

Appendix C

Appendix C: Claim Chart for U.S. Patent No.9,405,947

Claim No.	Claim Language	Accused Products ^{1,2,3}
1[a]	A method for operating a mobile communication device comprising:	To the extent that the claim's preamble is determined to be a limitation or otherwise limiting, the Accused Products are mobile communication devices. For example, the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, via LTE, CDMA, UMTS, and/or GSM), and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling), as well as RFID communication (<i>e.g.</i>, via NFC). (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, Via LTE, LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling), as well as RFID communication (<i>e.g.</i>, via RFID/NFC, including via Apple Pay, which uses NFC technology between the device and the payment terminal). (VAR0000639-1074).

¹ Accused Products, as used herein, are defined in the cover document to Varia's Preliminary Infringement Contentions. As set forth in the cover document to Varia's Preliminary Infringement Contentions, this is based on Varia's present understanding without the benefit of discovery.

² The citations in this Claim Chart are exemplary and illustrative. Varia reserves the right to amend and/or supplement these Contentions, including this Claim Chart, in any manner and for any of the reasons set forth in the cover document to Varia's Preliminary Infringement Contentions, including this Claim Chart, including after a complete production of the relevant source code and other non-public technical information and claim construction.

³ This Claim Chart incorporates Appendix D by reference in its entirety. Appendix D is based on publicly available information without the benefit of discovery. Varia reserves the right to amend and/or supplement Appendix D, in any manner and for any of the reasons set forth in the cover document to Varia's Preliminary Infringement Contentions, including this Claim Chart, including after a complete production of the relevant source code and other non-public technical information and claim construction.

For example, the iPhone as a whole is capable of entering two different modes, including a telephony mode and an RFID/NFC mode. A user can affirmatively launch the telephony and/or RFID/NFC modes, and/or the iPhone enters the telephony and/or RFID/NFC mode when its received the relevant signal (e.g., an incoming call or detecting an RFID reader), as shown below.



			When an RFID reader signal is detected by the mobile communications device, the user must first address how to respond to that signal telephony controls, and vice versa.
1[b]	receiving, by the mobile communication device, a radio frequency identification (RFID) probing signal from an RFID reader external to the mobile communication device;	The Accused Products receive a radio frequency identification (RFID) probing signal from an RFID reader external to the mobile communication device. For example, the Accused RFID/NFC Features (e.g. Apple Pay) conforms to the EMV Contactless standard, which incorporates the ISO/IEC 14443 standard for proximity cards. (VAR0000001-02). The Accused Products act as a proximity card (PICC) as defined by the ISO/IEC 14443 standard. The Accused Products use signals and commands according to ISO/IEC 14443 and/or ISO/IEC 7816-4.⁴ For example, the Accused Products, in accordance with ISO/IEC 14443, receive an RFID probing signal (e.g., Request (REQA) and Wake Up (WUPA) commands) from an RFID reader external to the mobile communication device (e.g., a coupling device).	

⁴ <https://developer.apple.com/documentation/corenfc/cardsession/>

	3.5 PICC <i>contactless integrated circuit card</i> (3.3) or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device Note 1 to entry: Commonly called a proximity card. (VAR0000054-71). 5.2.1 Polling In order to detect PICCs which are in the operating field, the PCD shall send repeated request commands. The PCD shall send REQA (or WUPA) and REQB (or WUPB) in any sequence using an equal or configurable duty cycle when polling Type A and Type B. In addition, the PCD may send other commands as described in Annex C. 6.4.1 REQA and WUPA commands The REQA and WUPA commands are sent by the PCD to probe the field for PICCs of Type A. They are transmitted within a short frame. See Figure 7 to check in which cases PICCs actually have to answer to these respective commands. Particularly, the WUPA command is sent by the PCD to put PICCs which have entered HALT state back into READY* state. They shall then participate in further anticollision and selection procedures. (VAR0000126-189).
1[c]	executing, on processing circuitry in the mobile communication device, instructions stored in a memory in the mobile communication device, the instructions configured to The Accused Products execute on processing circuitry in the mobile communication device, instructions stored in a memory in the mobile communication device, the instructions configured to cause the mobile communication device to perform the steps below. For example, the iPhone 7 has processing circuitry (e.g., A10 Fusion chip, NXP 67V04 NFC Controller, Secure Element) and a memory (e.g., SK Hynix 32 GB flash memory, NXP 67V04 NFC Controller, Secure Element), including instructions (e.g., iOS operating system, RFID/NFC protocols,

	cause the mobile communication device to: %	Secure Element applets), configured to cause the iPhone to perform the instructions discussed below. (VAR0000504-518). As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal circuitry and components, including, for each Accused Product, the components specified in Appendix D, including processing circuitry (specified in Column B), a memory (specified in Column C), and instructions (specified in Column G), configured to cause the Accused Product to perform the instructions discussed below. The components specified in Appendix D are incorporated here by reference. For example, as specified in Appendix D, the iPhone 6 has processing circuitry (e.g., A8 chip, NXP 65V10 NFC module, Secure Element) and a memory (e.g., SanDisk SDMFLBCB2 128GB (16GB) NAND flash, NXP 65V10 NFC module, Secure Element), including instructions (e.g., iOS operating system, RFID/NFC protocols, Secure Element applets), configured to cause the iPhone to perform the instructions discussed below. (VAR0000432-448). To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (e.g., emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (e.g., through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (e.g., mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions).
1[d]	output an RFID signal and output a voice call signal, wherein the RFID signal is output in response to the mobile communication	The Accused Products output an RFID signal and output a voice call signal, wherein the RFID signal is output in response to the mobile communication device determining the mobile communication device is in an operational space of the RFID reader based upon receipt of the RFID probing signal, and wherein the voice call signal is output over a wireless network and within a radio frequency range that is different than a radio frequency range used to output the RFID signal.

	device determining the mobile communication device is in an operational space of the RFID reader based upon receipt of the RFID probing signal, and wherein the voice call signal is output over a wireless network and within a radio frequency range that is different than a radio frequency range used to output the RFID signal. For example, the iPhone 7 is configured to output RFID signals, because the iPhone is capable of Near Field Communication (NFC), as evidenced by, <i>e.g.</i>, technical specifications of the iPhone 7 that specify NFC with tag emulation mode feature (Apple Pay). NFC is a RFID-based technology for data exchange using radio waves. NFC is a subset within the family of RFID technology. (VAR0000026-42) (“RFID is the process by which items are uniquely identified using radio waves, and NFC is a specialized subset within the family of RFID technology.”); (VAR0000043-53) (“Hierarchically, NFC is a subset of RFID.”)). The iPhone 7 is configured to output voice call signals over a wireless cellular network (<i>e.g.</i>, 850, 900, 1800, 1900 MHz for GSM/EDGE, and/or 3G UMTS), and is also configured to output voice call signals that are signals for audio calling services that use a Wi-Fi connection or a high-speed cellular connection (<i>e.g.</i>, FaceTime Audio, Voice over LTE (VoLTE), and Wi-Fi calling). (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, are configured to output RFID signals, because they are capable of Near Field Communication (NFC), as evidenced by, <i>e.g.</i>, technical specifications that specify NFC with tag emulation mode feature (Apple Pay). NFC is a RFID-based technology for data exchange using radio waves. NFC is a subset within the family of RFID technology. (VAR0000026-42) (“RFID is the process by which items are uniquely identified using radio waves, and NFC is a specialized subset within the family of RFID technology.”); (VAR0000043-53) (“Hierarchically, NFC is a subset of RFID.”)). The Accused Products, including iPhone models and Apple Watch models, are also configured to output voice call signals over a wireless cellular network (<i>e.g.</i>, UMTS, LTE, 5G), and/or output voice call signals that are signals for audio calling services that use a Wi-Fi connection or a high-speed cellular connection (<i>e.g.</i>, FaceTime Audio, Voice over LTE (VoLTE), and Wi-Fi calling). (VAR0000639-1074). The Accused Products output a an RFID signal in response to the mobile communication device determining the mobile communication device is in an operational space of the RFID reader based upon receipt of the RFID probing signal. For example, the Accused RFID/NFC Features (<i>e.g.</i> Apple Pay) conforms to the EMV Contactless standard, which incorporates the ISO/IEC 14443 standard for proximity cards. (VAR0000001-02). The Accused Products act as a proximity card (PICC) as defined by the ISO/IEC 14443 standard. The
--	---

	Accused Products use signals and commands according to ISO/IEC 14443 and/or ISO/IEC 7816-4.⁵ For example, the Accused Products, in accordance with ISO/IEC 14443, determine that they are in an operational space (e.g., operating field) of the RFID reader (e.g., proximity coupling device “PCD”) based upon receipt of an RFID probing signal (e.g., REQA and WUPA commands) received by the mobile device from the RFID reader. The Accused Products, acting in accordance with ISO/IEC 14443, output an RFID signal (e.g., Answer to Request or ATQA) in response. 3.5 PICC <i>contactless integrated circuit card (3.3)</i> or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device Note 1 to entry: Commonly called a proximity card. (VAR0000054-71). 5.2.1 Polling In order to detect PICCs which are in the operating field, the PCD shall send repeated request commands. The PCD shall send REQA (or WUPA) and REQB (or WUPB) in any sequence using an equal or configurable duty cycle when polling Type A and Type B. In addition, the PCD may send other commands as described in Annex C. 6.4.1 REQA and WUPA commands The REQA and WUPA commands are sent by the PCD to probe the field for PICCs of Type A. They are transmitted within a short frame. See Figure 7 to check in which cases PICCs actually have to answer to these respective commands. Particularly, the WUPA command is sent by the PCD to put PICCs which have entered HALT state back into READY* state. They shall then participate in further anticollision and selection procedures. (VAR0000126-189).
--	--

⁵ <https://developer.apple.com/documentation/corenfc/cardsession/>

	6.3.2 IDLE state Description: In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands. State exit conditions and transitions: The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA. (VAR0000126-189). The Accused Products output a voice call signal over a wireless network and within a radio frequency range that is different than a radio frequency range used to output the RFID signal. For example, the iPhone 7, acting in accordance with ISO/IEC 14443, outputs an RFID signal within a radio frequency range (<i>e.g.</i>, 13.56 MHz frequency). The iPhone 7 outputs a voice call signal (<i>e.g.</i>, via cellular and/or Wi-Fi) over a wireless network within a radio frequency range (<i>e.g.</i>, 850 MHz, 1900 MHz, 2.4 GHz) that is different than a radio frequency range used to output the RFID signal. (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, output an RFID signal within a radio frequency range (<i>e.g.</i>, 13.56 MHz frequency), and output a voice call signal (<i>e.g.</i>, via cellular and/or Wi-Fi) over a wireless network within a radio frequency range (<i>e.g.</i>, 850 MHz, 1900 MHz, 2.4 GHz) that is different than a radio frequency range used to output the RFID signal. (VAR0000639-1074). 6.2 Frequency The frequency, f_c of the RF operating field shall be 13,56 MHz $\pm$ 7 kHz. (VAR0000072-125).

2	The method of claim 1, wherein the RFID signal includes RFID data comprising a selected one of a security key and an identifier.	The Accused Products perform the method of claim 1, wherein the RFID signal includes RFID data comprising a selected one of a security key and an identifier. For example, credit cards can be added to Apple Pay, and the Accused Products may then be used to make contactless payments using those credit cards. In addition, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Products may then be used to unlock the hotel room and/or car. (VAR000003-09; VAR0000020-22; VAR0001075-1293). The data includes, e.g., data from applets within the Secure Element. Secure Element The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus. NFC controller As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server. (VAR0001075 at 1209).
---	---	--

		Privacy and security Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted. (VAR VAR0001075 at 12222).
3	The method of claim 2, wherein the security key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key.	The Accused Products perform the method of claim 2, wherein the security key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key. For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Products may then be used to unlock the hotel room and/or car. (VAR0000003-09). The keys include, e.g., keys stored on applets in the Secure Element. Privacy and security Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted. (VAR VAR0001075 at 12222).
4	The method of claim 2, wherein the identifier comprises a selected one of	The Accused Products perform the method of claim 2, wherein the identifier comprises a selected one of a social security number, a driver's license number, an affinity program account number, and a

	a social security number, a driver's license number, an affinity program account number, and a credit card number.	credit card number. For example, credit cards can be added to Apple Pay, and the Accused Products may then be used to make contactless payments using those credit cards. (VAR0000020-22, VAR0001075-1293).
5	The method of claim 2, wherein the method further comprises facilitating a user in selecting the RFID data from a plurality of the RFID data using the mobile communication device.	The Accused Products perform the method of claim 2, wherein the method further comprises facilitating a user in selecting the RFID data from a plurality of the RFID data using the mobile communication device. For example, multiple payment cards can be added to Apple Pay, and the Accused Products may then be used to select a card to make a contactless payment. (VAR0000020-22).
6	The method of claim 2, wherein the method further comprises facilitating provision of the RFID data to the mobile communication device.	The Accused Products perform the method of claim 2, wherein the method further comprises facilitating provision of the RFID data to the mobile communication device. For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments with Apple Pay using the Accused Products. (VAR0001075-1293 at 1210-211). Apple also directs and controls the provisioning of keys and passes. (VAR0000003-09).

		Credit, debit, and prepaid cards Card provisioning security overview When a user adds a credit, debit, or prepaid card (including store cards) to Apple Wallet, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer determines whether to approve adding the card to Apple Wallet. As part of the card provisioning process, Apple Pay uses three server-side calls to send and receive communication with the card issuer or network: • Required Fields • Check Card • Link and Provision The card issuer or network uses these calls to verify, approve, and add cards to Apple Wallet. These client-server sessions use TLS 1.2 to transfer the data. Full card numbers aren't stored on the device or on Apple Pay servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from most credit or debit card numbers; the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is never stored on Apple Pay servers or backed up to iCloud, and it is isolated from iOS, iPadOS, and watchOS devices and from Mac computers with Touch ID. Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone, or within a card issuer's iPhone app. Adding a card to Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch.

		Adding credit or debit cards manually To add a card manually, the name, card number, expiration date, and CVV are used to facilitate the provisioning process. From within Settings, Apple Wallet, or the Apple Watch app, users can enter that information either by typing or by using the device's camera. When the camera captures the card information, Apple attempts to populate the name, card number, and expiration date. The photo is never saved to the device or stored in the photo library. After all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are then encrypted and sent to the Apple Pay server. If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the terms and conditions, Apple sends the ID of the terms that were accepted as well as the CVV to the Link and Provision process. Additionally, as part of the Link and Provision process, Apple shares information from the device with the card issuer or network. This includes information about (a) the user's iTunes and App Store account activity (for example, whether the user has a long history of transactions within iTunes), (b) the user's device (for example, the phone number, name, and model of the user's device plus any companion Apple device necessary to set up Apple Pay), and (c) the user's approximate location at the time the user adds their card (if the user has Location Services enabled). Using this information, the card issuer determines whether to approve adding the card to Apple Pay. As the result of the Link and Provision process, two things occur: • The device begins to download the Apple Wallet pass file representing the credit or debit card. • The device begins to bind the card to the Secure Element. The pass file contains URLs to download card art, metadata about the card such as contact information, the related issuer's app, and supported features. It also contains the pass state, which includes information such as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whether additional verification is required before the card can make payments with Apple Pay.
--	--	--

7	The method of claim 6, wherein facilitating provisioning of the RFID data to the mobile communication device includes facilitating provision of at least a signaling attribute associated with the outputting of the RFID data.	The Accused Products perform the method of claim 6, wherein facilitating provisioning of the RFID data to the mobile communication device includes facilitating provision of at least a signaling attribute associated with the outputting of the RFID data. For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments with Apple Pay using the Accused Devices, and Apple further directs, controls, and specifies the communication and security protocols associated with making contactless payments via Apple Pay. (VAR0001075-1293 at 1208-09). Apple also directs and controls the provisioning of keys and passes. (VAR00000003-09). NFC controller The NFC controller handles Near Field Communication protocols and routes communication between the Application Processor and the Secure Element, and between the Secure Element and the point-of-sale terminal. NFC controller As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.
---	--	---

8	The method of claim 1, wherein the mobile communication device is one of a wireless mobile phone and a personal digital assistant equipped with communication capability. For example the Accused Products are wireless mobile phones and/or personal digital assistants equipped with communication capability. For example the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, via LTE, CDMA, UMTS, and/or GSM), and/o audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling). (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, Via LTE via LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling). (VAR0000639-1074).	The Accused Products perform the method of claim 1, wherein the mobile communication device is one of a wireless mobile phone and a personal digital assistant equipped with communication capability. For example the Accused Products are wireless mobile phones and/or personal digital assistants equipped with communication capability. For example the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, via LTE, CDMA, UMTS, and/or GSM), and/o audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling). (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, Via LTE via LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling). (VAR0000639-1074).
9[a]	A method for operating a mobile device comprising:	To the extent that the claim's preamble is determined to be a limitation or otherwise limiting, the Accused Products are mobile communication devices. For example, the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, via LTE, CDMA, UMTS, and/or GSM), and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling), as well as RFID communication (<i>e.g.</i>, via NFC). (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, Via LTE, LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling), as well as RFID communication (<i>e.g.</i>, via RFID/NFC, including via Apple Pay, which uses NFC technology between the device and the payment terminal). (VAR0000639-1074). For example, the iPhone as a whole is capable of entering two different modes, including a telephony mode and an RFID/NFC mode. A user can affirmatively launch the telephony and/or RFID/NFC

modes, and/or the iPhone enters the telephony and/or RFID/NFC mode when its received the relevant signal (e.g., an incoming call or detecting an RFID reader), as shown below.



		 
		When an RFID reader signal is detected by the mobile communications device, the user must first address how to respond to that signal telephony controls, and vice versa.
9[b]	executing, on processing circuitry in the mobile communication device, the instructions stored in a memory in the mobile communication device, the instructions configured to cause the mobile communication device to monitor, output an RFID signal, and output a voice call signal;	The Accused Products execute on processing circuitry in the mobile communication device, instructions stored in a memory in the mobile communication device, the instructions configured to cause the mobile communication device to monitor, output an RFID signal, and output a voice call signal. For example, the iPhone 7 has processing circuitry (e.g., A10 Fusion chip, NXP 67V04 NFC Controller, Secure Element) and a memory (e.g., SK Hynix 32 GB flash memory, NXP 67V04 NFC Controller, Secure Element), including instructions (e.g., iOS operating system, RFID/NFC protocols, Secure Element applets), configured to cause the iPhone to perform the steps discussed below. (VAR0000504-518).

	As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal circuitry and components, including, for each Accused Product, the components specified in Appendix D, including processing circuitry (specified in Column B), a memory (specified in Column C), and instructions (specified in Column G), configured to cause the Accused Product to perform the instructions discussed below. These components specified in Appendix D are incorporated here by reference. • For example, as specified in Appendix D, the iPhone 6 has processing circuitry (<i>e.g.</i>, A8 chip, NXP 65V10 NFC module, Secure Element) and a memory (<i>e.g.</i>, SanDisk SDMLFLBCB2 128GB (16GB) NAND flash, NXP 65V10 NFC module, Secure Element), including instructions (<i>e.g.</i>, iOS operating system, RFID/NFC protocols, Secure Element applets), configured to cause the iPhone to perform the instructions discussed below. (VAR0000432-448). For example, the iPhone 7 is configured to output RFID signals, because the iPhone is capable of Near Field Communication (NFC), as evidenced by, <i>e.g.</i>, technical specifications of the iPhone 7 that specify NFC with tag emulation mode feature (Apple Pay). NFC is a RFID-based technology for data exchange using radio waves. NFC is a subset within the family of RFID technology. (VAR0000026-42) (“RFID is the process by which items are uniquely identified using radio waves, and NFC is a specialized subset within the family of RFID technology.”); (VAR0000043-53) (“Hierarchically, NFC is a subset of RFID.”). The iPhone 7 is configured to output voice call signals over a wireless cellular network (<i>e.g.</i>, 850, 900, 1800, 1900 MHz for GSM/EDGE, and/or 3G UMTS), and is also configured to output voice call signals that are signals for audio calling services that use a Wi-Fi connection or a high-speed cellular connection (<i>e.g.</i>, FaceTime Audio, Voice over LTE (VoLTE), and Wi-Fi calling). (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, are configured to output RFID signals, because they are capable of Near Field Communication (NFC), as evidenced by, <i>e.g.</i>, technical specifications that specify NFC with tag emulation mode feature (Apple Pay). NFC is a RFID-based technology for data exchange using radio waves. NFC is a subset within the family of RFID technology. (VAR0000026-42) (“RFID is the process by which items are uniquely identified using radio waves, and NFC is a specialized subset within the family of RFID technology.”); (VAR0000043-53) (“Hierarchically, NFC is a subset of RFID.”). The Accused Products, including iPhone models and Apple Watch models, are also configured to output voice call
--	--

	signals over a wireless cellular network (e.g., UMTS, LTE, 5G), and/or output voice call signals that are signals for audio calling services that use a Wi-Fi connection or a high-speed cellular connection (e.g., FaceTime Audio, Voice over LTE (VoLTE), and Wi-Fi calling). (VAR00000639-1074). The Accused Products monitor for a proximal presence of a radio frequency identification (RFID) reader external to the mobile communication device. For example, the Accused RFID/NFC Features (e.g., Apple Pay) conforms to the EMV Contactless standard, which incorporates the ISO/IEC 14443 standard for proximity cards. (VAR0000001-02). The Accused Products act as a proximity card (PICC) as defined by the ISO/IEC 14443 standard. The Accused Products use signals and commands according to ISO/IEC 14443 and/or ISO/IEC 7816-4.⁶ For example, the Accused Products, in accordance with ISO/IEC 14443, receive an RFID probing signal (e.g., Request (REQA) and Wake Up (WUPA) commands) from an RFID reader external to the mobile communication device (e.g., a coupling device). 3.5 PICC <i>contactless integrated circuit card (3.3)</i> or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device Note 1 to entry: Commonly called a proximity card. (VAR00000054). 5.2.1 Polling In order to detect PICCs which are in the operating field, the PCD shall send repeated request commands. The PCD shall send REQA (or WUPA) and REQB (or WUPB) in any sequence using an equal or configurable duty cycle when polling Type A and Type B. In addition, the PCD may send other commands as described in Annex C.
--	--

⁶ <https://developer.apple.com/documentation/corenfc/cardsession/>

		6.4.1 REQA and WUPA commands The REQA and WUPA commands are sent by the PCD to probe the field for PICCs of Type A. They are transmitted within a short frame. See Figure 7 to check in which cases PICCs actually have to answer to these respective commands. Particularly, the WUPA command is sent by the PCD to put PICCs which have entered HALT state back into READY* state. They shall then participate in further anticollision and selection procedures. (VAR0000126-189). To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (<i>e.g.</i>, emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (<i>e.g.</i>, through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (<i>e.g.</i>, mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions).
9[c]	wherein the monitoring comprises monitoring for a proximal presence of a radio frequency identification (RFID) reader external to the mobile communication device and determining the mobile communication device is in an operational space of the RFID reader	The Accused Products monitor, wherein the monitoring comprises monitoring for a proximal presence of a radio frequency identification (RFID) reader external to the mobile communication device and determining the mobile communication device is in an operational space of the RFID reader based on an RFID probing signal received by the mobile communication device from the RFID reader. For example, the Accused RFID/NFC Features (<i>e.g.</i> Apple Pay) conforms to the EMV Contactless standard, which incorporates the ISO/IEC 14443 standard for proximity cards. (VAR0000001-02). The Accused Products act as a proximity card (PICC) as defined by the ISO/IEC 14443 standard. The Accused Products use signals and commands according to ISO/IEC 14443 and/or ISO/IEC 7816-4.7 For example, in accordance with ISO/IEC 14443, the Accused Products monitor for the proximal

⁷ <https://developer.apple.com/documentation/corenfc/cardsession/>

	based on an RFID probing signal received by the mobile communication device from the RFID reader;	presence of an RFID reader external to the mobile communication device (e.g., a contactless point-of-sale terminal) by listening for commands and recognizing Request (REQA) and Wake Up (WUPA) commands from the RFID reader. The Accused Products determine that they are in an operational space (e.g., operating field) of the RFID reader (e.g., proximity coupling device “PCD”) based on an RFID probing signal (e.g., REQA and WUPA commands) received by the mobile device from the RFID reader. 3.5 PICC <i>contactless integrated circuit card (3.3)</i> or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device Note 1 to entry: Commonly called a proximity card. (VAR0000054-71). 5.2.1 Polling In order to detect PICCs which are in the operating field, the PCD shall send repeated request commands. The PCD shall send REQA (or WUPA) and REQB (or WUPB) in any sequence using an equal or configurable duty cycle when polling Type A and Type B. In addition, the PCD may send other commands as described in Annex C. 6.4.1 REQA and WUPA commands The REQA and WUPA commands are sent by the PCD to probe the field for PICCs of Type A. They are transmitted within a short frame. See Figure 7 to check in which cases PICCs actually have to answer to these respective commands. Particularly, the WUPA command is sent by the PCD to put PICCs which have entered HALT state back into READY* state. They shall then participate in further anticollision and selection procedures. (VAR0000126-189).
--	--	--

9[d]	wherein the outputting of the RFID signal comprises outputting the RFID signal in response to determining the mobile communication device is within the proximal presence of the RFID reader based upon receipt of the RFID probing signal; and	The Accused Products output the RFID signal in response to determining the mobile communication device is within the proximal presence of the RFID reader based upon receipt of the RFID probing signal. The Accused Products use signals and commands according to ISO/IEC 14443 and/or ISO/IEC 7816-4.⁸ For example, the Accused Products, acting in accordance with ISO/IEC 14443, outputs an RFID signal (<i>e.g.</i>, Answer to Request or ATQA) in response to detection of the proximal presence (<i>e.g.</i>, IDLE state exit) of the RFID reader external to the mobile communication device based upon receipt of the RFID probing signal (<i>e.g.</i>, REQA and WUPA commands). The RFID signal is output in a radio frequency range (<i>e.g.</i>, 13.56 MHz frequency). 6.3.2 IDLE state Description: In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands. State exit conditions and transitions: The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA. (VAR0000126-189). 6.2 Frequency The frequency, f_c of the RF operating field shall be 13,56 MHz $\pm$ 7 kHz. (VAR0000072-125).
9[e]	wherein the outputting of the voice call signal	The Accused Products output the voice call signal over a wireless network in a radio frequency range different than a radio frequency range in which the RFID signal is output.

⁸ <https://developer.apple.com/documentation/corenfc/cardsession/>

	comprises outputting the voice call signal over a wireless network in a radio frequency range different than a radio frequency range in which the RFID signal is output.	For example, the Accused Products output a voice call signal (<i>e.g.</i> , cellular and/or Wi-Fi) for transmission over a wireless network in a radio frequency range (<i>e.g.</i> , 850 MHz, 3G UMTS in 1900 MHz, 2100 MHz, 4G LTE and LTE Advanced in bands 2, 3, 4, 5, 7, 8, 13, and Wi-Fi in 2.4 GHz and 5 GHz bands) different than a radio frequency range in which the RFID signal is output (<i>e.g.</i> , 12.56 MHz). (VAR00000639-1074).
10	The method of claim 9, wherein the RFID signal includes RFID data comprising a security key.	The Accused Products perform the method claim 9, wherein the RFID signal includes RFID data comprising a security key. For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Product may then be used to unlock the hotel room and/or car. (VAR0000003-09). The data includes, <i>e.g.</i>, data from applets within the Secure Element.

	Secure Element The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus. NFC controller As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server. (VAR0001075 at 1209). Privacy and security Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted. (VAR VAR0001075 at 12222). The keys include, e.g., keys stored on applets in the Secure Element.
--	---

		Privacy and security Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted. (VAR VAR0001075 at 12222).
11	The method of claim 10, wherein the security key comprises a door key.	The Accused Products perform the method of claim 10, wherein the security key comprises a door key. For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Product may then be used to unlock the hotel room and/or car. (VAR00000003-09). The keys include, e.g., keys stored on applets in the Secure Element. Privacy and security Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted. (VAR VAR0001075 at 12222).
12	The method of claim 11, wherein the door key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key.	The Accused Products perform the method of claim 11, wherein the door key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key. For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Product may then be used to unlock the hotel room and/or car. (VAR00000003-09).

	interior door key, and a motor vehicle door key.	The keys include, e.g., keys stored on applets in the Secure Element. Privacy and security Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted. (VAR VAR0001075 at 12222).
13	The method of claim 10, wherein the instructions are further configured to cause the mobile communication device to facilitate provision of the RFID data to the mobile communication device.	The Accused Products perform the method of claim 10, wherein the instructions are further configured to cause the mobile communication device to facilitate provision of the RFID data to the mobile communication device. For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments with Apple Pay using the Accused Products. (VAR0001075-1293 at 1210-211). Apple also directs and controls the provisioning of keys and passes. (VAR0000003-09).

		Credit, debit, and prepaid cards Card provisioning security overview When a user adds a credit, debit, or prepaid card (including store cards) to Apple Wallet, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer determines whether to approve adding the card to Apple Wallet. As part of the card provisioning process, Apple Pay uses three server-side calls to send and receive communication with the card issuer or network: • Required Fields • Check Card • Link and Provision The card issuer or network uses these calls to verify, approve, and add cards to Apple Wallet. These client-server sessions use TLS 1.2 to transfer the data. Full card numbers aren't stored on the device or on Apple Pay servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from most credit or debit card numbers; the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is never stored on Apple Pay servers or backed up to iCloud, and it is isolated from iOS, iPadOS, and watchOS devices and from Mac computers with Touch ID. Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone, or within a card issuer's iPhone app. Adding a card to Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch.

		Adding credit or debit cards manually To add a card manually, the name, card number, expiration date, and CVV are used to facilitate the provisioning process. From within Settings, Apple Wallet, or the Apple Watch app, users can enter that information either by typing or by using the device's camera. When the camera captures the card information, Apple attempts to populate the name, card number, and expiration date. The photo is never saved to the device or stored in the photo library. After all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are then encrypted and sent to the Apple Pay server. If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the terms and conditions, Apple sends the ID of the terms that were accepted as well as the CVV to the Link and Provision process. Additionally, as part of the Link and Provision process, Apple shares information from the device with the card issuer or network. This includes information about (a) the user's iTunes and App Store account activity (for example, whether the user has a long history of transactions within iTunes), (b) the user's device (for example, the phone number, name, and model of the user's device plus any companion Apple device necessary to set up Apple Pay), and (c) the user's approximate location at the time the user adds their card (if the user has Location Services enabled). Using this information, the card issuer determines whether to approve adding the card to Apple Pay. As the result of the Link and Provision process, two things occur: • The device begins to download the Apple Wallet pass file representing the credit or debit card. • The device begins to bind the card to the Secure Element. The pass file contains URLs to download card art, metadata about the card such as contact information, the related issuer's app, and supported features. It also contains the pass state, which includes information such as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whether additional verification is required before the card can make payments with Apple Pay.
--	--	--

14	The method of claim 13, wherein facilitating provisioning of the RFID data to the mobile communication device includes facilitating provision of at least a signaling attribute associated with the outputting of the RFID data.	The Accused Products perform the method of claim 13, wherein facilitating provisioning of the RFID data to the mobile communication device includes facilitating provision of at least a signaling attribute associated with the outputting of the RFID data. For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments with Apple Pay using the Accused Devices, and Apple further directs, controls, and specifies the communication and security protocols associated with making contactless payments via Apple Pay. (VAR0001075-1293 at 1208-09). Apple also directs and controls the provisioning of keys and passes. (VAR0000003-09). NFC controller The NFC controller handles Near Field Communication protocols and routes communication between the Application Processor and the Secure Element, and between the Secure Element and the point-of-sale terminal. NFC controller As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.
----	---	--

15	The method of claim 9, wherein the mobile communication device is one of a wireless mobile phone and a personal digital assistant equipped with communication capability. For example the Accused Products are wireless mobile phones and/or personal digital assistants equipped with communication capability. For example the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, via LTE, CDMA, UMTS, GSM and/or 5G), and/o audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling). (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, Via LTE via LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling). (VAR0000639-1074).	The Accused Products perform the method of claim 9, wherein the mobile communication device is one of a wireless mobile phone and a personal digital assistant equipped with communication capability. For example the Accused Products are wireless mobile phones and/or personal digital assistants equipped with communication capability. For example the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, via LTE, CDMA, UMTS, GSM and/or 5G), and/o audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling). (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, Via LTE via LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling). (VAR0000639-1074).
16[a]	A mobile communication device comprising:	To the extent that the claim's preamble is determined to be a limitation or otherwise limiting, the Accused Products are mobile communication devices. For example, the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, via LTE, CDMA, UMTS, and/or GSM), and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling), as well as RFID communication (<i>e.g.</i>, via NFC). (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, Via LTE, LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling), as well as RFID communication (<i>e.g.</i>, via RFID/NFC, including via Apple Pay, which uses NFC technology between the device and the payment terminal). (VAR0000639-1074).

For example, the iPhone as a whole is capable of entering two different modes, including a telephony mode and an RFID/NFC mode. A user can affirmatively launch the telephony and/or RFID/NFC modes, and/or the iPhone enters the telephony and/or RFID/NFC mode when its received the relevant signal (e.g., an incoming call or detecting an RFID reader), as shown below.



		
		When an RFID reader signal is detected by the mobile communications device, the user must first address how to respond to that signal telephony controls, and vice versa.
16[b]	communication circuitry configured to output voice call signals in a first radio frequency range over a wireless network and output radio frequency identification (RFID) signals in a second radio frequency range, which is different than the first radio frequency range;	The Accused Products have communication circuitry configured to output voice call signals in a first radio frequency range over a wireless network and output radio frequency identification (RFID) signals in a second radio frequency range, which is different than the first radio frequency range. For example, the iPhone 7 has communication circuitry including the components identified by their chip markings as: NXP 67V04 NF Controller, Qualcomm WTR4905 Transceiver, Qualcomm WTR3925 Transceiver, and Murata 339S00199 Wi-Fi/Bluetooth Module. (VAR0000504-518). The communication circuitry of the iPhone 7 is configured to output voice call signals in a first radio frequency range over a wireless network (e.g., 850, 900, 1800, 1900 Mhz for GSM/EDGE). (VAR0000849-855). The communication circuitry of the iPhone 7 is also configured to output voice call signals that are signals for audio calling services that use a Wi-Fi connection (in the 2.4 GHz and 5 GHz frequency bands) or a high-speed cellular connection (e.g., FaceTime Audio, Voice over LTE

	(VoLTE), and Wi-Fi calling). (VAR00000849-855). The communication circuitry of the iPhone 7 is configured to output RFID signals, because the iPhone is capable of Near Field Communication (NFC), as evidenced by, <i>e.g.</i>, technical specifications of the iPhone 7 that specify NFC with card or tag emulation feature (Apple Pay). (VAR00000849-855). NFC is a RFID-based technology for data exchange using radio waves. NFC is a subset within the family of RFID technology. (VAR00000026-42) (“RFID is the process by which items are uniquely identified using radio waves, and NFC is a specialized subset within the family of RFID technology.”); (VAR00000043-53) (“Hierarchically, NFC is a subset of RFID.”)). The communication circuitry of the iPhone 7, acting in accordance with ISO/IEC 14443 and/or ISO/IEC 7816-4, outputs RFID signals in a second radio frequency range (<i>e.g.</i>, 13.56 MHz frequency), which is different than the first radio frequency range. (VAR00000072-125). As further examples, the Accused Products, including iPhone models and Apple Watch models, each have communication circuitry, including, for each Accused Product, the components specified in Column D of Appendix D, configured to output voice call signals in a first radio frequency range over a wireless network (<i>e.g.</i>, 850 MHz for GSM/EDGE/UMTS, and/or LTE band 1, 2, 3) and/or output voice call signals that are signals for audio calling services that use a Wi-Fi connection (<i>e.g.</i>, FaceTime Audio, Wi-Fi calling in 2.4 GHz). (VAR00000639-1074). The communication circuitry of the Accused Products is also configured to output RFID signals, because the Accused Products are capable of Near Field Communication (NFC), as evidenced by, <i>e.g.</i>, technical specifications of the Accused Products that specify NFC with card or tag emulation feature (Apple Pay). (VAR00000639-1074). NFC is a RFID-based technology for data exchange using radio waves. NFC is a subset within the family of RFID technology. (VAR00000026-42) (“RFID is the process by which items are uniquely identified using radio waves, and NFC is a specialized subset within the family of RFID technology.”); (VAR00000043-53) (“Hierarchically, NFC is a subset of RFID.”)). The communication circuitry of the Accused Products, acting in accordance with ISO/IEC 14443 and/or ISO/IEC 7816-4, outputs RFID signals in a second radio frequency range (<i>e.g.</i>, 13.56 MHz frequency), which is different than the first radio frequency range. (VAR00000072-125). These components specified in Appendix D are incorporated here by reference. • For example, as specified in Appendix D, the iPhone 6 has communication circuitry, including the components identified by their chip markings as: Qualcomm WTR1625L RF Transceiver, NXP 65V10 NFC module, and Murata 339S0228 Wi-Fi Module. (VAR00000821-827). The communication circuitry of the iPhone 6 is configured to output voice call signals in a first
--	--

	radio frequency range over a wireless network (<i>e.g.</i>, 850, 900, 1800, 1900 Mhz for GSM/EDGE). The communication circuitry of the iPhone 6 is also configured to output voice call signals that are signals for audio calling services that use a Wi-Fi connection (in the 2.4 GHz and 5 GHz frequency bands) or a high-speed cellular connection (<i>e.g.</i>, FaceTime Audio, Voice over LTE (VoLTE), and Wi-Fi calling). (VAR0000821-827). The communication circuitry of the iPhone 6 is configured to output RFID signals, because the iPhone is capable of Near Field Communication (NFC), as evidenced by, <i>e.g.</i>, technical specifications of the iPhone 7 that specify NFC with card or tag emulation feature (Apple Pay). (VAR0000821-827). NFC is a subset within the family of RFID technology. (VAR0000026-42) (“RFID is the process by which items are uniquely identified using radio waves, and NFC is a specialized subset within the family of RFID technology.”); (VAR0000043-53) (“Hierarchically, NFC is a subset of RFID.”)). The communication circuitry of the iPhone 6, acting in accordance with ISO/IEC 14443 and/or ISO/IEC 7816-4, outputs RFID signals in a second radio frequency range (<i>e.g.</i>, 13.56 MHz frequency), which is different than the first radio frequency range. (VAR0000072-125). To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (<i>e.g.</i>, emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (<i>e.g.</i>, through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (<i>e.g.</i>, mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions).
16[c]	The Accused Products have processing circuitry. For example, the iPhone 7 has processing circuitry (<i>e.g.</i>, A10 fusion chip, NXP 67V04 NFC controller, Secure Element). (VAR0000849-55).

		As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal processing circuitry, including, for each Accused Product, the components specified in Column B of Appendix D (processing circuitry). These components specified in Appendix D are incorporated here by reference. • For example, as specified in Appendix D, the iPhone 6 has processing circuitry (<i>e.g.</i>, A8 chip, NXP 65V10 NFC module, Secure Element). (VAR0000432-438). To the extent this limitation is not literally met by the Accused Products because the processing circuitry is not a single chip, the Accused Products' processing circuitry is insubstantially different from, and equivalent to, this limitation. The Accused Products' processing circuitry performs substantially the same function (<i>i.e.</i>, executing instructions), in substantially the same way (<i>i.e.</i>, the executing instructions stored in a storage medium), to achieve substantially the same result (<i>i.e.</i>, the instructions configured to cause the mobile device to perform the steps below) as the claimed processing circuitry.
16[d]	a storage medium including instructions, which, when executed by the processing circuitry cause the mobile communication device to:	The Accused Products have a storage medium including instructions, which, when executed by the processing circuitry cause the mobile communication device to perform the instructions below. For example, the iPhone 7 has a storage medium (<i>e.g.</i>, SK Hynix 32 GB flash memory, NXP 67V04 NFC Controller, Secure Element), that includes instructions (<i>e.g.</i>, iOS operating system, RFID/NFC protocols, Secure Element applets), which when executed by the processing circuitry (<i>e.g.</i>, A10 Fusion chip, NXP 67V04 NFC Controller, Secure Element) cause the iPhone to perform the instructions discussed below. (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal circuitry and components, including, for each Accused Product, the components specified in Appendix D, including processing circuitry (specified in Column B), a storage medium (specified in Column C), and instructions (specified in Column G), configured to cause the Accused Product to perform the instructions discussed below. These components specified in Appendix D are incorporated here by reference. • For example, as specified in Appendix D, the iPhone 6 has a storage medium (<i>e.g.</i>, SanDisk SDMLBCB2 128GB (16GB) NAND flash, NXP 65V10 NFC module, Secure Element), that includes instructions (<i>e.g.</i>, iOS operating system, RFID/NFC protocols, Secure Element

	applets), which when executed by the processing circuitry (e.g., A8 chip, NXP 65V10 NFC module, Secure Element), cause the iPhone to perform the instructions discussed below. (VAR0000432-438). To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (e.g., emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (e.g., through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (e.g., mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions).
16[e]	monitor for a proximal presence of an RFID reader external to the mobile communication device via the communication circuitry, the monitoring comprising determining the mobile communication device is in an operational space of the RFID reader based on an RFID probing signal received by the mobile device from the RFID reader. For example, the Accused RFID/NFC features (e.g. Apple Pay) conform to the EMV Contactless standard, which incorporates the ISO/IEC 14443 standard for proximity cards. (VAR0000001-02). The Accused Products act as a proximity card (PICC) as defined by the ISO/IEC 14443 standard. The Accused Products use signals and commands according to ISO/IEC 14443 and/or ISO/IEC 7816-4.⁹ For example, in accordance with ISO/IEC 14443, the Accused Products monitor for the proximal presence of an RFID reader external to the mobile communication device (e.g., a contactless point-of-sale terminal) via the communication circuitry (e.g., NXP 67V04 NFC Controller) by listening for commands and recognizing Request (REQA) and Wake Up (WUPA) commands from the RFID reader. The Accused Products determine that they are in an operational space (e.g., operating field) of the RFID reader (e.g., proximity coupling device “PCD”) based on an RFID probing signal (e.g., REQA and WUPA commands) received by the mobile device from the RFID reader.

⁹ <https://developer.apple.com/documentation/corenfc/cardsession/>

	3.5 PICC <i>contactless integrated circuit card (3.3)</i> or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device Note 1 to entry: Commonly called a proximity card. (VAR0000054-71). 5.2.1 Polling In order to detect PICCs which are in the operating field, the PCD shall send repeated request commands. The PCD shall send REQA (or WUPA) and REQB (or WUPB) in any sequence using an equal or configurable duty cycle when polling Type A and Type B. In addition, the PCD may send other commands as described in Annex C. 6.4.1 REQA and WUPA commands The REQA and WUPA commands are sent by the PCD to probe the field for PICCs of Type A. They are transmitted within a short frame. See Figure 7 to check in which cases PICCs actually have to answer to these respective commands. Particularly, the WUPA command is sent by the PCD to put PICCs which have entered HALT state back into READY* state. They shall then participate in further anticollision and selection procedures. (VAR0000126-189). The Communication Circuitry for each Accused Product is specified in Column D of Appendix D and is incorporated herein by reference.
16[f]	output a voice call signal for transmission over a wireless network via the communication circuitry in the first radio frequency range; and For example, the iPhone 7 outputs a voice call signal (e.g., cellular and/or Wi-Fi) for transmission over a wireless network via the communication circuitry (e.g., Qualcomm WTR4905 Transceiver, Qualcomm WTR3925 Transceiver, Murata 339S00199 Wi-Fi/Bluetooth Module) in the first radio

	frequency range (<i>e.g.</i>, 850 MHz, 3G UMTS in 1900 MHz, 2100 MHz, 4G LTE and LTE Advanced in bands 2, 3, 4, 5, 7, 8, 13, and Wi-Fi in 2.4 GHz and 5 GHz bands). (VAR0000504-518). As further examples, the Accused Products, including iPhone models and Apple Watch models, each have communication circuitry, including, for each Accused Product, the components specified in Column D Appendix D. The Accused Products output a voice call signal for transmission over a wireless network via the communication circuitry in the first radio frequency range. These components specified in Appendix D are incorporated here by reference. • For example, as specified in Appendix D, the iPhone 6 outputs a voice call signal (<i>e.g.</i>, cellular and/or Wi-Fi) for transmission over a wireless network via the communication circuitry (<i>e.g.</i>, Qualcomm WTR1625L RF Transceiver, NXP 65V10 NFC module, and Murata 339S0228 Wi-Fi Module) in the first radio frequency range (<i>e.g.</i>, 850 MHz, 3G UMTS in 1900 MHz, 2100 MHz, 4G LTE and LTE Advanced in bands 2, 3, 4, 5, 7, 8, 13, and Wi-Fi in 2.4 GHz and 5 GHz bands) (VAR0000432-438; VAR0000821-827). To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (<i>e.g.</i>, emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (<i>e.g.</i>, through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (<i>e.g.</i>, mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions).
16[g]	The Accused Products output an RFID signal via the communication circuitry in response to detection of the proximal presence of the RFID reader external to the mobile communication device based upon receipt of the RFID probing signal, wherein the RFID signal is output in the second radio frequency range. output an RFID signal via the communication circuitry in response to detection of the proximal presence of the RFID reader external to the mobile communication

	device based upon receipt of the RFID probing signal, wherein the RFID signal is output in the second radio frequency range.	The Accused Products use signals and commands according to ISO/IEC 14443 and/or ISO/IEC 7816-4.¹⁰ For example, the iPhone 7, acting in accordance with ISO/IEC 14443, outputs an RFID signal (e.g., Answer to Request or ATQA) via the communication circuitry (e.g., NXP 67V04 NFC Controller) in response to detection of the proximal presence (e.g., IDLE state exit) of the RFID reader external to the mobile communication device based upon receipt of the RFID probing signal (e.g., REQA and WUPA commands). (VAR00000849-855). The RFID signal is output in the second radio frequency range (e.g., 13.56 MHz frequency). The Communication Circuitry for each Accused Product is specified in Column D of Appendix D and is incorporated herein by reference. 6.3.2 IDLE state Description: In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands. State exit conditions and transitions: The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA. (VAR0000126-189). 6.2 Frequency The frequency, f_c of the RF operating field shall be 13,56 MHz $\pm$ 7 kHz. (VAR0000072-125).
17	The mobile communication device of claim 16, wherein	The Accused Products embody the device of claim 16, wherein the RFID signal includes RFID data comprising a selected one of a security key and an identifier. For example, credit cards can be added

¹⁰ <https://developer.apple.com/documentation/corenfc/cardsession/>

	the RFID signal includes RFID data comprising a selected one of a security key and an identifier.	to Apple Pay, and the Accused Products may then be used to make contactless payments using those credit cards. In addition, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Products may then be used to unlock the hotel room and/or car. (VAR000003-09; VAR0000020-22; VAR0001075-1293). The data includes, e.g., data from applets within the Secure Element. Secure Element The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus. NFC controller As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server. (VAR0001075 at 1209).
--	--	---

		Privacy and security Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted. (VAR VAR0001075 at 12222). The keys include, e.g., keys stored on applets in the Secure Element.
		Privacy and security Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted. (VAR VAR0001075 at 12222).
18	The mobile communication device of claim 17, wherein the security key comprises a door key.	The Accused Products embody the device of claim 17, wherein the security key comprises a door key. For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Products may then be used to unlock the hotel room and/or car. (VAR00000003-09; VAR00000020-22; VAR0001075-1293). The keys include, e.g., keys stored on applets in the Secure Element.

		Privacy and security Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted. (VAR VAR0001075 at 12222).
19	The mobile communication device of claim 18, wherein the door key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key.	The Accused Products embody the device of claim 18, wherein the door key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key. For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Products may then be used to unlock the hotel room and/or car. (VAR0000003-09). The keys include, e.g., keys stored on applets in the Secure Element.
20	The mobile communication device of claim 17, wherein the identifier comprises a	Privacy and security Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted. (VAR VAR0001075 at 12222). The Accused Products embody the device of claim 17, wherein the identifier comprises a selected one of a social security number, a driver's license number, an affinity program account number, and a

	selected one of a social security number, a driver's license number, an affinity program account number, and a credit card number.	credit card number. For example, credit cards can be added to Apple Pay, and the Accused Products may then be used to make contactless payments using those credit cards. (VAR0000020-22, VAR0001075-1293).
21	The mobile communication device of claim 17, wherein the instructions are further configured to cause the mobile communication device to facilitate a user in selecting the RFID data from a plurality of RFID data. For example, multiple payment cards can be added to Apple Pay, and the Accused Products may then be used to select a card to make a contactless payment. (VAR0000020-22).	The Accused Products embody the device of claim 17, wherein the instructions are further configured to cause the mobile communication device to facilitate a user in selecting the RFID data from a plurality of RFID data. For example, multiple payment cards can be added to Apple Pay, and the Accused Products may then be used to select a card to make a contactless payment. (VAR0000020-22).
22	The mobile communication device of claim 17, wherein the instructions are further configured to cause the mobile communication device to facilitate provision of the RFID data to the mobile communication device.	The Accused Products embody the device of claim 17, wherein the instructions are further configured to cause the mobile communication device to facilitate provision of the RFID data to the mobile communication device. For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments with Apple Pay using the Accused Products. (VAR0001075-1293 at 1210-211). Apple also directs and controls the provisioning of keys and passes. (VAR0000003-09).

		Credit, debit, and prepaid cards Card provisioning security overview When a user adds a credit, debit, or prepaid card (including store cards) to Apple Wallet, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer determines whether to approve adding the card to Apple Wallet. As part of the card provisioning process, Apple Pay uses three server-side calls to send and receive communication with the card issuer or network: • Required Fields • Check Card • Link and Provision The card issuer or network uses these calls to verify, approve, and add cards to Apple Wallet. These client-server sessions use TLS 1.2 to transfer the data. Full card numbers aren't stored on the device or on Apple Pay servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from most credit or debit card numbers; the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is never stored on Apple Pay servers or backed up to iCloud, and it is isolated from iOS, iPadOS, and watchOS devices and from Mac computers with Touch ID. Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone, or within a card issuer's iPhone app. Adding a card to Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch.

		Adding credit or debit cards manually To add a card manually, the name, card number, expiration date, and CVV are used to facilitate the provisioning process. From within Settings, Apple Wallet, or the Apple Watch app, users can enter that information either by typing or by using the device's camera. When the camera captures the card information, Apple attempts to populate the name, card number, and expiration date. The photo is never saved to the device or stored in the photo library. After all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are then encrypted and sent to the Apple Pay server. If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the terms and conditions, Apple sends the ID of the terms that were accepted as well as the CVV to the Link and Provision process. Additionally, as part of the Link and Provision process, Apple shares information from the device with the card issuer or network. This includes information about (a) the user's iTunes and App Store account activity (for example, whether the user has a long history of transactions within iTunes), (b) the user's device (for example, the phone number, name, and model of the user's device plus any companion Apple device necessary to set up Apple Pay), and (c) the user's approximate location at the time the user adds their card (if the user has Location Services enabled). Using this information, the card issuer determines whether to approve adding the card to Apple Pay. As the result of the Link and Provision process, two things occur: • The device begins to download the Apple Wallet pass file representing the credit or debit card. • The device begins to bind the card to the Secure Element. The pass file contains URLs to download card art, metadata about the card such as contact information, the related issuer's app, and supported features. It also contains the pass state, which includes information such as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whether additional verification is required before the card can make payments with Apple Pay.
--	--	--

23	The mobile communication device of claim 22, wherein the instructions are further configured to cause the mobile communication device to include provisioning of at least a signaling attribute associated with the RFID data in the form of a radio frequency signal.	The Accused Products embody the device of claim 22, wherein the instructions are further configured to cause the mobile communication device to include provisioning of at least a signaling attribute associated with the RFID data in the form of a radio frequency signal. For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments with Apple Pay using the Accused Devices, and Apple further directs, controls, and specifies the communication and security protocols associated with making contactless payments via Apple Pay. (VAR0001075-1293 at 1208-09). Apple also directs and controls the provisioning of keys and passes. (VAR0000003-09). NFC controller The NFC controller handles Near Field Communication protocols and routes communication between the Application Processor and the Secure Element, and between the Secure Element and the point-of-sale terminal. NFC controller As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.
----	---	---

24	The mobile communication device of claim 17, wherein the RFID data includes information identifying a user.	The Accused Products embody the device of claim 17, wherein the RFID data includes information identifying a user. For example, identity cards such as employee badges can be added to Apple Wallet, and the Accused Devices may then be used to access locations in the office building where the physical badge is accepted. (VAR0000018-19). The data includes, e.g., data from applets within the Secure Element. Secure Element The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus. NFC controller As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server. (VAR0001075 at 1209).
----	--	--

25	The mobile communication device of claim 16, wherein the mobile communication device is one of a wireless mobile phone and a personal digital assistant equipped with communication capability. For example the Accused Products are wireless mobile phones and/or personal digital assistants equipped with communication capability. For example the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, via LTE, CDMA, UMTS, and/or GSM), and/o audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling). (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, Via LTE via LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling). (VAR0000639-1074).	The Accused Produced embody the device of claim 16, wherein the mobile communication device is one of a wireless mobile phone and a personal digital assistant equipped with communication capability. For example the Accused Products are wireless mobile phones and/or personal digital assistants equipped with communication capability. For example the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, via LTE, CDMA, UMTS, and/or GSM), and/o audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling). (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, Via LTE via LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling). (VAR0000639-1074).
26[a]	A mobile communication device comprising:	To the extent that the claim's preamble is determined to be a limitation or otherwise limiting, the Accused Products are mobile communication devices. For example, the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, via LTE, CDMA, UMTS, and/or GSM), and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling), as well as RFID communication (<i>e.g.</i>, via NFC). (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, Via LTE, LTE, CDMA, UMTS, GSM and/or %G) and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling), as well as RFID communication (<i>e.g.</i>, via RFID/NFC, including via Apple Pay, which uses NFC technology between the device and the payment terminal). (VAR0000639-1074).

For example, the iPhone as a whole is capable of entering two different modes, including a telephony mode and an RFID/NFC mode. A user can affirmatively launch the telephony and/or RFID/NFC modes, and/or the iPhone enters the telephony and/or RFID/NFC mode when its received the relevant signal (e.g., an incoming call or detecting an RFID reader), as shown below.



		 
		When an RFID reader signal is detected by the mobile communications device, the user must first address how to respond to that signal telephony controls, and vice versa.
26[b]	communication circuitry configured to transmit voice call signals in a first radio frequency range over a wireless network;	The Accused Products have communication circuitry configured to transmit voice call signals in a first radio frequency range over a wireless network. For example, the iPhone 7 has communication circuitry including the components identified by their chip markings as: NXP 67V04 NF Controller, Qualcomm WTR4905 Transceiver, Qualcomm WTR3925 Transceiver, and Murata 339S00199 Wi-Fi/Bluetooth Module. (VAR0000504-518) The communication circuitry of the iPhone 7 is configured to transmit voice call signals in a first radio frequency range over a wireless network (<i>e.g.</i>, 850, 900, 1800, 1900 Mhz for <i>e.g.</i> GSM/EDGE and/or voice call signals that are signals for audio calling services that use a Wi-Fi connection (<i>e.g.</i>, in the 2.4 GHz and 5 GHz frequency bands), or a high-speed cellular connection (<i>e.g.</i>, FaceTime Audio, Voice over LTE (VoLTE), and Wi-Fi calling)). (VAR0000849-855).

	As further examples, the Accused Products, including iPhone models and Apple Watch models, each have communication circuitry, including, for each Accused Product, the components specified in Column D of Appendix D, configured to output voice call signals in a first radio frequency range over a wireless network (<i>e.g.</i>, 850 MHz for GSM/EDGE/UMTS, and/or LTE band 1, 2, 3 and/or output voice call signals that are signals for audio calling services that use a Wi-Fi connection (<i>e.g.</i>, FaceTime Audio, Wi-Fi calling in 2.4 GHz)). (VAR0000639-1074). These components specified in Appendix D are incorporated here by reference. For example, as specified in Appendix D, the iPhone 6 has communication circuitry, including the components identified by their chip markings as: Qualcomm WTR1625L RF Transceiver, NXP 65V10 NFC module, and Murata 339S0228 Wi-Fi Module. (VAR0000821-827). The communication circuitry of the iPhone 6 is configured to transmit voice call signals in a first radio frequency range over a wireless network (<i>e.g.</i>, 850, 900, 1800, 1900 Mhz for <i>e.g.</i> GSM/EDGE and/or voice call signals that are signals for audio calling services that use a Wi-Fi connection (in the 2.4 GHz and 5 GHz frequency bands) or a high-speed cellular connection (<i>e.g.</i>, FaceTime Audio, Voice over LTE (VoLTE), and Wi-Fi calling)). (VAR0000821-827). To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (<i>e.g.</i>, emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (<i>e.g.</i>, through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (<i>e.g.</i>, mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions).
26[c]	The Accused Products have processing circuitry. For example, the iPhone 7 has processing circuitry (<i>e.g.</i>, A10 fusion chip, NXP 67V04 NFC controller, Secure Element). (VAR0000849-855).

	As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal processing circuitry, including, for each Accused Product, the components specified in Column B of Appendix D (processing circuitry). These components specified in Appendix D are incorporated here by reference. For example, as specified in Appendix D, the iPhone 6 has processing circuitry (<i>e.g.</i>, A8 chip, NXP 65V10 NFC module, Secure Element). (VAR0000821-826). To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (<i>e.g.</i>, emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (<i>e.g.</i>, through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (<i>e.g.</i>, mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions).
26[d]	The Accused Products have a memory storing instructions, which, when executed by the processing circuitry cause the mobile communication device to perform the instructions below. For example, the iPhone 7 has a memory (<i>e.g.</i>, SK Hynix 32 GB flash memory, NXP 67V04 NFC Controller, Secure Element), that includes instructions (<i>e.g.</i>, iOS operating system, RFID/NFC protocols, Secure Element applets), which when executed by the processing circuitry (<i>e.g.</i>, A10 Fusion chip, NXP 67V04 NFC Controller, Secure Element) cause the iPhone to perform the instructions discussed below. (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal circuitry and components, including, for each Accused Product, the components specified in Appendix D, including processing circuitry (specified in Column B), a memory (specified in Column C), and instructions (specified in Column G), configured to cause the Accused Product to perform the instructions discussed below. These components specified in Appendix D are incorporated here by reference.

	For example, as specified in Appendix D, the iPhone 6 has a memory (e.g., SanDisk SDMLB2 128GB (16GB) NAND flash, NXP 65V10 NFC module, Secure Element), that includes instructions (e.g., iOS operating system, RFID/NFC protocols, Secure Element applets), which when executed by the processing circuitry (e.g., A8 chip, NXP 65V10 NFC module, Secure Element), cause the iPhone to perform the instructions discussed below. (VAR0000432-448). To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (e.g., emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (e.g., through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (e.g., mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions).
26[e]	The Accused Products monitor for a proximal presence of a radio frequency identification (RFID) reader external to the mobile communication device via the communication circuitry, the monitoring comprising determining the mobile communication device is in an operational space of the RFID reader based on an RFID probing signal received by the mobile communication device from the RFID reader. For example, the Accused RFID/NFC features (e.g. Apple Pay) conform to the EMV Contactless standard, which incorporates the ISO/IEC 14443 standard for proximity cards. (VAR0000001-02). The Accused Products act as a proximity card (PICC) as defined by the ISO/IEC 14443 standard. The Accused Products use signals and commands according to ISO/IEC 14443 and/or ISO/IEC 7816-4.¹¹ For example, in accordance with ISO/IEC 14443, the Accused Products monitor for a proximal presence of an RFID reader external to the mobile communication device (e.g., a contactless point-of-sale terminal) via the communication circuitry (e.g., NXP 67V04 NFC Controller) by listening for commands and recognizing Request (REQA) and Wake Up (WUPA) commands from the RFID reader.

¹¹ <https://developer.apple.com/documentation/corenfc/cardsession/>

	received by the mobile communication device from the RFID reader;	The Accused Products determine that they are in an operational space (e.g., operating field) of the RFID reader (e.g., proximity coupling device “PCD”) based on an RFID probing signal (e.g., REQA and WUPA commands) received by the mobile device from the RFID reader. 3.5 PICC <i>contactless integrated circuit card (3.3)</i> or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device Note 1 to entry: Commonly called a proximity card. (VAR0000054-71). 5.2.1 Polling In order to detect PICCs which are in the operating field, the PCD shall send repeated request commands. The PCD shall send REQA (or WUPA) and REQB (or WUPB) in any sequence using an equal or configurable duty cycle when polling Type A and Type B. In addition, the PCD may send other commands as described in Annex C. 6.4.1 REQA and WUPA commands The REQA and WUPA commands are sent by the PCD to probe the field for PICCs of Type A. They are transmitted within a short frame. See Figure 7 to check in which cases PICCs actually have to answer to these respective commands. Particularly, the WUPA command is sent by the PCD to put PICCs which have entered HALT state back into READY* state. They shall then participate in further anticollision and selection procedures. (VAR0000126-189). The Communication Circuitry for each Accused Product is specified in Column D of Appendix D and is incorporated herein by reference.
26[f]	in response to determining the mobile communication	The Accused Products in response to determining the mobile communication device is in the operational space of the RFID reader based upon the receipt of the RFID probing signal, output an

	device is in the operational space of the RFID reader based upon the receipt of the RFID probing signal, output an RFID signal via the communication circuitry in a second radio frequency range that is different than the first radio frequency range; and	RFID signal via the communication circuitry in a second radio frequency range that is different than the first radio frequency range. The Accused Products use signals and commands according to ISO/IEC 14443 and/or ISO/IEC 7816-4.¹² For example, the iPhone 7, acting in accordance with ISO/IEC 14443, outputs an RFID signal (e.g., Answer to Request or ATQA) via the communication circuitry (e.g., NXP 67V04 NFC Controller) in response to detection of the proximal presence (e.g., IDLE state exit) of the RFID reader external to the mobile communication device based upon receipt of the RFID probing signal (e.g., REQA and WUPA commands). (VAR0000849-855). The RFID signal is output in the second radio frequency range (e.g., 13.56 MHz frequency) that is different than the first radio frequency range. The Communication Circuitry for each Accused Product is specified in Column D of Appendix D and is incorporated herein by reference. 6.3.2 IDLE state Description: In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands. State exit conditions and transitions: The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA. (VAR0000126-189). 6.2 Frequency The frequency, f_c of the RF operating field shall be 13,56 MHz $\pm$ 7 kHz. (VAR0000072-125).
--	---	---

¹² <https://developer.apple.com/documentation/corenfc/cardsession/>

26[g]	transmit a voice call signal to another mobile communication device via the communication device via the communication circuitry at least in part over a wireless network in the first radio frequency range. For example, the iPhone 7 transmits a voice call signal (<i>e.g.</i>, cellular and/or Wi-Fi) to another mobile communication device via the communication circuitry (<i>e.g.</i>, Qualcomm WTR4905 Transceiver, Qualcomm WTR3925 Transceiver, Murata 339S00199 Wi-Fi/Bluetooth Module) at least in part over a wireless network in the first radio frequency range (<i>e.g.</i>, 850 MHz, 3G UMTS in 1900 MHz, 2100 MHz, 4G LTE and LTE Advanced in bands 2, 3, 4, 5, 7, 8, 13, and Wi-Fi in 2.4 GHz and 5 GHz bands). (VAR0000849-855; VAR0000504-518). As further examples, the Accused Products, including iPhone models and Apple Watch models, each have communication circuitry, including, for each Accused Product, the components specified in Column D Appendix D. The Accused Products transmit a voice call signal (<i>e.g.</i> cellular and/or Wi-Fi) to another mobile communication device via the communication circuitry at least in part over a wireless network in the first radio frequency range. These components specified in Appendix D are incorporated here by reference. • For example, as specified in Appendix D, the iPhone 6 outputs a voice call signal (<i>e.g.</i>, cellular and/or Wi-Fi) for transmission over a wireless network via the communication circuitry (<i>e.g.</i>, Qualcomm WTR1625L RF Transceiver, NXP 65V10 NFC module, and Murata 339S0228 Wi-Fi Module) in the first radio frequency range (<i>e.g.</i>, 850 MHz, 3G UMTS in 1900 MHz, 2100 MHz, 4G LTE and LTE Advanced in bands 2, 3, 4, 5, 7, 8, 13, and Wi-Fi in 2.4 GHz and 5 GHz bands) (VAR0000432-448; VAR0000821-827). To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (<i>e.g.</i>, emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (<i>e.g.</i>, through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (<i>e.g.</i>, mobile communications device capable
-------	--

	of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions).
27	The mobile communication device of claim 26, wherein the RFID signal includes RFID data comprising a security key. The Accused Products embody the device of claim 26, wherein the RFID signal includes RFID data comprising a security key. For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Product may then be used to unlock the hotel room and/or car. (VAR0000003-09). The data includes, e.g., data from applets within the Secure Element. Secure Element The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus. NFC controller As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server. (VAR0001075 at 1209).

		The keys include, e.g., keys stored on applets in the Secure Element. Privacy and security Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted. (VAR VAR0001075 at 12222).
28	The mobile communication device of claim 27, wherein the security key comprises a door key.	The Accused Products embody the device of claim 27, wherein the security key comprises a door key. For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Product may then be used to unlock the hotel room and/or car. (VAR00000003-09). The keys include, e.g., keys stored on applets in the Secure Element. Privacy and security Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted. (VAR VAR0001075 at 12222).
29	The mobile communication device of claim 28, wherein the door key comprises a	The Accused Products embody the device of claim 28, wherein the door key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key.

	selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key.	For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Product may then be used to unlock the hotel room and/or car. (VAR00000003-09). The keys include, e.g., keys stored on applets in the Secure Element. Privacy and security Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted. (VAR VAR0001075 at 1222).
30	The mobile communication device of claim 26, wherein the instructions are further configured to cause the mobile communication device to facilitate the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments with Apple Pay using the Accused Products. (VAR0001075-1293 at 1210-211). Apple also directs and controls the provisioning of keys and passes. (VAR00000003-09).	The Accused Products embody the device of claim 26, wherein the instructions are further configured to cause the mobile communication device to facilitate provision of RFID data to the mobile communication device. For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments with Apple Pay using the Accused Products. (VAR0001075-1293 at 1210-211). Apple also directs and controls the provisioning of keys and passes. (VAR00000003-09).

		Credit, debit, and prepaid cards Card provisioning security overview When a user adds a credit, debit, or prepaid card (including store cards) to Apple Wallet, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer determines whether to approve adding the card to Apple Wallet. As part of the card provisioning process, Apple Pay uses three server-side calls to send and receive communication with the card issuer or network: • Required Fields • Check Card • Link and Provision The card issuer or network uses these calls to verify, approve, and add cards to Apple Wallet. These client-server sessions use TLS 1.2 to transfer the data. Full card numbers aren't stored on the device or on Apple Pay servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from most credit or debit card numbers; the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is never stored on Apple Pay servers or backed up to iCloud, and it is isolated from iOS, iPadOS, and watchOS devices and from Mac computers with Touch ID. Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone, or within a card issuer's iPhone app. Adding a card to Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch.

		Adding credit or debit cards manually To add a card manually, the name, card number, expiration date, and CVV are used to facilitate the provisioning process. From within Settings, Apple Wallet, or the Apple Watch app, users can enter that information either by typing or by using the device's camera. When the camera captures the card information, Apple attempts to populate the name, card number, and expiration date. The photo is never saved to the device or stored in the photo library. After all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are then encrypted and sent to the Apple Pay server. If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the terms and conditions, Apple sends the ID of the terms that were accepted as well as the CVV to the Link and Provision process. Additionally, as part of the Link and Provision process, Apple shares information from the device with the card issuer or network. This includes information about (a) the user's iTunes and App Store account activity (for example, whether the user has a long history of transactions within iTunes), (b) the user's device (for example, the phone number, name, and model of the user's device plus any companion Apple device necessary to set up Apple Pay), and (c) the user's approximate location at the time the user adds their card (if the user has Location Services enabled). Using this information, the card issuer determines whether to approve adding the card to Apple Pay. As the result of the Link and Provision process, two things occur: • The device begins to download the Apple Wallet pass file representing the credit or debit card. • The device begins to bind the card to the Secure Element. The pass file contains URLs to download card art, metadata about the card such as contact information, the related issuer's app, and supported features. It also contains the pass state, which includes information such as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whether additional verification is required before the card can make payments with Apple Pay.
--	--	--

	The data includes, e.g., data from applets within the Secure Element. Secure Element The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus. NFC controller As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server. (VAR0001075 at 1209).
31	The mobile communication device of claim 30, wherein the instructions are further configured to cause the mobile communication device to include provisioning of at least a signaling attribute associated with the outputting of the RFID data in the form of a radio frequency signal. For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments with Apple Pay using the Accused Devices, and Apple further directs, controls, and specifies the communication and security protocols associated with making contactless payments via

	outputting of the RFID data in the form of a radio frequency signal.	Apple Pay. (VAR0001075-1293 at 1208-09). Apple also directs and controls the provisioning of keys and passes. (VAR0000003-09). NFC controller The NFC controller handles Near Field Communication protocols and routes communication between the Application Processor and the Secure Element, and between the Secure Element and the point-of-sale terminal. NFC controller As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.
32	The mobile communication device of claim 26, wherein the mobile communication device is one of a wireless mobile phone and a personal digital assistant	The Accused Products embody the device of claim 26, wherein the mobile communication device is one of a wireless mobile phone and a personal digital assistant equipped with communication capability. For example the Accused Products are wireless mobile phones and/or personal digital assistants equipped with communication capability. For example the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (e.g., via LTE, CDMA, UMTS, and/or

	equipped with communication capability.	GSM), and/o audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling). (VAR0000849-855). As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (<i>e.g.</i>, Via LTE via LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (<i>e.g.</i>, via FaceTime audio and Wi-Fi calling). (VAR00000639-1074).
--	---	--