IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
MIDLAND DIVISION

MOBILITY IP HOLDINGS, INC.,	§	
	§	
Plaintiff,	§	
	§	Case No. 7:26-cv- 00075
v.	§	
	§	
APPLE INC.,	§	
	§	Jury Trial Demanded
Defendants.	§	
	§	
	§	
	§	

PLAINTIFF'S COMPLAINT

Plaintiff **Mobility IP Holdings, Inc.** ("Mobility IP") files this suit against Defendant Apple Inc. ("Apple" or "Defendant") for infringement of United States Patent Nos. 8,151,345; 8,548,924; 8,766,772; 8,933,807; 10,235,513; 10,706,412; and 10,762,187 and alleges, with personal knowledge as to its own actions and on information and belief as to the actions of others, as follows:

THE PARTIES

1. Plaintiff Mobility IP is a Texas corporation that holds all right, title, and interest in United States Patent Nos. 8,151,345 ("'345 Patent"); 8,548,924 ("'924 Patent"); 8,766,772 ("'772 Patent"); 8,933,807 ("'807 Patent"); 10,235,513 ("'513 Patent"); 10,706,412 ("'412 Patent"); and 10,762,187 ("'187 Patent") (collectively, "Asserted Patents"). *See* Exhibits 1–7. Mobility IP has a principal place of business at 1917 Palomar Oaks Way, Suite 110, Carlsbad, California 92008.

2. Defendant Apple is a California corporation with its principal place of business at One Apple Park Way, Cupertino, California 95014. Apple can be served through its registered

APPLE-1030

agent, CT Corporation System, 330 North Brand Boulevard, Suite 700, Glendale, California 91203.

JURISDICTION & VENUE

3. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because the action brought by Mobility IP against Apple arises under the patent laws of the United States, 35 U.S.C. § 1 *et seq*.

4. This Court has personal jurisdiction over Apple at least because Apple conducts business in this District and throughout the state of Texas.

5. This Court also has personal jurisdiction over Apple because Apple has committed acts of patent infringement in this District and throughout Texas, including selling, and offering for sale, products and services that infringe Mobility IP's Asserted Patents.

6. This Court also has personal jurisdiction over Apple because Apple has placed infringing products and services into the stream of commerce, with the expectation they will be purchased and used by customers in Texas and in this District, such that customers in Texas and in this District have purchased and used, and continue to purchase and use, Apple's infringing products and services, which has allowed Apple to derive substantial benefits from infringing acts in Texas and in this District.

7. Venue is proper in this District against Apple pursuant to 28 U.S.C. §§ 1391 and 1400(b) because Apple is subject to the personal jurisdiction of this Court as set forth above, has committed patent infringement in this District, and maintains regular and established places of business in this District, including campuses at 5505 West Parmer Lane, Austin, Texas 78727 and 12535 Riata Vista Circle, Austin, Texas 78727, and additional locations at 2901 S. Capital of Texas

Highway, Austin, Texas 78746; 3121 Palm Way, Austin, Texas 78758; 15900 La Cantera Parkway, San Antonio, Texas 78256; and 8401 Gateway Boulevard West, El Paso, Texas 79925.

FACTUAL BACKGROUND

Mobile-Device Payments

8. Use of mobile devices such as smartphones to pay for goods and services has become an enormous business that continues to grow, with some analysts estimating a total contactless transaction volume of over a trillion dollars annually in the United States.

9. Apple is one of the largest manufacturers of mobile devices in the United States and in the world. Apple's mobile devices enable users to pay at a point of sale ("POS") terminal by confirming their identity via the mobile device, then placing the mobile device close to a near-field communication ("NFC") receiver located at the POS terminal.[1] Using information stored in the mobile device via the Apple Wallet, the POS terminal can process the payment without requiring the user to physically present a payment card.

10. Because of the convenience and security of payments using mobile devices, the use of mobile devices for payments has grown substantially since the introduction of payments via mobile device. Mobile device payments are convenient because users typically carry their mobile device with them. Mobile device payments are more secure than card payments because a transaction cannot occur unless the user first authenticates themselves on the mobile device, which is a form of protection that does not exist with in-person card transactions.

Mobility IP and Its Patented Inventions

11. Well over a decade before Apple first introduced its mobile payment technology, Mobility IP began developing the technology at issue in this case.

[1] Apple Support, *How to use Apple Pay*, (Jan. 29, 2026), https://youtu.be/cxchWpM_I-0?t=88.

12. In the early 2000s, Neology, Inc. began applying for patents that embodied the innovations that resulted from innovations in this space. The United States Patent and Trademark Office ("USPTO") has since issued numerous patents to Neology, including the '772 Patent, the '807 Patent, the '513 Patent, the '412 Patent, and the '187 Patent. Neology eventually assigned these patents to Mobility IP.

13. In addition, Neology also acquired patents directed to technology involving the use of secure elements to store transaction information that can be later transmitted via near-field communication ("NFC") and other means. These inventions are reflected in the '345 Patent and the '924 Patent. Neology eventually assigned these patents to Mobility IP.

14. Mobility IP is the sole and exclusive owner of all right, title and interest to and in, or is the exclusive licensee with the right to sue for, the Asserted Patents and holds the exclusive right to take all actions necessary to enforce its rights to the Asserted Patents, including the filing of this patent infringement lawsuit. Mobility IP also has the right to recover all damages for past, present, and future infringement of the Asserted Patents and to seek injunctive relief as appropriate under the law.

Apple's Use of the Patented Technology

15. Apple markets itself as a leading provider of mobile devices in the United States such as smartphones, tablets, and watches. The ecosystem of Apple products spans billions of mobile devices. The mobile devices Apple sells in the United States include the following: iPhone XR, XS and XS Max; iPhone 11, 11 Pro, and 11 Pro Max; iPhone SE (second generation); iPhone 12, 12 mini, 12 Pro, and 12 Pro Max; iPhone 13, 13 mini, 13 Pro, and 13 Pro Max; iPhone SE (third generation); iPhone 14, 14 Plus, 14 Pro, and 14 Pro Max; iPhone 15, 15 Plus, 15 Pro, and 15 Pro Max; iPhone 16, 16 Plus, 16 Pro, 16 Pro Max, and 16e; iPhone 17, 17 Plus, 17 Pro, 17 Pro

Max, 17e; iPhone Air; Apple Watch 5 and later; and iPad, iPad Air, iPad Mini, and iPad Pro (referred to collectively as the "Accused Instrumentalities").[2] Throughout this complaint, if an exemplary mobile device is discussed, such as the Apple iPhone 14 Pro,[3] it should be understood that the accusations against the exemplary mobile device are also applicable to all other Apple mobile devices sold in the United States in the past six years.

16. Near Field Communication ("NFC") can be used to facilitate mobile payments when an NFC-equipped device (such as a smartphone or an electronic wearable like a watch) is placed near a contactless merchant terminal allowing the devices to exchange payment data.

17. Contactless merchant terminal adoption in the U.S. has been expedited by card issuer security requirements. Card issuers in the United States set an October 2015 deadline for merchants to upgrade payment terminals capable of accepting credit cards with embedded chips for security, and many of these upgraded terminals have NFC capability built in. In December 2015, approximately 2.36 million contactless terminals were in service in the United States. As a result of the COVID-19 pandemic, there has been a sharp rise in adoption of contactless payment in the United States and all over the globe. By 2024, there were over 10 million contactless terminals in service in the United States and contactless payments accounted for approximately 25% of all card transactions in the United States.[4]

18. Each of the Accused Instrumentalities includes features including a processor, memory, a secure element, biometric security, a display, a cellular radio, and an NFC radio.

---

[2] Amalia S., *Full List of Every iPhone Model from 2007-2026*, https://www.macobserver.com/tips/round-ups/full-list-of-every-iphone-model-from-2007/ (last visited Mar. 4, 2026).
[3] Apple, *iPhone 14 Pro – Technical Specifications*, https://support.apple.com/en-us/111849 (last visited Feb. 26, 2026).
[4] Clearly Payments, *The Contactless Payments Market Overview in USA for 2024*, https://www.clearlypayments.com/blog/the-contactless-payments-market-overview-in-usa-for-2024/ (last visited Feb. 17, 2026).

19. On September 9, 2014, Apple launched its Apple Pay mobile payment service that enabled its users to make a payment using a mobile device.[5] The mobile device first authenticates the user using biometrics such as a fingerprint reader or facial recognition. After authentication, the user places the mobile device near a POS terminal. The mobile device then transmits transaction information (such as card information) to the POS terminal via NFC to complete the transaction.

20. By making, using, offering to sell, and/or selling the Accused Instrumentalities, Apple has infringed and is infringing the Asserted Patents as described in further detail below.

Causes of Action

Count I: Infringement of U.S. Patent No. 8,151,345 ("'345 Patent")

21. All preceding factual allegations above are incorporated as if fully set forth herein.

22. The USPTO duly and legally issued U.S. Patent No. 8,151,345 to C. Douglas Yeager as the named inventor. All right, title, and interest in the '345 Patent have been assigned to Mobility IP.

23. The '345 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

24. Apple has directly infringed and continues to directly infringe the '345 Patent. The infringing acts include, but are not limited to, the manufacture, use, sale, importation, and/or offer for sale of the Accused Instrumentalities to practice the claimed invention in the '345 Patent. For example, claim 23 of the '345 Patent[6] recites:

---

[5] Apple, *Apple Announces Apple Pay*, (Sep. 9, 2014), https://www.apple.com/newsroom/2014/09/09Apple-Announces-Apple-Pay/; *see also* scaceres, *Apple Pay Presentation (2014)*, (Sep. 11, 2014), https://youtu.be/5ExcCyS1ZH8.

[6] Claim 23 is referenced herein for representative purposes. Plaintiff reserves the right to identify additional asserted claims and reserves its right to provide greater detail and scope via its Infringement Contentions at the time required under this Court's scheduling order.

A cellular network adapter for a cellular network device configured with a cellular network application interface comprising;

a secure element comprising a data file;

a secure element reader in the cellular network adapter configured to interrogate the secure element by executing file system functions according to ISO 7816-4 and to generate file information from the secure element data file;

a near field communications controller bridge chip to convert the file information to an RF data signal for an external reader; and

a communications controller configured to receive the file information from the secure element reader and to convert at least a portion of the file information into transaction authorization information and to transmit the transaction authorization information from the cellular network device over a wireless network through the cellular network application interface, wherein the wireless network comprises a cellular network and the secure element reader in the cellular network adapter is configured to await a startup instruction comprising an unpredictable number originating over the cellular wireless network prior to interrogating the secure element.

25. The Accused Instrumentalities meet the recited elements of Claim 23. For example, the Accused Instrumentalities include a secure element. The teardown of an exemplary Apple iPhone 14 Pro is presented below.[7] The motherboard includes a secure element, a near field communications controller bridge chip, and one or more processors that are configured to receive file information from the secure element and to convert the information into transaction authorization information:

[7] Hemant Kumar Vishwakarma, *Apple iPhone 14 Pro – Teardown Report*, https://unitedlex.com/insights/apple-iphone-14-pro-teardown-report/ (last visited Feb. 26, 2026).

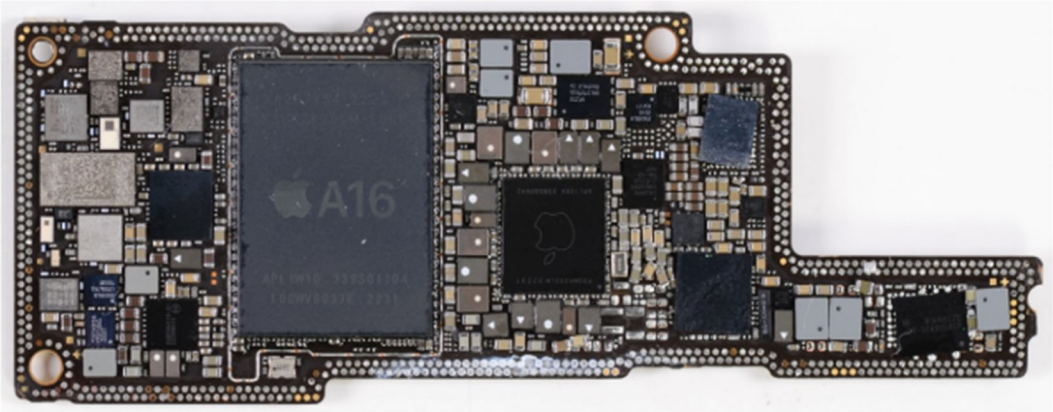


Figure 10

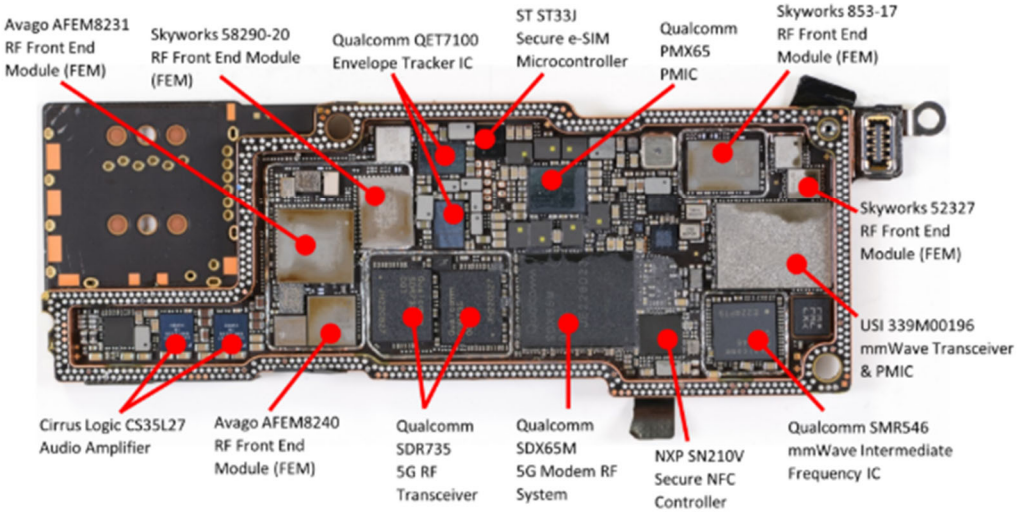


Figure 11

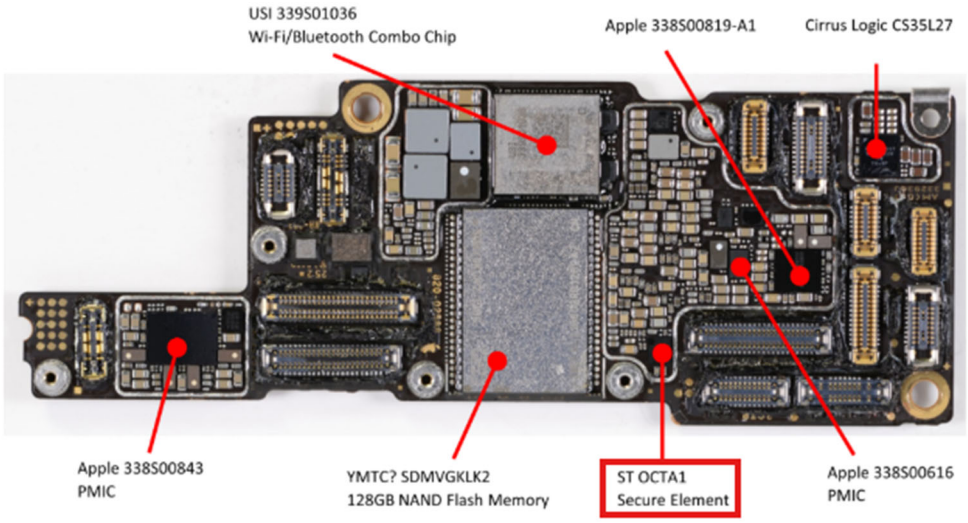


Figure 12

26. The secure element is used to store card information.[8] The Accused Instrumentalities follow Europay, Mastercard, and Visa's (EMV's) standards for processing contactless payments.[9]

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

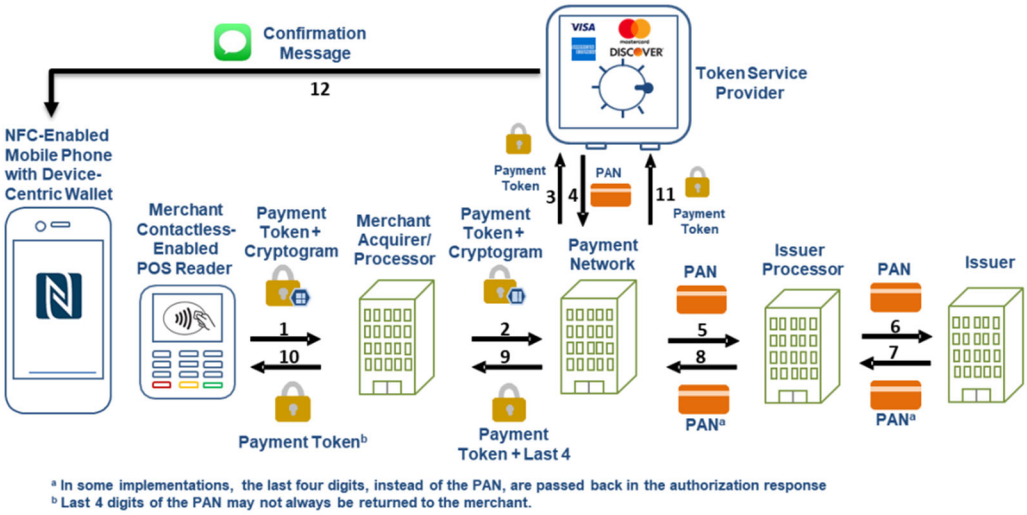


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

[8] Apple, *Apple Pay security and privacy overview*, https://support.apple.com/en-us/101554 (last visited Feb. 26, 2026) ("The Device Account Number can't be decrypted by Apple but is stored in the Secure Element.")
[9] US Payments Forum, *EMV Payment Tokenization Primer and Lessons Learned*, (Jun. 2019), https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf at 24–25; *see also* EMVCo, *EMV Payment Tokenisation: A Guide to Use Cases* (Jan. 16, 2023) at 42–43, found at https://www.emvco.com/emv-technologies/payment-tokenisation/.

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

27. The cardholder's primary account number (PAN) is sent to a token provider that verifies the card via the card issuer. Once verified, a token known as the Device Account Number is activated and stored in the mobile device. The Device Account Number is a surrogate that represents the PAN for purposes of payment processing.[10] Thus, the secure element includes a data file.

28. The above-described functionality is initiated by the processor that accessed the transaction information (e.g., the Device Account Number) from the secure element. The information is then combined into a communications data package (the unique cryptogram) based on the transaction information.

[10] *See* EMVCo, *supra*, at 41–42.

29. During an Apple Pay transaction, the mobile device creates a dynamic cryptogram specific to the transaction. The dynamic cryptogram is created using the token (based on the credit card), token key, transaction amount, etc. according to the EMV contactless specification.[11] The dynamic cryptogram, token, and other data is transmitted via NFC from the mobile device to the terminal. The Accused Instrumentalities allow for the emulation of ISO 7816-4 cards.[12]

30. The Accused Instrumentalities include a communications controller configured to receive the file information from the secure element reader and to convert at least a portion of the file information into transaction authorization information and to transmit the transaction authorization information from the cellular network device over a wireless network through the cellular network application interface, wherein the wireless network comprises a cellular network and the secure element reader in the cellular network adapter is configured to await a startup instruction comprising an unpredictable number originating over the cellular wireless network prior to interrogating the secure element.

31. Apple committed the infringing activities without a license from Mobility IP. Apple's acts of infringement have damaged Mobility IP, as owner of the '345 Patent. Mobility IP is entitled to recover from Apple the damages it has sustained as a result of Apple's wrongful acts in an amount subject to proof at trial. The infringement of the '345 Patent by Apple has damaged and will continue to damage Plaintiff.

32. Apple's infringement of Mobility IP's '345 Patent is willful as of the date of the service of Mobility IP's Original Complaint.

---

[11] US Payments Forum, *supra* at 41.
[12] Apple Developer, *CardSession*, https://developer.apple.com/documentation/corenfc/cardsession/ (last visited Feb. 26, 2026).

Count II: Infringement of U.S. Patent No. 8,548,924 ("'924 Patent")

33. All preceding factual allegations above are incorporated as if fully set forth herein.

34. The USPTO duly and legally issued U.S. Patent No. 8,548,924 to C. Douglas Yeager as the named inventor. All right, title, and interest in the '924 Patent have been assigned to Mobility IP.

35. The '924 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

36. Apple has directly infringed and continues to directly infringe the '924 Patent. The infringing acts include, but are not limited to, the manufacture, use, sale, importation, and/or offer for sale of the Accused Instrumentalities to practice the claimed invention in the '924 Patent. For example, claim 60 of the '924 Patent[13] recites:

> A token for transmitting a communications data package to a host device, the token comprising:
>
> > a mounting structure;
> >
> > a secure element affixed to the mounting structure, the secure element including a data file containing transaction information;
> >
> > a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire the transaction information from the data file by exchanging at least one transaction data communication between the secure element and the secure element interrogator and to generate the communications data package based on the transaction information; and
> >
> > a communications controller affixed to the mounting structure and configured to receive the communications data package from the secure element interrogator and to transmit the communications data package to the host device.

37. The Accused Instrumentalities meet the recited elements of claim 60.

[13] Claim 60 is referenced herein for representative purposes. Plaintiff reserves the right to identify additional asserted claims and reserves its right to provide greater detail and scope via its Infringement Contentions at the time required under this Court's scheduling order.

38. For example, the Accused Instrumentalities include a mounting structure and a secure element affixed to the mounting structure. The teardown of an exemplary Apple iPhone 14 Pro is presented below.[14] The motherboard includes a mounting structure, a secure element, a secure element interrogator, and a communications controller that is configured to interrogate the secure element to acquire transaction information and generate a communications package and further configured to transmit a communications data package to a host device.

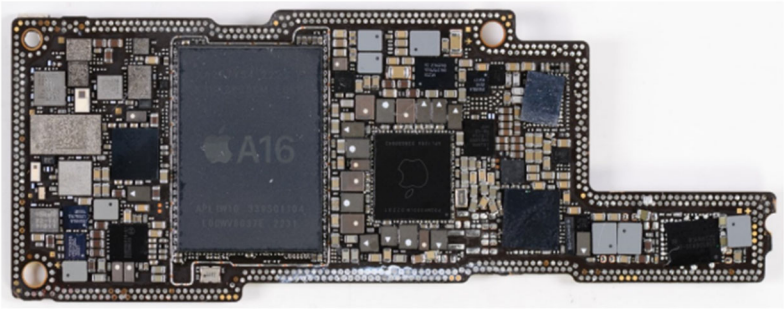


Figure 10

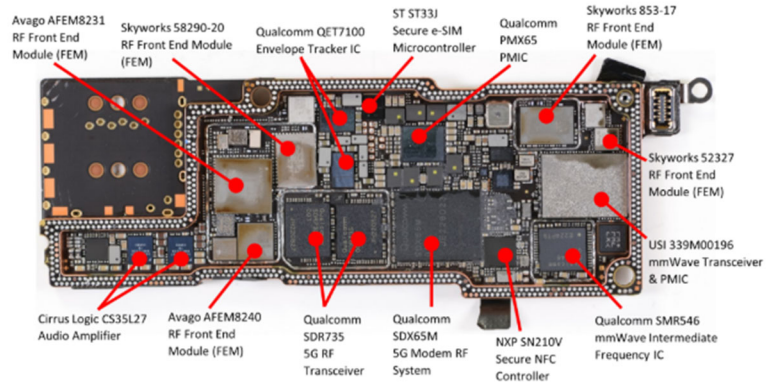


Figure 11

[14] Vishwakarma, *supra*.

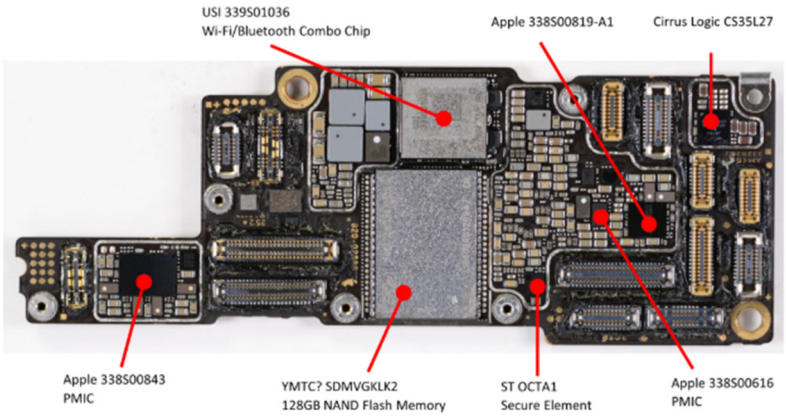


Figure 12

39. The secure element is used to store card information.[15] The Accused Instrumentalities follow EMV's standards for processing contactless payments.[16]

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

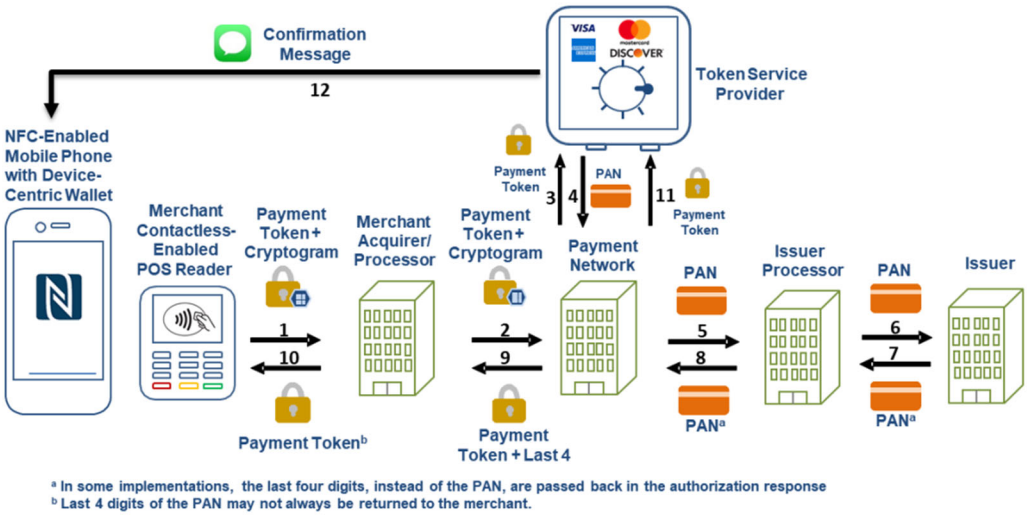


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

[15] Apple, *Apple Pay security and privacy overview*, *supra* ("The Device Account Number can't be decrypted by Apple but is stored in the Secure Element.")
[16] US Payments Forum, *supra* at 24–25; *see also* EMVCo., *supra* at 42–43.

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

40. The cardholder's primary account number (PAN) is sent to a token provider that verifies the card via the card issuer. Once verified, a token known as the Device Account Number is activated and stored in the mobile device. The Device Account Number is a surrogate that represents the PAN for purposes of payment processing.[17] Thus, the secure element includes a data file containing transaction information.

41. The above-described functionality is initiated by the processor that accessed the transaction information (e.g., the Device Account Number) from the secure element. The information is then combined into a communications data package (the unique cryptogram) based on the transaction information. During an Apple Pay transaction, the mobile device creates a

[17] *See* EMVCo., *supra* at 41–42.

dynamic cryptogram specific to the transaction. The cryptogram is created using the token (based on the credit card), token key, transaction amount, etc. according to the EMV contactless specification.[18] The dynamic cryptogram, token and other data is transmitted via NFC from the mobile device to the terminal. Thus, the communications data package is based on the transaction information.

42. The communications data package is created and transmitted to the host device. The processor is used to perform such functionality.

43. Apple committed the infringing activities without license from Mobility IP. Apple's acts of infringement have damaged Mobility IP, as owner of the '924 Patent. Mobility IP is entitled to recover from Apple the damages it has sustained as a result of Apple's wrongful acts in an amount subject to proof at trial. The infringement of the '924 Patent by Apple has damaged and will continue to damage Plaintiff.

44. Apple's infringement of Mobility IP's '924 Patent is willful as of the date of the service of Mobility IP's Original Complaint.

Count III: Infringement of U.S. Patent No. 8,766,772

45. All preceding factual allegations are incorporated as if fully set forth herein.

46. The USPTO duly and legally issued U.S. Patent No. 8,766,772 ("'772 Patent") to Mr. Franciso Martinez de Velasco Cortina and Mr. Manfred Rietzler as named inventors. All right, title, and interest in the '772 Patent have been assigned to Mobility IP.

47. The '772 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

[18] US Payments Forum, *supra* at 41.

48. Apple has directly infringed the ’772 Patent. The infringing acts include, but are not limited to, the manufacture, use, sale, importation, and/or offer for sale of the Accused Instrumentalities to practice the claimed invention in the ’772 Patent. For example, Claim 9 of the ’772 Patent[19] recites:

> A mobile device, comprising:
>
> a biometric input device configured to receive biometric data; and
>
> a radio frequency antenna and a chip, the chip comprising:
>
> > a memory, the memory configured to store transaction information and biometric information for identifying an individual associated with the transaction, and
> >
> > a processor coupled with the memory and the biometric input, the processor configured to:
> >
> > > receive a signal via the radio frequency antenna, the signal comprising a request to access the memory and retrieve the transaction information,
> > >
> > > receive biometric information from the biometric input device,
> > >
> > > compare the received biometric information with the biometric information stored in the memory, and
> > >
> > > provide the transaction information in response to the access request when the biometric information matches.

The Accused Instrumentalities meet the recited elements of Claim 9.

49. For instance, Apple’s mobile devices include a biometric input device such as a fingerprint sensor (Touch ID) or facial recognition (Face ID):[20]

> **Use Touch ID to unlock your iPhone or make purchases**
>
> After you set up Touch ID, you can use Touch ID to unlock your iPhone. Just press the Touch ID sensor using the finger that you registered with Touch ID.

[19] Claim 9 is referenced herein for representative purposes. Plaintiff reserves the right to identify additional asserted claims and reserves its right to provide greater detail and scope via its Infringement Contentions at the time required under this Court’s scheduling order.

[20] Apple, *Use Touch ID on iPhone and iPad*, https://support.apple.com/en-us/102528 (last visited Feb. 26, 2026) (Touch ID); Apple, *Use Face ID on your iPhone or iPad Pro*, https://support.apple.com/en-us/108411 (last visited Feb. 26, 2026) (Face ID).

50. The Accused Instrumentalities include a radio frequency antenna. For example, the Accused Instrumentalities include NFC technology that includes a chip and an antenna configured to communicate via NFC, which utilizes radio frequency.[21]

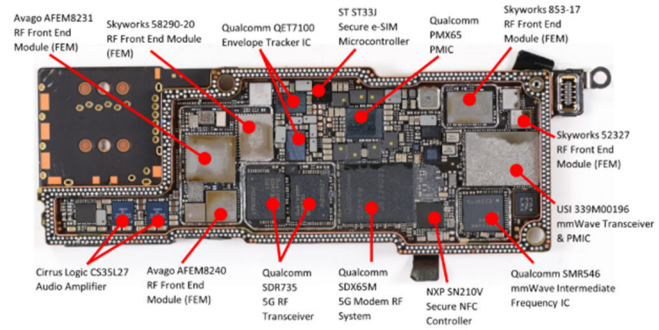


Figure 11

[21] Vishwakarma, *supra.*

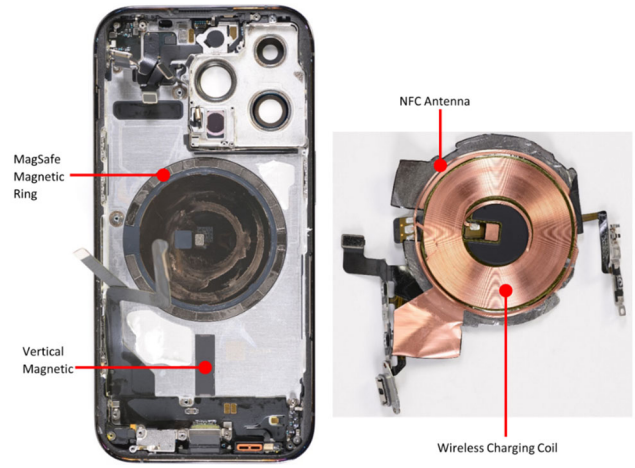


Figure 13: MagSafe system

51. The Accused Instrumentalities include a chip. For illustrative purposes, the main board of an Apple iPhone 14 Pro is illustrated below.[22] The main board includes multiple chips, including an A16 System on a Chip (SoC).

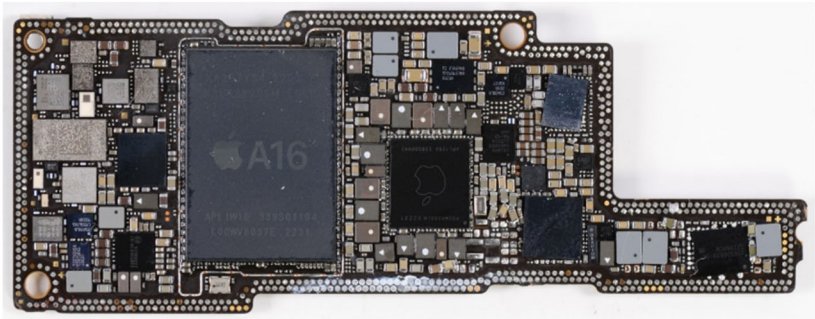
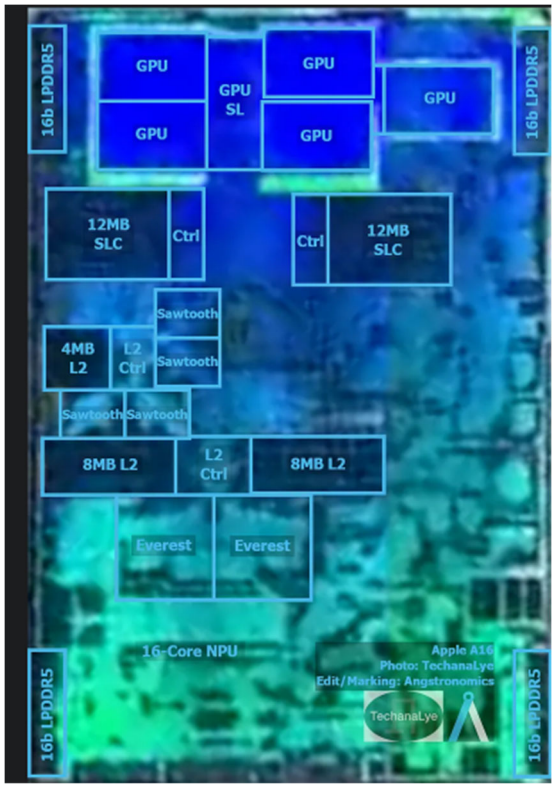


Figure 10

52. The Accused Instrumentalities include a memory. The memory is configured to store transaction information and biometric information for identifying an individual associated with the transaction. For example, the Accused Instrumentalities include random access memory (RAM) which qualifies as memory.[23]

---

[22] Vishwakarma, *supra*.
[23] Skyjuice, *Apple A16 Die Analysis*, (Sep. 22, 2022), https://www.angstronomics.com/p/apple-a16-die-analysis; *see also* GSMArena, *iPhone 14 Pro*, https://www.gsmarena.com/apple_iphone_14_pro-11860.php (last visited Feb. 26, 2026) (stating that the iPhone 14 Pro includes 6 GB of RAM.)



53. The memory is used to store biometric information and transaction information. For example, Apple's iPhones use a secure subsystem called the Secure Enclave to store sensitive data such as biometric information and transaction information.[24] All of the Accused Instrumentalities have the Secure Enclave system.[25]

54. The Accused Instrumentalities store sensitive data such as biometric authentication information and transaction information in a variety of different ways. Face ID and Touch ID information, which qualify as "biometric authentication information" is "encrypted and protected by the Secure Enclave."[26] Credit card payment information (which qualifies as transaction

[24] Apple Platform Security, *The Secure Enclave*, https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web (last visited Feb. 26, 2026).
[25] *Id.*
[26] Apple, *About Face ID advanced technology*, https://support.apple.com/en-us/102381 (last visited Feb. 26, 2026) (describing Face ID); Apple, *About Touch ID advanced technology*, https://support.apple.com/en-us/105095 (last visited Feb. 26, 2026) (describing Touch ID).

information) is stored in memory.[27] The secure element may also be used to store card information.[28]

> After your card is approved, your bank, your bank's authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such as the key used to generate dynamic security codes that are unique to each transaction) to Apple. The Device Account Number can't be decrypted by Apple but is stored in the Secure Element — an industry-standard, certified chip designed to store your payment information safely — on your device. Unlike with usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS, watchOS, macOS, and visionOS, is never stored on Apple servers, and is never backed up to iCloud.

55. The Accused Instrumentalities include a processor coupled with the memory and the biometric input. For example, the Apple iPhone 14 Pro includes an A16 processor.[29]

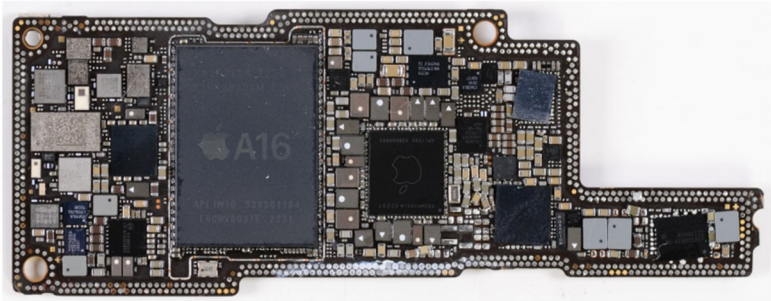


Figure 10

56. In the Accused Instrumentalities, the processor is configured to receive a signal via the radio frequency antenna, the signal comprising a request to access the memory and retrieve the transaction information. For example, the Accused Instrumentalities follow EMV's standards for processing contactless payments.[30]

---

[27] Apple Platform Security, *Apple Pay component security*, https://support.apple.com/guide/security/apple-pay-component-security-sec2561eb018/web (last visited Feb. 26, 2026).
[28] Apple, *Apple Pay security and privacy overview*, *supra*; *see also* James Hoodja, *Where Are Card Details Stored On iPhone*, (Jun. 28, 2023), https://www.safewiper.com/blog/where-are-card-details-stored-on-iphone.html ("card details ... are stored in the iPhone's Secure Element, which is a dedicated chip designed to store sensitive information.")
[29] Vishwakarma, *supra*.
[30] US Payments Forum, *supra* at 24–25; *see also* EMVCo., *supra* at 42–43.

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

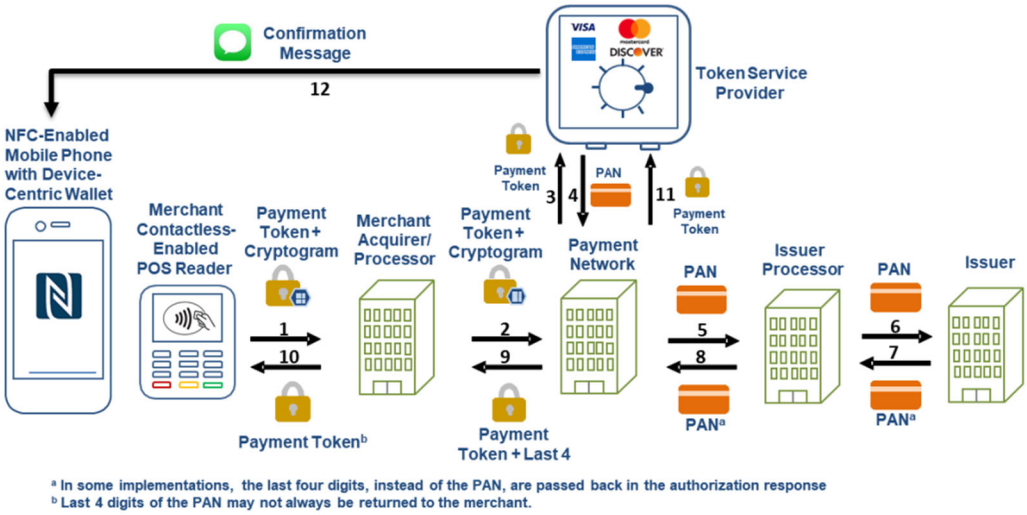


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

57. During a transaction, as exemplarily illustrated above, the user places the mobile device in proximity to the NFC reader in the POS terminal. As part of the process, the POS terminal sends a signal to the user's mobile device—"One device (usually the NFC reader) generates an electromagnetic field to establish a connection."[31]

58. In the Accused Instrumentalities, the processor is configured to receive biometric information from the biometric input device. The user authenticates himself/herself using biometric information, such as through the use of Touch ID or Face ID. Face ID works by projecting infrared dots on a user's face, then comparing the resulting three-dimensional image to the version stored on the mobile device.[32]

59. Touch ID uses an embedded fingerprint sensor built into the home button of some mobile devices.[33] The sensor uses capacitive touch to capture high-resolution images of the user's fingerprints, maps individual details, and compiles the data together. Touch ID then uses the data to match and recognize fingerprints.[34]

60. The Face ID and Touch ID templates are encrypted and stored by the Secure Enclave within the Accused Instrumentalities.[35] That data is then compared with the received biometric information.

61. In the Accused Instrumentalities, the processor is configured to provide the transaction information in response to the access request when the biometric information matches. A video on the Apple.com website explains how a user operates the Apple Pay functionality of the

---

[31] Katie Nelson, *What is NFC and How Does it Work?*, Lightspeed (Jun. 5, 2025) https://www.lightspeedhq.com/blog/near-field-communication-payments-explained/.
[32] Zackdfilms, *How Apple's Face ID Works*, https://www.youtube.com/shorts/gEV8kjtn5QA (last visited Feb. 26, 2026).
[33] Elyse Betters Picaro, Apple's Touch ID fingerprint sensor explained, (Mar. 4, 2022) https://www.pocket-lint.com/phones/news/apple/123832-apple-s-touch-id-fingerprint-sensor-explained-here-s-what-you-need-to-know/
[34] *Id.*; Apple, *About Touch ID advanced technology*, *supra*.
[35] Apple, *About Face ID advanced technology*, *supra*; Apple, *About Touch ID advanced technology*, *supra.*

iPhone.[36] Apple also has posted videos on YouTube explaining how a transaction proceeds after the user authenticates using biometric information—"When you want to make a purchase on an iPhone with Face ID, simply double-click the side button and glance at your iPhone to authenticate. If you have an iPhone with Touch ID, double-click the home button, then rest your finger on it to authenticate …. When you're ready to pay, just hold the top of your iPhone near the contactless symbol on the card reader."[37] After the user is authenticated, the process follows the EMV standard for processing contactless payments, illustrated below. This includes providing the transaction information in response to the transaction request when the biometric information matches.[38]

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

[36] Apple, *Apple Pay*, https://www.apple.com/apple-pay/ (last visited Feb. 26, 2026).
[37] Apple Support, *How to use Apple Pay*, *supra*.
[38] US Payments Forum, *supra* at 24–25.

62. Apple committed the infringing activities without license from Mobility IP. Apple's acts of infringement have damaged Mobility IP, as owner of the '772 Patent. Mobility IP is entitled to recover from Apple the damages it has sustained as a result of Apple's wrongful acts in an amount subject to proof at trial. The infringement of the '772 Patent by Apple has damaged Plaintiff.

Count IV: Infringement of U.S. Patent No. 8,933,807

63. All preceding factual allegations are incorporated as if fully set forth herein.

64. The USPTO duly and legally issued U.S. Patent No. 8,933,807 to Mr. Franciso Martinez de Velasco Cortina and Mr. Manfred Rietzler as named inventors. All right, title, and interest in the '807 Patent have been assigned to Mobility IP.

65. The '807 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

66. Apple has directly infringed the '807 Patent. The infringing acts include, but are not limited to, the manufacture, use, sale, importation, and/or offer for sale of the Accused Instrumentalities to practice the claimed invention in the '807 Patent. For example, claim 1 of the '807 Patent[39] recites:

A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

short range RF circuitry;

memory configured to store biometric authentication information and transaction information, wherein the biometric authentication information has been previously associated with the transaction information;

a biometric reading device configured to read biometric information;

[39] Claim 1 is referenced herein for representative purposes. Plaintiff reserves the right to identify additional asserted claims and reserves its right to provide greater detail and scope via its Infringement Contentions at the time required under this Court's scheduling order.

an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in memory; and

a transaction module configured to provide the transaction information via the short range RF circuitry for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated as being associated with the transaction information by the authentication module.

67. The Accused Instrumentalities meet the recited elements of the claimed mobile device of claim 1.

68. Apple's mobile devices include radio frequency cellular circuitry that allows access to various cellular networks. For example, the Apple iPhone 14 Pro includes multiple radios:[40]

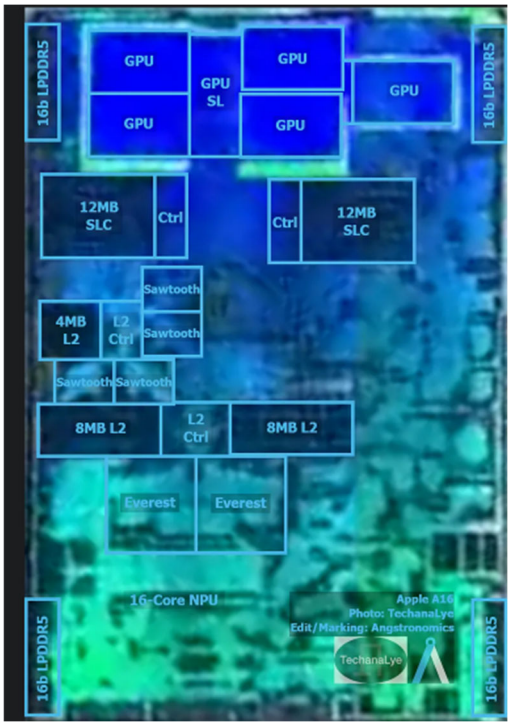
Cellular and Wireless

- Model A2650*
  - 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n77, n78 n79)
  - 5G NR mmWave (Bands n258, n260, n261)
  - FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71)
  - TD-LTE (Bands 34, 38, 39, 40, 41, 42, 46, 48, 53)
  - UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - GSM/EDGE (850, 900, 1800, 1900 MHz)
- Model A2651*
  - 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n77, n78 n79)
  - 5G NR mmWave (Bands n258, n260, n261)
  - FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71)
  - TD-LTE (Bands 34, 38, 39, 40, 41, 42, 46, 48, 53)
  - UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - GSM/EDGE (850, 900, 1800, 1900 MHz)
- All models
  - 5G (sub-6 GHz and mmWave) with 4x4 MIMO[8]
  - Gigabit LTE with 4x4 MIMO and LAA[8]
  - Wi-Fi 6 (802.11ax) with 2x2 MIMO
  - Bluetooth 5.3
  - Ultra Wideband chip for spatial awareness[9]
  - NFC with reader mode
  - Express Cards with power reserve

[40] Apple, *iPhone 14 Pro – Technical Specifications*, *supra*.

69. The Accused Instrumentalities include short-range RF circuitry. For example, as shown above, the Accused Instrumentalities include "NFC with reader mode."[41]

70. The Accused Instrumentalities include a memory. The memory is configured to store transaction information and biometric information. For example, the Accused Instrumentalities include random access memory (RAM) which qualifies as memory.[42]



71. The memory is used to store fingerprint information and transaction information. For example, Apple's iPhones use a secure subsystem called the Secure Enclave to store sensitive data such as biometric information and transaction information.[43] All of the Accused Instrumentalities have the Secure Enclave system.[44]

72. The Accused Instrumentalities store sensitive data such as biometric authentication information and transaction information in a variety of different ways. Face ID and Touch ID

---

[41] *Id*.
[42] Skyjuice, *supra*; *see also* GSMArena, *supra*.
[43] Apple Platform Security, *The Secure Enclave*, *supra*.
[44] *Id.*

information, which qualify as "biometric authentication information" is "encrypted and protected by the Secure Enclave."[45] Credit card payment information (which qualifies as transaction information) is stored in memory.[46] The biometric authentication information is associated with the transaction information in that the card owner is also the iPhone's user. The secure element also may be used to store card information.[47]

> After your card is approved, your bank, your bank's authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such as the key used to generate dynamic security codes that are unique to each transaction) to Apple. The Device Account Number can't be decrypted by Apple but is stored in the Secure Element — an industry-standard, certified chip designed to store your payment information safely — on your device. Unlike with usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS, watchOS, macOS, and visionOS, is never stored on Apple servers, and is never backed up to iCloud.

73. Apple's Accused Instrumentalities include a biometric reading device configured to read biometric information such as a fingerprint sensor (Touch ID) or facial recognition (Face ID):[48]

> **Use Touch ID to unlock your iPhone or make purchases**
>
> After you set up Touch ID, you can use Touch ID to unlock your iPhone. Just press the Touch ID sensor using the finger that you registered with Touch ID.

[45] Apple, *About Face ID advanced technology*, *supra*; Apple, *About Touch ID advanced technology*, *supra*.
[46] Apple Platform Security, *Apple Pay component security*, *supra*.
[47] Apple, *Apple Pay security and privacy overview*, *supra*; *see also* Hoodja, *supra* ("card details ... are stored in the iPhone's Secure Element, which is a dedicated chip designed to store sensitive information.")
[48] Apple, *Use Touch ID on iPhone and iPad*, *supra*; Apple, *Use Face ID on your iPhone or iPad Pro*, *supra*.

Use Face ID on your iPhone or iPad Pro

Face ID lets you securely unlock your iPhone or iPad, authenticate purchases, sign in to apps, and more — all with just a glance.

74. The Accused Instrumentalities include an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in memory.

75. In the Accused Instrumentalities, the processor is configured to receive biometric information from the biometric input device. The user authenticates himself/herself using biometric information, such as through the use of Touch ID or Face ID. Face ID works by projecting infrared dots on a user's face, then comparing the resulting three-dimensional image to the version stored on the mobile device.[49]

76. Touch ID uses an embedded fingerprint sensor built into the home button of some mobile devices.[50] The sensor uses capacitive touch to capture high-resolution images of the user's fingerprints, maps individual details and compiles the data together. Touch ID then uses the data to match and recognize fingerprints.[51]

---

[49] Zackdfilms, *supra*.
[50] Picaro, *supra*.
[51] *Id*.; Apple, *About Touch ID advanced technology*, *supra*.

77. The Face ID and Touch ID template are encrypted and stored by the Secure Enclave within the Accused Instrumentalities.[52] That data is later compared with the received biometric information.

78. The Accused Instrumentalities include a transaction module configured to provide the transaction information via the short-range RF circuitry for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated as being associated with the transaction information by the authentication module.

79. A video on the Apple.com website explains how a user operates Apple Pay.[53] In addition, Apple has posted videos on YouTube explaining how a transaction proceeds after the user authenticates using biometric information—"When you want to make a purchase, you don't need to unlock your iPhone or open Wallet. On an iPhone with Face ID, simply double-click the side button and glance at your iPhone to authenticate. If you have an iPhone with Touch ID, double-click the home button, then rest your finger on it to authenticate …. When you're ready to pay, just hold the top of your iPhone near the contactless symbol on the card reader."[54] After the user is authenticated, the process follows the EMV standard for processing contactless payments, illustrated below. This includes providing the transaction information in response to the transaction request when the biometric information matches.[55]

---

[52] Apple, *About Face ID advanced technology*, *supra*; Apple, *About Touch ID advanced technology*, *supra.*
[53] Apple, *Apple Pay*, *supra.*
[54] Apple Support, *How to use Apple Pay*, *supra*.
[55] US Payments Forum, *supra* at 24–25.

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

80. During a transaction, the user places the mobile device in proximity to the NFC reader in the POS terminal. As part of the handshaking process, the POS terminal sends a signal to the user's mobile device—"One device (usually the NFC reader) generates an electromagnetic field to establish a connection."[56]

81. Apple committed the infringing activities without license from Mobility IP. Apple's acts of infringement have damaged Mobility IP, as owner of the '807 Patent. Mobility IP is entitled to recover from Apple the damages it has sustained as a result of Apple's wrongful acts in an amount subject to proof at trial. The infringement of the '807 Patent by Apple has damaged Plaintiff.

[56] Nelson, *supra*.

Count V: Infringement of U.S. Patent No. 10,235,513

82. All preceding factual allegations are incorporated as if fully set forth herein.

83. The USPTO duly and legally issued U.S. Patent No. 10,235,513 to Mr. Franciso Martinez de Velasco Cortina and Mr. Manfred Rietzler as named inventors. All right, title, and interest in the ’513 Patent have been assigned to Mobility IP.

84. The ’513 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

85. Apple has directly infringed the ’513 Patent. The infringing acts include, but are not limited to, the manufacture, use, sale, importation, and/or offer for sale of the Accused Instrumentalities to practice the claimed invention in the ’513 Patent. For example, Claim 1 of the ’513 Patent[57] recites:

> A mobile device, comprising:
>
> a biometric input device configured to receive biometric data;
>
> a short range radio frequency circuit;
>
> memory configured to store biometric information for identifying an individual associated with transaction information;
>
> a processor coupled with the memory and the biometric input device, the processor configured to:
>
> receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information,
>
> receive the biometric data from the biometric input device,
>
> compare the received biometric data with the biometric information stored in the memory, and

[57] Claim 1 is referenced herein for representative purposes. Plaintiff reserves the right to identify additional asserted claims and reserves its right to provide greater detail and scope via its Infringement Contentions at the time required under this Court’s scheduling order.

transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received biometric data matches the stored biometric information; and

a mobile device body housing the biometric input device, short range radio frequency circuit, memory, and processor.

86. The Accused Instrumentalities meet the recited elements of Claim 1.

87. Apple's Accused Instrumentalities include a biometric reading device configured to read biometric information such as a fingerprint sensor (Touch ID) or facial recognition (Face ID):[58]

Use Touch ID to unlock your iPhone or make purchases

After you set up Touch ID, you can use Touch ID to unlock your iPhone. Just press the Touch ID sensor using the finger that you registered with Touch ID.

Use Face ID on your iPhone or iPad Pro

Face ID lets you securely unlock your iPhone or iPad, authenticate purchases, sign in to apps, and more — all with just a glance.

88. The Accused Instrumentalities include a short-range radio frequency circuit. For example, the Apple iPhone 14 Pro includes multiple radios including "NFC with reader mode":[59]

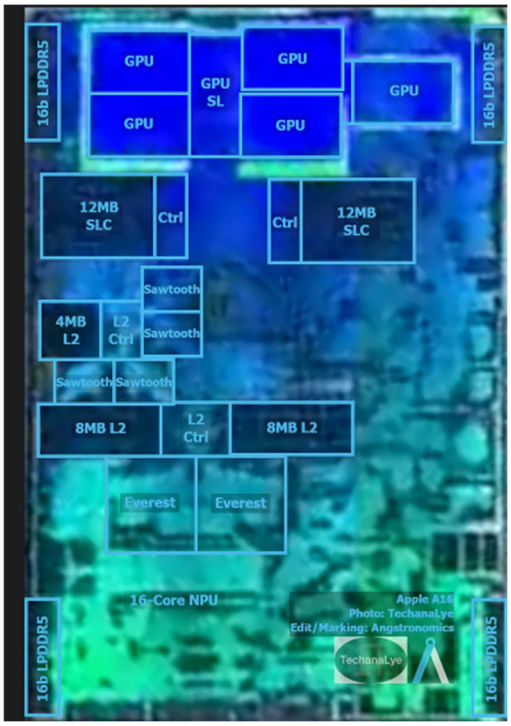
[58] Apple, *Use Touch ID on iPhone and iPad*, *supra*; Apple, *Use Face ID on your iPhone or iPad Pro*, *supra*.
[59] Apple, *iPhone 14 Pro – Technical Specifications*, *supra*.

Cellular and Wireless

- Model A2650*
  - 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n77, n78 n79)
  - 5G NR mmWave (Bands n258, n260, n261)
  - FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71)
  - TD-LTE (Bands 34, 38, 39, 40, 41, 42, 46, 48, 53)
  - UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - GSM/EDGE (850, 900, 1800, 1900 MHz)
- Model A2651*
  - 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n77, n78 n79)
  - 5G NR mmWave (Bands n258, n260, n261)
  - FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71)
  - TD-LTE (Bands 34, 38, 39, 40, 41, 42, 46, 48, 53)
  - UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - GSM/EDGE (850, 900, 1800, 1900 MHz)
- All models
  - 5G (sub-6 GHz and mmWave) with 4x4 MIMO[8]
  - Gigabit LTE with 4x4 MIMO and LAA[8]
  - Wi-Fi 6 (802.11ax) with 2x2 MIMO
  - Bluetooth 5.3
  - Ultra Wideband chip for spatial awareness[9]
  - NFC with reader mode
  - Express Cards with power reserve

89. The Accused Instrumentalities include a memory. The memory is configured to store biometric information for identifying an individual associated with transaction information. For example, the Accused Instrumentalities include random access memory (RAM) which qualifies as memory.[60]

[60] Skyjuice, *supra*; *see also* GSMArena*, supra*.



90. The memory is used to store biometric information and transaction information. For example, Apple's iPhones use a secure subsystem called the Secure Enclave to store sensitive data such as biometric information and transaction information.[61] All of the Accused Instrumentalities have the Secure Enclave system.[62]

91. The Accused Instrumentalities store sensitive data such as biometric information and transaction information in a variety of different ways. Face ID and Touch ID information, which qualify as "biometric information" is "encrypted and protected by the Secure Enclave."[63] Credit card payment information (which qualifies as transaction information) is stored in memory.[64] The biometric information is associated with the transaction information in that the card owner is also the iPhone's user. The secure element also may be used to store card information.[65]

---

[61] Apple Platform Security, *The Secure Enclave*, *supra*.
[62] *Id.*
[63] Apple, *About Face ID advanced technology*, *supra*; Apple, *About Touch ID advanced technology*, *supra*.
[64] Apple Platform Security, *Apple Pay component security*, *supra*.
[65] Apple, *Apple Pay security and privacy overview*, *supra*; *see also* Hoodja, *supra* ("card details ... are stored in the iPhone's Secure Element, which is a dedicated chip designed to store sensitive information.")

After your card is approved, your bank, your bank's authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such as the key used to generate dynamic security codes that are unique to each transaction) to Apple. The Device Account Number can't be decrypted by Apple but is stored in the Secure Element — an industry-standard, certified chip designed to store your payment information safely — on your device. Unlike with usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS, watchOS, macOS, and visionOS, is never stored on Apple servers, and is never backed up to iCloud.

92. The Accused Instrumentalities include a processor. The processor is coupled with the memory and fingerprint scanner. For example, the Apple iPhone 14 Pro includes an A16 processor.[66]

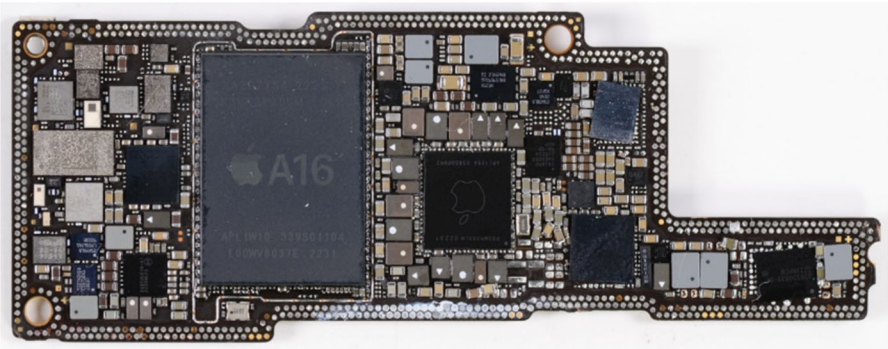


Figure 10

93. The processor is configured to receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information. The processor is also configured to receive the biometric data from the biometric input device and compare the received biometric data with the biometric information stored in the memory. The processor is further configured to transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received biometric data matches the stored biometric information.

94. For example, the Accused Instrumentalities follow EMV's standards for processing contactless payments.[67]

---

[66] Vishwakarma, *supra*.
[67] US Payments Forum, *supra* at 24–25; *see also* EMVCo., *supra* at 42–43.

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

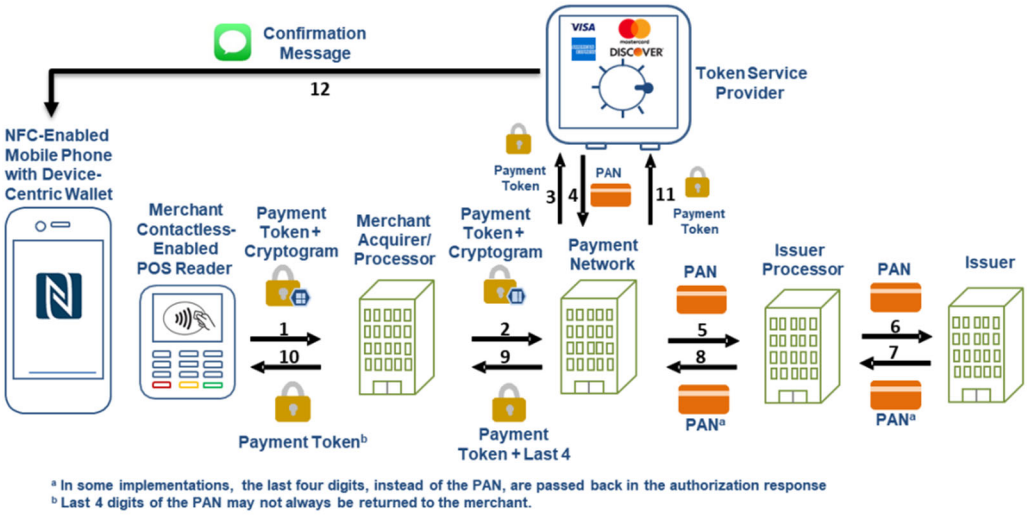


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

95. During a transaction, the user places the mobile device in proximity to the NFC reader in the POS terminal. As a part of the process, the mobile device transmits transaction information. As part of the handshaking process, the POS terminal sends a signal that is received by the user's mobile device—"One device (usually the NFC reader) generates an electromagnetic field to establish a connection."[68]

96. In the Accused Instrumentalities, the user authenticates himself/herself using biometric information, such as through the use of Touch ID or Face ID. Face ID works by projecting infrared dots on a user's face, then comparing the resulting three-dimensional image to the version stored on the mobile device.[69]

97. Touch ID uses an embedded fingerprint sensor built into the home button of some mobile devices.[70] The sensor uses capacitive touch to capture high-resolution images of the user's fingerprints, maps individual details, and compiles the data together. Touch ID then uses the data to match and recognize fingerprints.[71]

98. The Face ID and Touch ID template are encrypted and stored by the Secure Enclave within the Accused Instrumentalities.[72] That data is then compared with the received biometric information.

99. The Accused Instrumentalities include a mobile device body housing the biometric input device, short range radio frequency circuit, memory, and processor. This can be seen in a teardown of an exemplary Accused Instrumentality, such as the Apple iPhone 14 Pro.[73]

---

[68] Nelson, *supra*.
[69] Zackdfilms, *supra*.
[70] Picaro, *supra*.
[71] *Id*.; Apple, *About Touch ID advanced technology*, *supra*.
[72] Apple, *About Face ID advanced technology*, *supra*; Apple, *About Touch ID advanced technology*, *supra.*
[73] Vishwakarma, *supra*; *see also* Restore Technique, iPhone 14 Pro Teardown – Full Disassembly, (Sep. 16, 2022), https://youtu.be/UEPetgMIdAc.

100. Apple committed the infringing activities without license from Mobility IP. Apple's acts of infringement have damaged Mobility IP, as owner of the '513 Patent. Mobility IP is entitled to recover from Apple the damages it has sustained as a result of Apple's wrongful acts in an amount subject to proof at trial. The infringement of the '513 Patent by Apple has damaged Plaintiff.

Count VI: Infringement of U.S. Patent No. 10,706,412

101. All preceding factual allegations are incorporated as if fully set forth herein.

102. The USPTO duly and legally issued U.S. Patent No. 10,706,412 to Mr. Franciso Martinez de Velasco Cortina and Mr. Manfred Rietzler as named inventors. All right, title, and interest in the '412 Patent have been assigned to Mobility IP.

103. The '412 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

104. Apple has directly infringed the '412 Patent. The infringing acts include, but are not limited to, the manufacture, use, sale, importation, and/or offer for sale of the Accused Instrumentalities to practice the claimed invention in the '412 Patent. For example, Claim 1 of the '412 Patent[74] recites:

A mobile device, comprising:

short range radio frequency (RF) circuitry;

a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information; and

[74] Claim 1 is referenced herein for representative purposes. Plaintiff reserves the right to identify additional asserted claims and reserves its right to provide greater detail and scope via its Infringement Contentions at the time required under this Court's scheduling order.

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processors configured to execute instructions stored in the memory that, when executed by the one or more processors, causes the one or more processors to perform operations of:

establishing a connection with a point of sale (POS) device, via the short range RF circuitry, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

prompting the user to provide biometric information to the biometric reading device,

authenticating that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in the memory,

in response to the authentication, generating a key,

securing the payment information stored in the memory, and

transmitting to the POS device, via the short range RF circuitry, the key and the secured payment information for use in the secure transaction.

105. The Accused Instrumentalities meet the recited elements of Claim 1.

106. The Accused Instrumentalities include a short-range radio frequency circuit. For example, the Apple iPhone 14 Pro includes multiple radios, including "NFC with reader mode":[75]

[75] Apple, *iPhone 14 Pro – Technical Specifications*, *supra.*

Cellular and Wireless

- Model A2650*
  - 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n77, n78 n79)
  - 5G NR mmWave (Bands n258, n260, n261)
  - FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71)
  - TD-LTE (Bands 34, 38, 39, 40, 41, 42, 46, 48, 53)
  - UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - GSM/EDGE (850, 900, 1800, 1900 MHz)
- Model A2651*
  - 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n77, n78 n79)
  - 5G NR mmWave (Bands n258, n260, n261)
  - FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71)
  - TD-LTE (Bands 34, 38, 39, 40, 41, 42, 46, 48, 53)
  - UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - GSM/EDGE (850, 900, 1800, 1900 MHz)
- All models
  - 5G (sub-6 GHz and mmWave) with 4x4 MIMO[8]
  - Gigabit LTE with 4x4 MIMO and LAA[8]
  - Wi-Fi 6 (802.11ax) with 2x2 MIMO
  - Bluetooth 5.3
  - Ultra Wideband chip for spatial awareness[9]
  - NFC with reader mode
  - Express Cards with power reserve

107. The NFC chip and antenna of an iPhone 14 Pro can be seen in the following images of a teardown:[76]

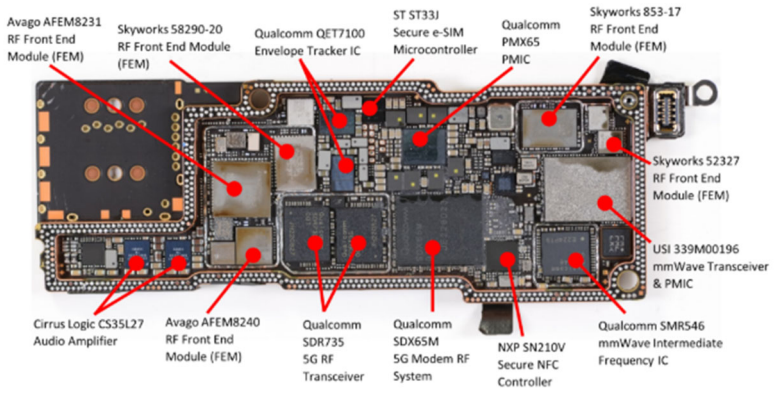


Figure 11

[76] Vishwakarma, *supra*.

The new iPhone 14 lineup features MagSafe charging that Apple first introduced with the iPhone 12. MagSafe charging uses magnets for easier Qi-charging by snapping on to the back of iPhones with the capability. The magnetic ring embedded under the wireless charging coil along with a vertical strip of magnet below the ring is identical to the system on the iPhone 13 series. The wireless charging further houses a wireless charging coil along with the NFC antenna used for Apple Pay transactions.

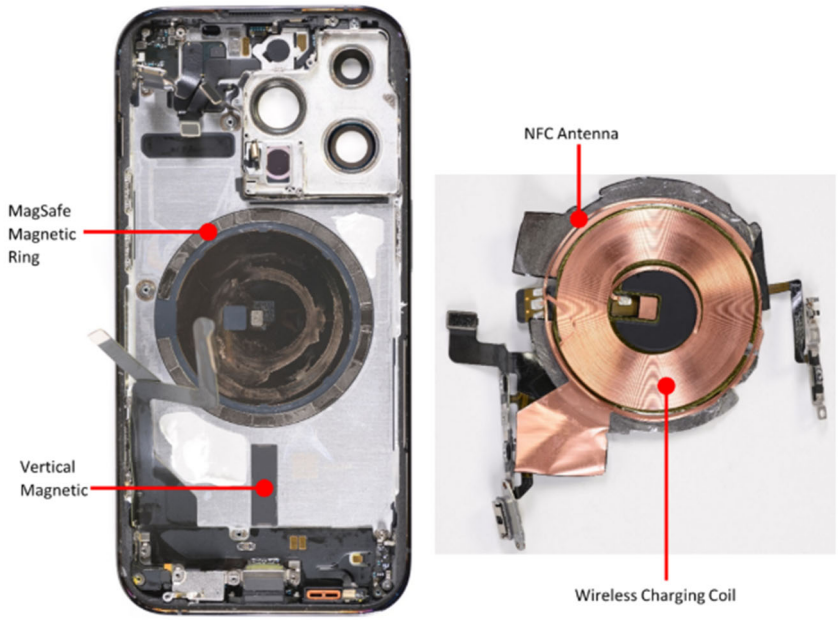
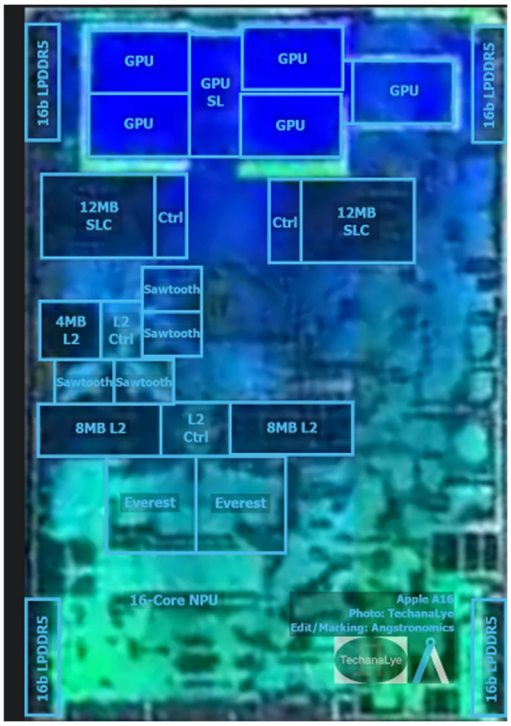


Figure 13: MagSafe system

108. The Accused Instrumentalities include a memory. The memory is configured to store transaction information and fingerprint information. For example, the Accused Instrumentalities include random access memory (RAM) which qualifies as memory.[77]

[77] Skyjuice, *supra*; *see also* GSMArena, *supra*.



109. The memory is used to store biometric information and transaction information. For example, Apple's iPhones use a secure subsystem called the Secure Enclave to store sensitive data such as biometric information and transaction information.[78] All of the Accused Instrumentalities have the Secure Enclave system.[79]

110. The Accused Instrumentalities store sensitive data such as biometric authentication information and transaction information in a variety of different ways. Face ID and Touch ID information, which qualify as "biometric authentication information" is "encrypted and protected by the Secure Enclave."[80] Credit card payment information (which qualifies as transaction information) is stored in memory.[81] The biometric authentication information is associated with

[78] Apple Platform Security, *The Secure Enclave*, *supra*.
[79] *Id.*
[80] Apple, *About Face ID advanced technology*, *supra*; Apple, *About Touch ID advanced technology*, *supra*.
[81] Apple Platform Security, *Apple Pay component security*, *supra*.

the transaction information in that the card owner is also the iPhone's user. The secure element may also be used to store card information.[82]

> After your card is approved, your bank, your bank's authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such as the key used to generate dynamic security codes that are unique to each transaction) to Apple. The Device Account Number can't be decrypted by Apple but is stored in the Secure Element — an industry-standard, certified chip designed to store your payment information safely — on your device. Unlike with usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS, watchOS, macOS, and visionOS, is never stored on Apple servers, and is never backed up to iCloud.

111. The Accused Instrumentalities include one or more processors that are coupled with the memory, short-range RF circuitry, and the biometric reading device.

112. For example, the Apple iPhone 14 Pro includes an A16 processor.[83]

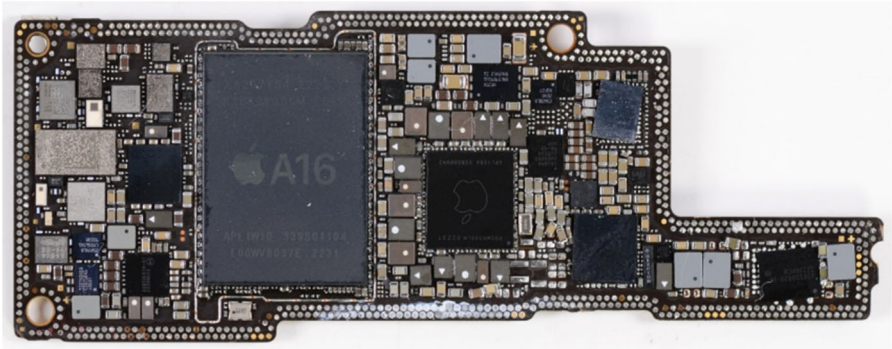


Figure 10

113. The processor is configured to establish a connection with a point of sale (POS) device via the short-range RF circuitry to conduct a secure transaction between the mobile device and the POS device. For example, the Accused Instrumentalities follow EMV's standards for processing contactless payments.[84]

---

[82] Apple, *Apple Pay security and privacy overview*, *supra*; *see also* Hoodja, *supra* ("card details ... are stored in the iPhone's Secure Element, which is a dedicated chip designed to store sensitive information.")
[83] Vishwakarma, *supra.*
[84] US Payments Forum, *supra* at 24–25; *see also* EMVCo., *supra* at 42–43.

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

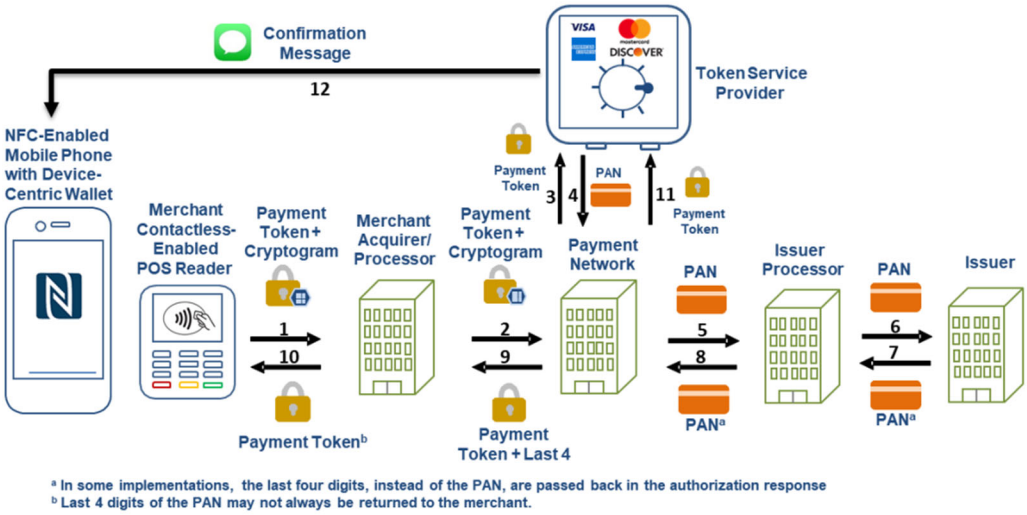
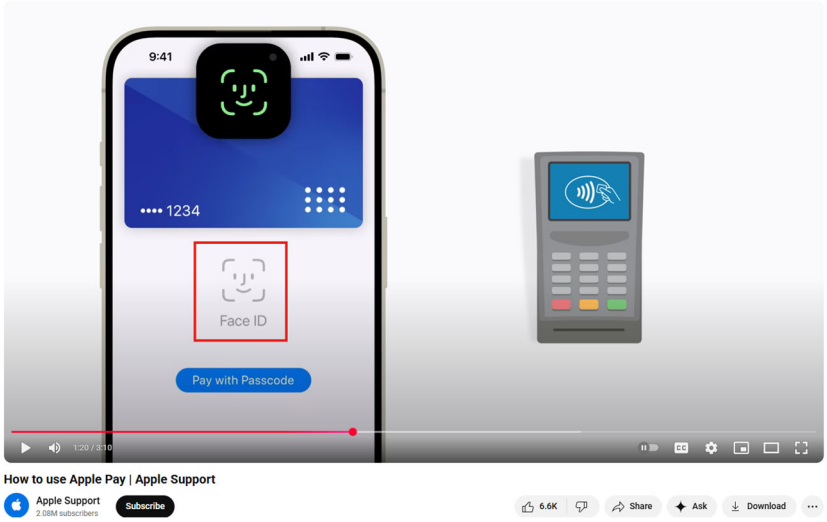


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

114. During a transaction, the user places the mobile device in proximity to the NFC reader in the POS terminal. As part of the process, the mobile device transmits transaction information. As part of the handshaking process, the POS terminal sends a signal that is received by the user's mobile device—"One device (usually the NFC reader) generates an electromagnetic field to establish a connection."[85]

115. The processor is configured to prompt the user to provide biometric information to the biometric reading device.[86]



116. In the Accused Instrumentalities, the Accused Instrumentalities generate a key. For example, the EMV standard described above involves the generation of a cryptogram after authentication. A cryptogram (also known as a token cryptogram or a "transaction specific dynamic security code") is a secure code generated during a transaction that verifies the transaction and helps prevent fraud. The payment network validates the cryptogram and de-tokenizes the token to determine the PAN, which is then processed by the payment network. Thus, the cryptogram acts as a key to the transaction.

---

[85] Nelson, *supra*.
[86] Apple Support, *How to use Apple Pay*, *supra*.

117. In the Accused Instrumentalities, the processor is configured to secure the payment information stored in the memory. Credit card payment information (which qualifies as payment information) is stored in memory.[87] The biometric authentication information is associated with the transaction information in that the card owner is also the iPhone's user. The secure element also may be used to store card information.[88]

> After your card is approved, your bank, your bank's authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such as the key used to generate dynamic security codes that are unique to each transaction) to Apple. The Device Account Number can't be decrypted by Apple but is stored in the Secure Element — an industry-standard, certified chip designed to store your payment information safely — on your device. Unlike with usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS, watchOS, macOS, and visionOS, is never stored on Apple servers, and is never backed up to iCloud.

118. In the Accused Instrumentalities, the processor is configured to transmit to the POS device, via the short-range RF circuitry, the key and the secured payment information for use in the secure transaction. For example, as described above, the EMV standard involves transmitting the cryptogram and the secured payment information from the Accused Instrumentality to the POS device.

119. Apple committed the infringing activities without license from Mobility IP. Apple's acts of infringement have damaged Mobility IP, as owner of the '412 Patent. Mobility IP is entitled to recover from Apple the damages it has sustained as a result of Apple's wrongful acts in an amount subject to proof at trial. The infringement of the '412 Patent by Apple has damaged Plaintiff.

Count VII: Infringement of U.S. Patent No. 10,762,187

120. All preceding factual allegations are incorporated as if fully set forth herein.

---

[87] Apple Platform Security, *Apple Pay component security*, *supra*.
[88] Apple, *Apple Pay security and privacy overview*, *supra*; *see also* Hoodja, *supra* ("card details ... are stored in the iPhone's Secure Element, which is a dedicated chip designed to store sensitive information.")

121. The USPTO duly and legally issued U.S. Patent No. 10,762,187 to Mr. Franciso Martinez de Velasco Cortina and Mr. Manfred Rietzler as named inventors. All right, title, and interest in the '187 Patent have been assigned to Mobility IP.

122. The '187 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

123. Apple has directly infringed the '187 Patent. The infringing acts include, but are not limited to, the manufacture, use, sale, importation, and/or offer for sale of the Accused Instrumentalities to practice the claimed invention in the '187 Patent. For example, Claim 1 of the '187 Patent[89] recites:

> A mobile device, comprising:
>
> > short range radio frequency (RF) circuitry;
> >
> > memory configured to store biometric authentication information and payment information;
> >
> > a biometric module configured to read biometric information;
> >
> > an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and
> >
> > a secure module configured to:
> >
> > > generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;
> > >
> > > encrypt the key and the payment information stored in memory; and
> > >
> > > provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

124. The Accused Instrumentalities meet the recited elements of Claim 1.

[89] Claim 1 is referenced herein for representative purposes. Plaintiff reserves the right to identify additional asserted claims and reserves its right to provide greater detail and scope via its Infringement Contentions at the time required under this Court's scheduling order.

125. The Accused Instrumentalities include short-range radio frequency circuitry. For example, the Apple iPhone 14 Pro includes multiple radios, including "NFC with reader mode":[90]

Cellular and Wireless

- Model A2650*
  - 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n77, n78 n79)
  - 5G NR mmWave (Bands n258, n260, n261)
  - FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71)
  - TD-LTE (Bands 34, 38, 39, 40, 41, 42, 46, 48, 53)
  - UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - GSM/EDGE (850, 900, 1800, 1900 MHz)
- Model A2651*
  - 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n77, n78 n79)
  - 5G NR mmWave (Bands n258, n260, n261)
  - FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71)
  - TD-LTE (Bands 34, 38, 39, 40, 41, 42, 46, 48, 53)
  - UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - GSM/EDGE (850, 900, 1800, 1900 MHz)
- All models
  - 5G (sub-6 GHz and mmWave) with 4x4 MIMO[8]
  - Gigabit LTE with 4x4 MIMO and LAA[8]
  - Wi-Fi 6 (802.11ax) with 2x2 MIMO
  - Bluetooth 5.3
  - Ultra Wideband chip for spatial awareness[9]
  - NFC with reader mode
  - Express Cards with power reserve

126. The NFC chip and antenna of an iPhone 14 Pro can be seen in the following images of a teardown:[91]

[90] Apple, *iPhone 14 Pro – Technical Specifications*, *supra*.
[91] Vishwakarma, *supra*.

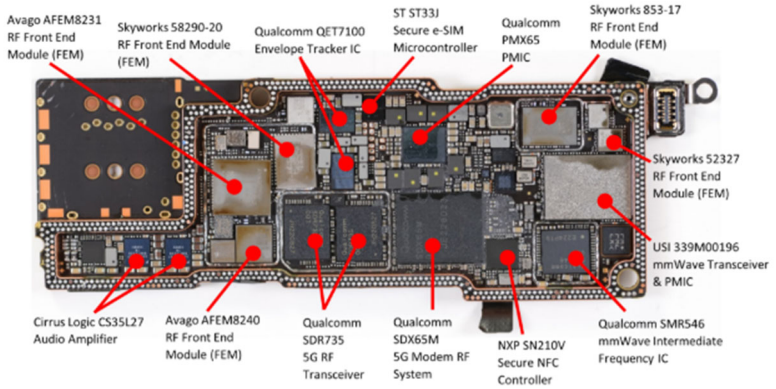


Figure 11

The new iPhone 14 lineup features MagSafe charging that Apple first introduced with the iPhone 12. MagSafe charging uses magnets for easier Qi-charging by snapping on to the back of iPhones with the capability. The magnetic ring embedded under the wireless charging coil along with a vertical strip of magnet below the ring is identical to the system on the iPhone 13 series. The wireless charging further houses a wireless charging coil along with the NFC antenna used for Apple Pay transactions.

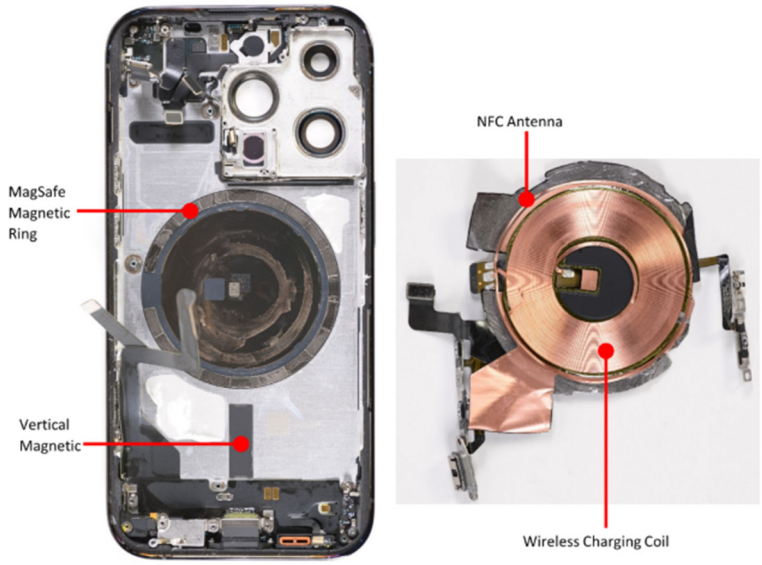
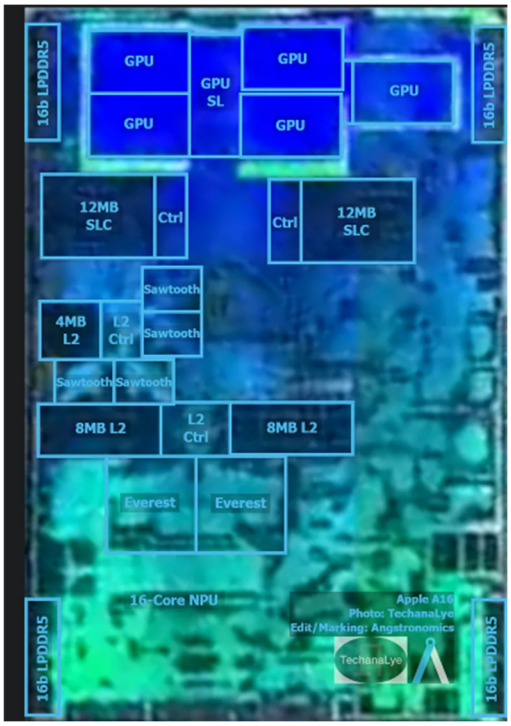


Figure 13: MagSafe system

127. The Accused Instrumentalities include memory. The memory is configured to store payment information and fingerprint information. For example, the Accused Instrumentalities include random access memory (RAM) which qualifies as memory.[92]

[92] Skyjuice, *supra*; *see also* GSMArena, *supra*.



128. The memory is used to store biometric authentication information and payment information. For example, Apple's iPhones use a secure subsystem called the Secure Enclave to store sensitive data such as biometric information and transaction information.[93] All of the Accused Instrumentalities have the Secure Enclave system.[94]

129. The Accused Instrumentalities store sensitive data such as biometric authentication information and transaction information in a variety of different ways. Face ID and Touch ID information, which qualify as "biometric authentication information" is "encrypted and protected by the Secure Enclave."[95] Credit card payment information (which qualifies as payment information) is stored in memory.[96] The biometric authentication information is associated with

[93] Apple Platform Security, *The Secure Enclave*, *supra*.
[94] *Id.*
[95] Apple, *About Face ID advanced technology*, *supra*; Apple, *About Touch ID advanced technology*, *supra*.
[96] Apple Platform Security, *Apple Pay component security*, *supra*.

the transaction information in that the card owner is also the iPhone's user. The secure element also may be used to store card information.[97]

> After your card is approved, your bank, your bank's authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such as the key used to generate dynamic security codes that are unique to each transaction) to Apple. The Device Account Number can't be decrypted by Apple but is stored in the Secure Element — an industry-standard, certified chip designed to store your payment information safely — on your device. Unlike with usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS, watchOS, macOS, and visionOS, is never stored on Apple servers, and is never backed up to iCloud.

130. Apple's Accused Instrumentalities include a biometric module configured to read biometric information. For example, the Accused Instrumentalities include either a fingerprint sensor (Touch ID) or facial recognition (Face ID):[98]

> **Use Touch ID to unlock your iPhone or make purchases**
>
> After you set up Touch ID, you can use Touch ID to unlock your iPhone. Just press the Touch ID sensor using the finger that you registered with Touch ID.

> **Use Face ID on your iPhone or iPad Pro**
>
> Face ID lets you securely unlock your iPhone or iPad, authenticate purchases, sign in to apps, and more — all with just a glance.

[97] Apple, *Apple Pay security and privacy overview*, *supra*; *see also* Hoodja, *supra* ("card details ... are stored in the iPhone's Secure Element, which is a dedicated chip designed to store sensitive information.")
[98] Apple, *Use Touch ID on iPhone and iPad*, *supra*; Apple, *Use Face ID on your iPhone or iPad Pro*, *supra*.

131. The Accused Instrumentalities include an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory. For example, in the Accused Instrumentalities, the user authenticates himself/herself using biometric information, such as through the use of Touch ID or Face ID. Face ID works by projecting infrared dots on a user's face, then comparing the resulting three-dimensional image to the version stored on the mobile device.[99]

132. Touch ID uses an embedded fingerprint sensor built into the home button of some mobile devices.[100] The sensor uses capacitive touch to capture high-resolution images of the user's fingerprints, maps individual details and compiles the data together. Touch ID then uses the data to match and recognize fingerprints.[101]

133. The Face ID and Touch ID template are encrypted and stored by the Secure Enclave within the Accused Instrumentalities.[102] That data is then compared with the received biometric information.

134. The Accused Instrumentalities include one or more processors that can be configured as a secure module. For example, the Apple iPhone 14 Pro includes an A16 processor.[103]

---

[99] Zackdfilms, *supra*.
[100] Picaro, *supra*.
[101] *Id*.; Apple, *About Touch ID advanced technology*, *supra*
[102] Apple, *About Face ID advanced technology*, *supra*; Apple, *About Touch ID advanced technology*, *supra.*
[103] Vishwakarma, *supra*.

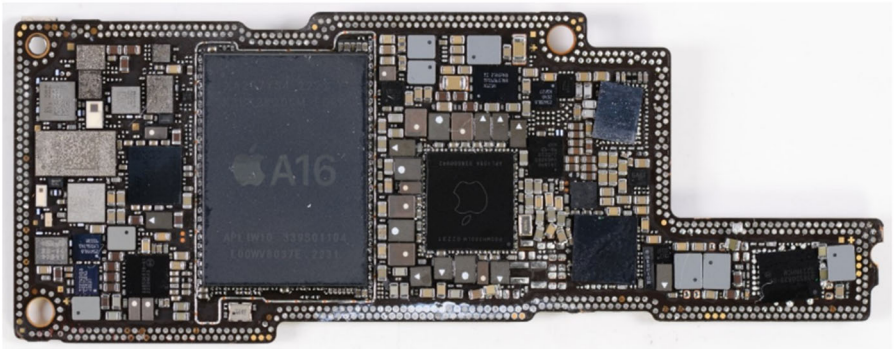


Figure 10

135. The processor is configured to generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory. For example, the Accused Instrumentalities follow EMV's standards for processing contactless payments.[104]

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

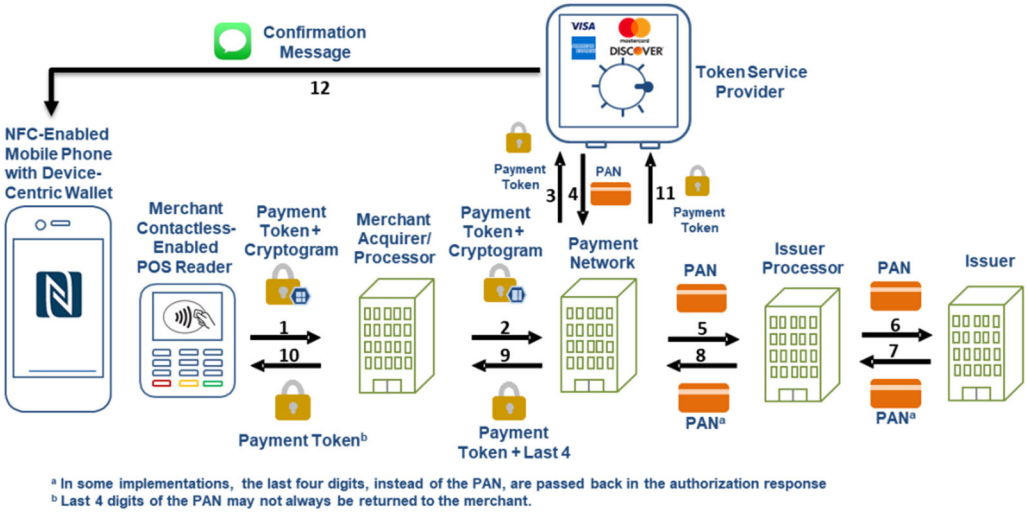


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

[104] US Payments Forum, *supra* at 24–25; *see also* EMVCo., *supra* at 42–43.

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

136. In the Accused Instrumentalities, the Accused Instrumentalities generate a key. For example, the EMV standard described above involves the generation of a cryptogram after authentication. A cryptogram (also known as a token cryptogram or a "transaction specific dynamic security code") is a secure code generated during a transaction that verifies the transaction and helps prevent fraud. The payment network validates the cryptogram and de-tokenizes the token to determine the PAN, which is then processed by the payment network. Thus, the cryptogram acts as a key to the transaction.

137. In the Accused Instrumentalities, the user authenticates himself/herself using biometric information, such as through the use of Touch ID or Face ID. Face ID works by

projecting infrared dots on a user's face, then comparing the resulting three-dimensional image to the version stored on the mobile device.[105]

138. Touch ID uses an embedded fingerprint sensor built into the home button of some mobile devices.[106] The sensor uses capacitive touch to capture high-resolution images of the user's fingerprints, maps individual details and compiles the data together. Touch ID then uses the data to match and recognize fingerprints.[107]

139. In the Accused Instrumentalities, the processor is configured to encrypt the key and the payment information stored in the memory. Credit card payment information (which qualifies as payment information) is stored in memory.[108] The biometric authentication information is associated with the transaction information in that the card owner is also the iPhone's user. The secure element may also be used to store card information.[109]

> After your card is approved, your bank, your bank's authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such as the key used to generate dynamic security codes that are unique to each transaction) to Apple. The Device Account Number can't be decrypted by Apple but is stored in the Secure Element — an industry-standard, certified chip designed to store your payment information safely — on your device. Unlike with usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS, watchOS, macOS, and visionOS, is never stored on Apple servers, and is never backed up to iCloud.

140. In the Accused Instrumentalities, the processor is configured to provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction. For example, as described above, the EMV standard involves transmitting the cryptogram and the secured payment information from the Accused Instrumentality to the POS device.

---

[105] Zackdfilms, *supra*.
[106] Picaro, *supra*.
[107] *Id*.; Apple, *About Touch ID advanced technology*, *supra*.
[108] Apple Platform Security, *Apple Pay component security*, *supra*.
[109] Apple, *Apple Pay security and privacy overview*, *supra*; *see also* Hoodja, *supra* ("card details ... are stored in the iPhone's Secure Element, which is a dedicated chip designed to store sensitive information.")

141. Apple committed the infringing activities without license from Mobility IP. Apple's acts of infringement have damaged Mobility IP, as owner of the '187 Patent. Mobility IP is entitled to recover from Apple the damages it has sustained as a result of Apple's wrongful acts in an amount subject to proof at trial. The infringement of the '187 Patent by Apple has damaged Plaintiff.

JURY DEMAND

142. Mobility IP hereby demands a trial by jury on all issues.

PRAYER

Wherefore, Mobility IP prays for entry of judgment as follows:

143. A judgment in favor of Mobility IP that Apple has infringed and is infringing, either literally and/or under the doctrine of equivalents, the Asserted Patents;

144. A judgment in favor of Mobility IP that Apple's infringement of the '345 patent and the '924 patent is willful and continues to be willful as of the date Apple received notice of its infringement through this lawsuit;

145. An award of damages in favor of Mobility IP adequate to compensate Mobility IP for Apple's infringement of the Asserted Patents which shall in no event be less than a reasonable royalty, together with interest and cost as fixed by the court pursuant to 35 U.S.C. § 284;

146. An award of enhanced damages in favor of Mobility IP against Apple for up to three times the award of actual damages for Apple's willful infringement of the '345 patent and '924 patent, pursuant to 35 U.S.C. § 284;

147. A permanent injunction in favor of Mobility IP against Apple enjoining Apple, its officers, agents, employees, and others acting in privity, from further infringement of the '345 and '924 Patents;

148. An award of an ongoing royalty for Apple's post-judgment infringement in the event a permanent injunction is not granted;

149. An award of attorneys' fees pursuant to 35 U.S.C. § 285 or as otherwise permitted by law in an amount deemed just and appropriate by the Court;

150. An award of costs and expenses as deemed appropriate by the Court; and

Any other legal or equitable relief to which Mobility IP is justly entitled.

Dated: March 4, 2026

Respectfully submitted,

/s/ Jason S. McManis

Jason S. McManis
State Bar No.: 24088032
Weining Bai
State Bar No.: 24101477
Thomas Delrosario
State Bar No.: 24110645
Justin Kenney
State Bar No.: 24126702
Ab Henry
State Bar No.: 24131987
Zach Grinovich
State Bar No.: 24149804
AHMAD, ZAVITSANOS & MENSING, PLLC
1221 McKinney Street, Suite 2500
Houston, Texas 77010
(713) 655-1101

Of Counsel:

Howard Wisnia
Wisnia PC
California Bar No. 184626
howard@wisnialaw.com
12636 High Bluff Dr., Suite 400
San Diego CA 92130
Tel: +1 858 461 0989

Andrea L. Fair
Texas Bar No. 24078488
andrea@wsfirm.com
WARD, SMITH & HILL, PLLC
1507 Bill Owens Parkway
Longview, Texas 75604
Tel: 903-757-6400
Fax: 903-757-2323

Attorneys for Plaintiff
Mobility IP Holdings, Inc.