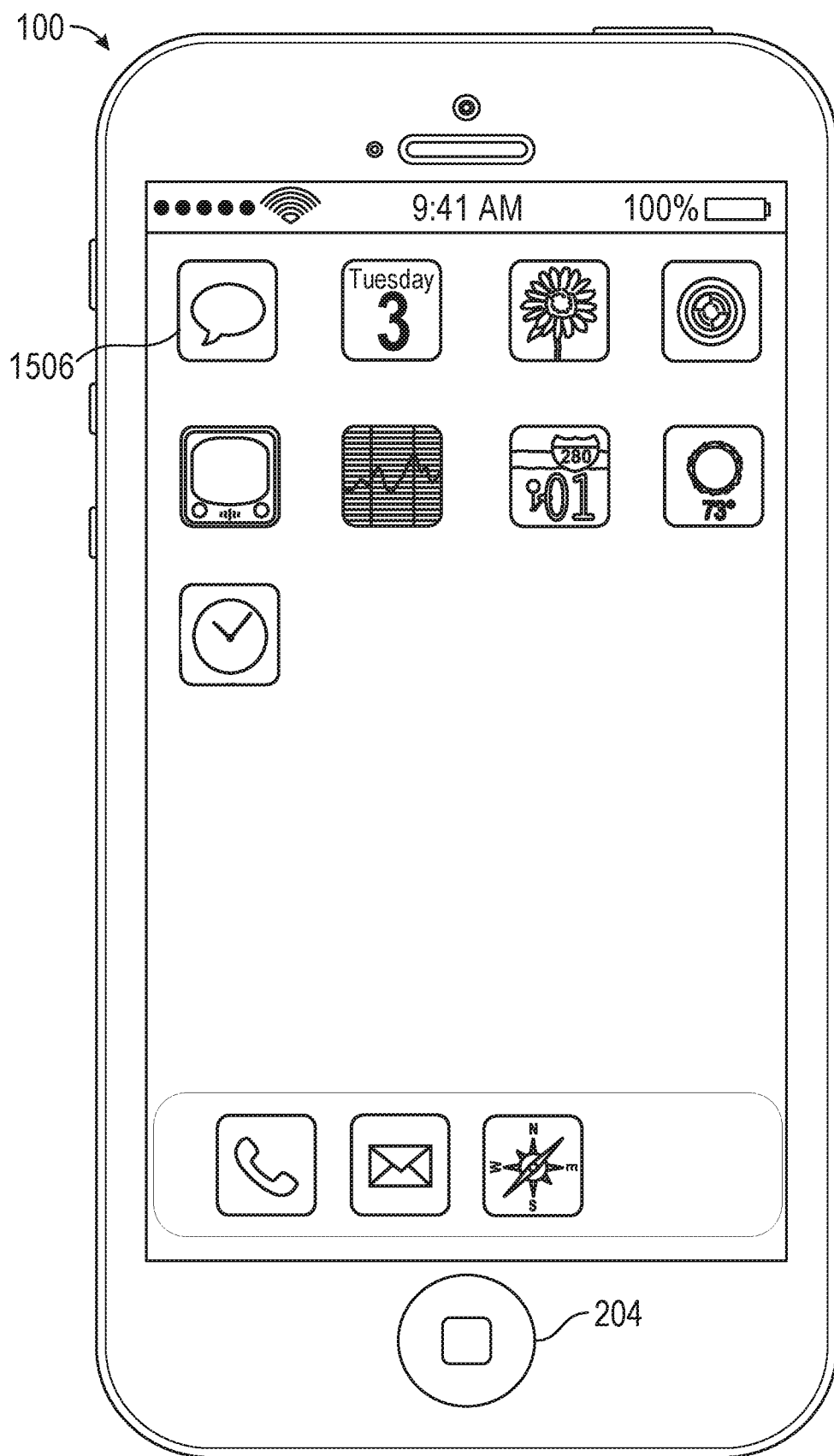


FIG. 15C

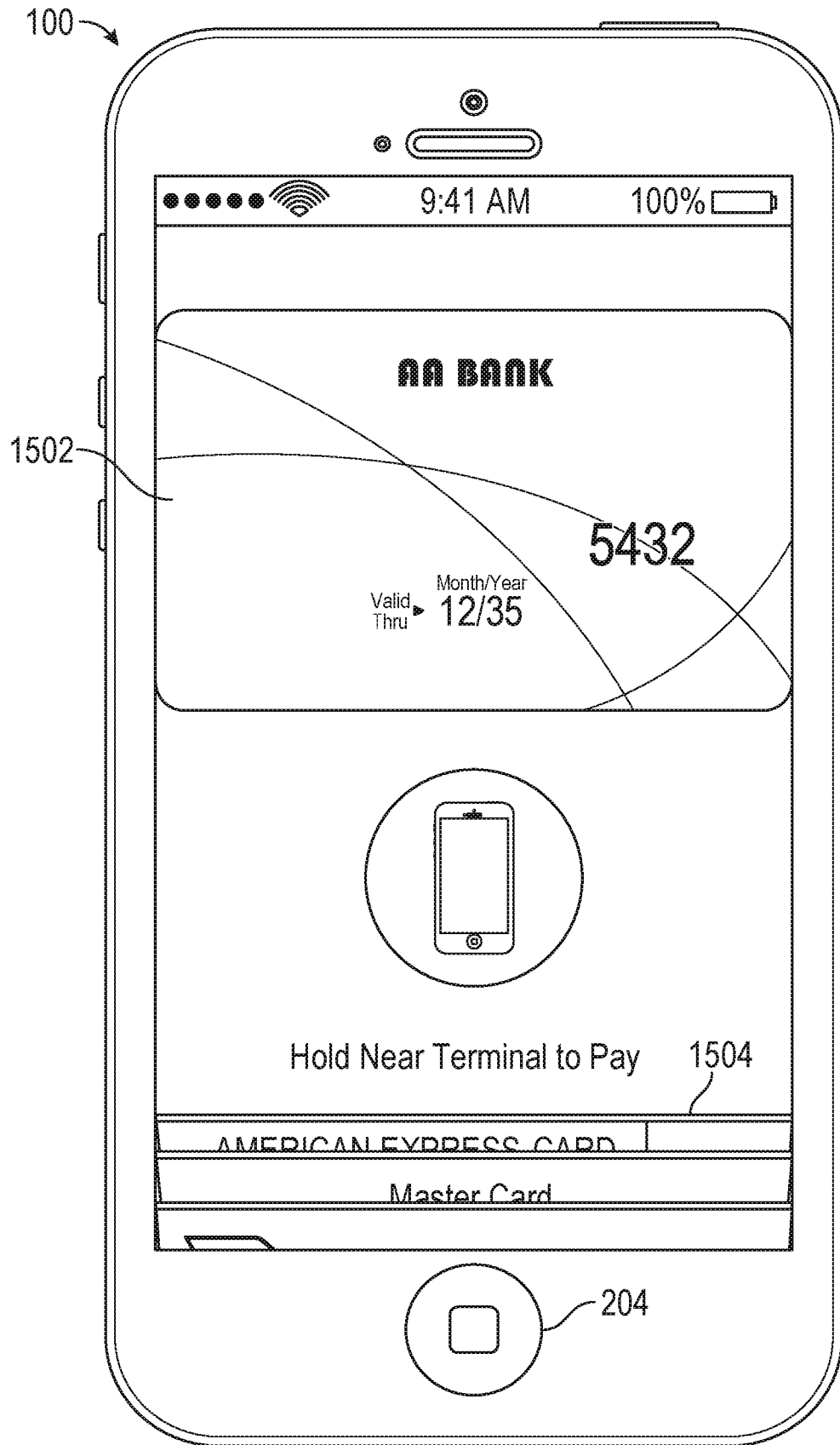


FIG. 15D

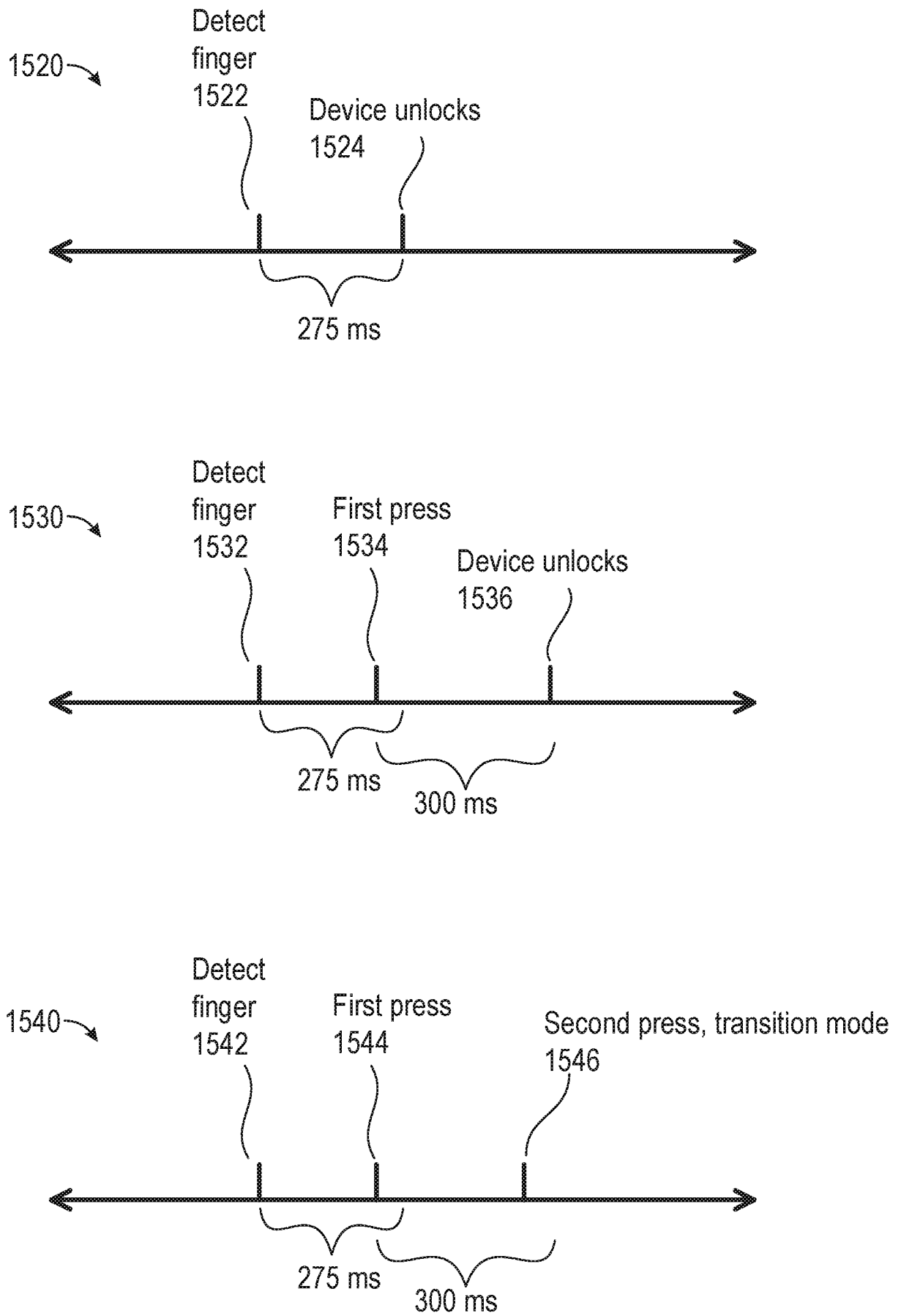


FIG. 15E

16001602

While the electronic device is locked and in a first short-range communication radio payment mode:

1604

Detect a fingerprint using the integrated biometric sensor.

1606

Determine whether the fingerprint is consistent with an enrolled fingerprint.

1608

Determine whether a set of one or more criteria is met, wherein the set of one or more criteria includes a criteria that is met when the physical input mechanism is activated within a first predetermined period of time after detecting the fingerprint using the biometric sensor.

1610

In accordance with a determination that the fingerprint is consistent with an enrolled fingerprint and a determination that the set of one or more criteria is not met, unlock the device.

1612

In accordance with a determination that the set of one or more criteria is met:

1614

Determine whether the physical input mechanism is reactivated within a second predetermined period of time after the activation of the physical input mechanism.

1616

In accordance with a determination that the physical input mechanism is not reactivated within the second predetermined period of time and a determination that the fingerprint is consistent with an enrolled fingerprint, unlock the device.

1618

In accordance with a determination that the physical input mechanism is reactivated within the second predetermined period of time and in accordance with a determination that the fingerprint is consistent with an enrolled fingerprint, transition to a second short-range communication radio payment mode different from the first short-range communication radio payment mode.

FIG. 16

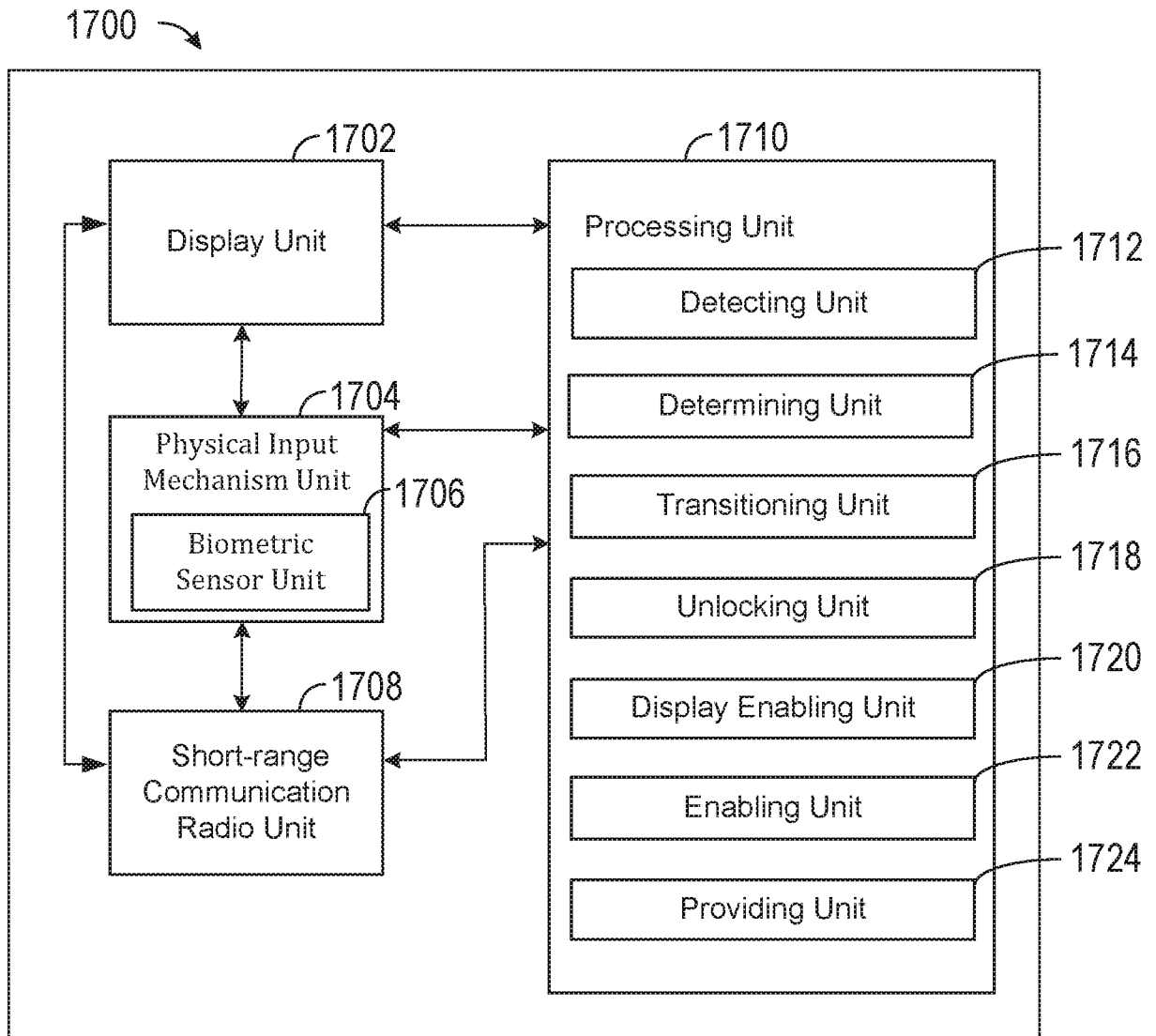


FIG. 17

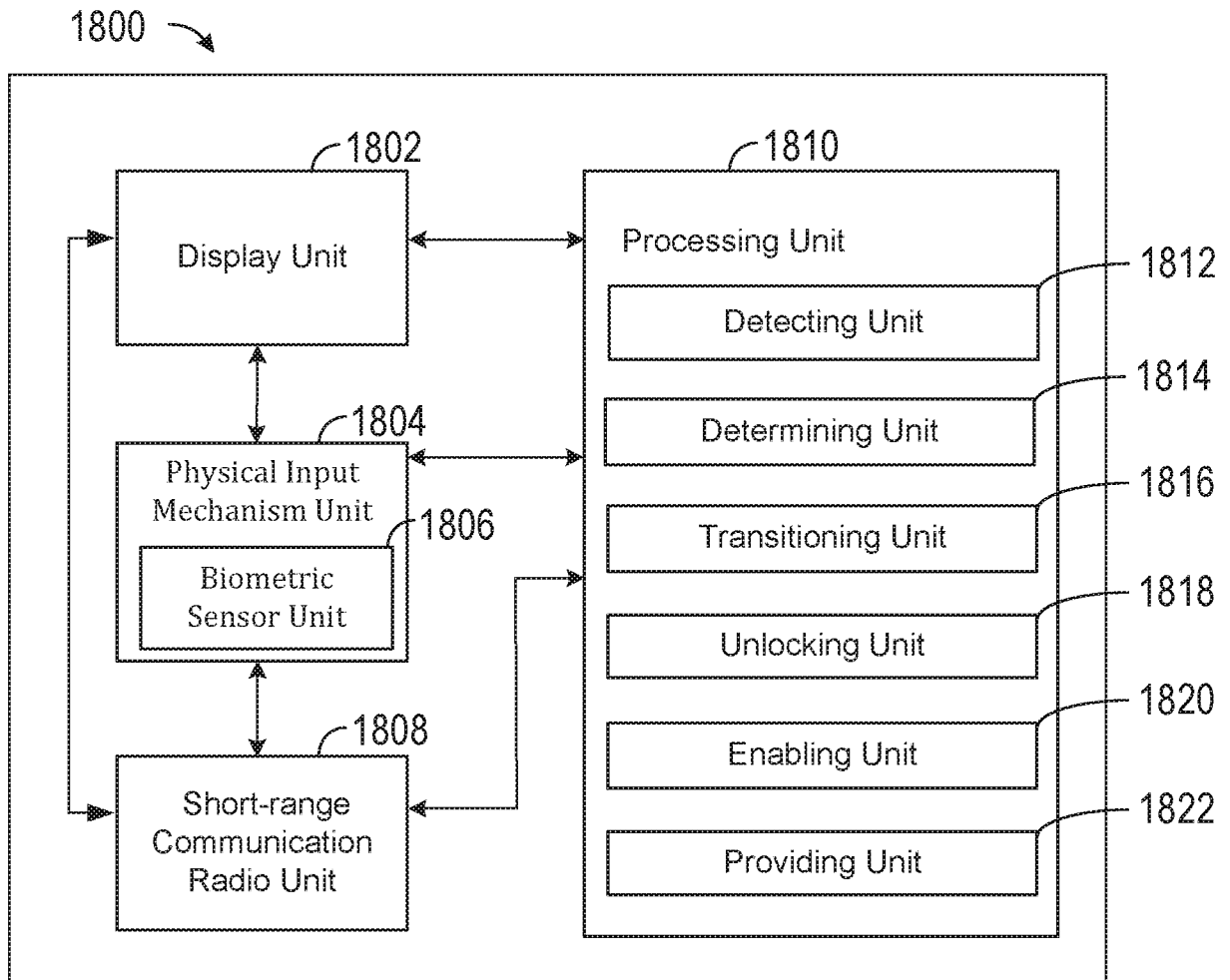


FIG. 18