UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

VINDOLOR, LLC, Plaintiff v. **WALMART, INC.,** Defendant	**Case No. 6:19-cv-00339** **JURY TRIAL DEMANDED**

PLAINTIFF'S ORIGINAL COMPLAINT

Plaintiff Vindolor, LLC ("Vindolor") hereby asserts the following claims for patent infringement against Defendant Walmart, Inc. ("Defendant" or "Walmart"), and alleges as follows:

THE PARTIES

1. Vindolor is a limited liability company organized and existing under the laws of the Texas with its principal place of business at 3616 Far West Blvd, Suite 117-292, Austin, Texas 78731.

2. Defendant is a corporation organized and existing under the laws of Delaware with corporate address of 702 S.W. 8th Street, Bentonville, Arkansas 72716.

JURISDICTION AND VENUE

3. This action arises under the patent laws of the United States, 35 U.S.C. § 1, *et seq*. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

4. Defendant has committed acts of infringement in this judicial district.

5. Defendant has a regular established place of business in this judicial district at 5017 W. E Hwy 290, Austin, Texas 78735.

6. Defendant has infringed U.S. Patent No. 6,213,391 ("the '391 Patent") in Texas by, among other things, engaging in infringing conduct within this judicial district. For example, Defendant has purposefully and voluntarily sold one or more infringing products, as described below, in this judicial district.

7. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1400(b).

OVERVIEW OF THE '391 PATENT

8. Vindolor is the owner, by assignment, of the '391 Patent, entitled PORTABLE SYSTEM FOR PERSONAL IDENTIFICATION BASED UPON DISTINCTIVE CHARACTERISTICS OF THE USER, which issued on April 10, 2001. A copy of the '391 Patent is attached as **Exhibit A**.

9. The '391 Patent describes in detail and claims inventions in systems conceived by William H. Lewis for electronic personal identification.

10. As described in the following passages from the specification of the '391 Patent, there were problems and shortcomings in the then-existing field of ***portable electronic personal identification systems***. *Id.* at col. 3, l. 47 – col. 7, l. 13.

11. Claim 1 of the '391 Patent recites:

> 1. A portable identification system comprising
>
> [a] a storage medium for storing electronic data;
>
> [b] one or more inputs; one or more outputs;
>
> [c] a verifying means for determining user authorization or non-authorization, said verifying means receiving data from at least one of said one or more inputs, which data is derived from biometric or other distinctive characteristics of the user, said verifying means generating an

identification profile for each user, wherein said identification profile is determined from said data, and

[d] a code generator employing at least one code generating algorithm for generating one or more access codes based upon said identification profile wherein at least one of the said one or more access codes is an identification specific digital signature.

Id. at col. 12, ll. 24-37.

12. The claimed invention of the '391 Patent recites an ordered combination of elements that were not conventional in prior portable electronic personal identification systems.

13. For example, claim 1 of the '391 Patent recites a verifying means element that determines the user authorization prior to the code generator element generating an access code that is an identification specific digital signature. Because the code generator generates the access code after the verifying means determines the user authorization, the claimed invention of the '391 Patent improves security and reduces the risk of a data breach of the portable electronic personal identification system because the access code is not stored and available on the portable identification system.

14. As another example, claim 1 of the '391 Patent recites a verifying means element that generates an identification profile and a code generator that generates an access code based on the identification profile. By generating the access code based on the generated identification profile, the claimed invention of the '391 Patent improves security and reduces the risk of a fraudulent transaction because a false profile cannot be inserted into the claimed system.

15. Additionally, by generating an access code that is an identification specific digital signature, the claimed invention of the '391 Patent improves efficiency and security of

the portable electronic identification system because the access code functions as an authorization code for another system as well as it functions to identify the user in a single access code. The combination of an access code and identification signature reduces the data transmitted from the personal identification system in order to authorize access and identify the user. The combination of an access code and identification signature also reduces the risk of fraudulent transactions because a successful fraudulent access code would need to incorporate identification specific digital signature characteristics as well as an appropriate authorization code. The generation of an access code that is an identification specific digital signature was not conventional at the time the '391 Patent application was filed.

16. As appreciated from the substance and disclosure of the '391 Patent application, the record disclosed from the examination of the '391 Patent, including the statements in the notice of allowance, the record of the prior art identified and considered by the examiner, and the patents and patent applications citing to and discusses the '391 Patent, the claimed inventions of the '391 Patent:

- increase the accuracy of portable electronic personal identification systems, which had been an issue with prior systems;
- improve the security and portability of portable electronic personal identification systems, which had been an issue with prior systems;
- improve personal identification security of portable electronic personal identification systems, which had been an issue with prior systems;
- improve the ease and flexibility of use of portable electronic personal identification systems, which had been an issue with prior systems;
- decrease fraudulent transactions associated with the use portable electronic personal identification systems, which had been an issue with prior systems;

- improve the uniqueness of access codes generated by portable electronic personal identification systems, which had been an issue with prior systems;
- improve the complexity of access codes generated by portable electronic personal identification systems while improving its ease of using the portable electronic personal identification systems, which had been an issue with prior systems;
- improve the security and uniqueness of access codes generated by portable electronic personal identification systems by generating an access code that is an identification specific digital signature, which had been an issue with prior systems;
- improve the security and uniqueness of access codes generated by portable electronic personal identification systems by generating an access code that is identification specific, which had been an issue with prior systems;
- improve portable electronic personal identification systems by requiring positive identification prior to granting access to a secure objective, which had been an issue with prior systems;
- reduce risks associated with security and data breaches of portable electronic personal identification systems, which had been an issue with prior systems;
- reduce infrastructure, support, and maintenance of portable electronic personal identification systems, which had been an issue with prior systems;
- increase the efficiencies of portable electronic personal identification systems, which had been an issue with prior systems;
- reduce infrastructure, support, and maintenance of portable electronic personal identification systems, which had been an issue with prior systems; and
- are directed to improvements in the electronic personal identification technology itself and not directed to generic components performing conventional activities.

See, e.g., id. at col. 1, l. 16 – col. 12, l. 39, *infra.*

17. The '391 Patent describes and claims novel and inventive technological improvements and solutions to such problems and shortcomings, including an improved portable system for personal identification based on distinctive characteristics of the user. *Id.* at col. 3, l. 35 – col. 12, l. 39.

18. The '391 Patent describes and claims systems that solve a technical problem—how to provide a portable identification system with accurate means of identifying a particular known or unknown person that utilizes a biometric input and generates an access code that is an identification specific digital signature. *Id.*

19. The technological improvements and solutions described and claimed in the '391 Patent were not conventional or generic at the time of their respective inventions but involved novel and non-obvious approaches to the problems and shortcomings prevalent in the art at the time. *Id.*

20. The inventions claimed in the '391 Patent involve and cover more than just the performance of well-understood, routine or conventional activities known to the industry prior to the invention of such novel and non-obvious systems and devices by the '391 Patent inventor. *Id.*

21. The inventions claimed in the '391 Patent represent technological solutions to technological problems. The written description of the '391 Patent describes in technical detail each of the limitations of the claims, allowing a person of ordinary skill in the art to understand what the limitations cover and how the non-conventional and non-generic combination of claim elements differ markedly from and improved upon what may have been considered conventional or generic. *Id.*

22. As demonstrated above by its frequent citation (over 265) by the United Stated Patent Office in other later-issued patents, reexaminations, and patent applications, the '391 Patent represents a fundamental technical improvement in the area of electronic identification systems.

"USPTO Patent Full-Text and Image Database – ref/6213391" ("**USPTO Patent Search**"), available at http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=6213391.PN.&OS=PN/6213391&RS=PN/6213391 (last accessed April 9, 2018), "USPTO Patent Application Full Text and Image Database" ("**USPTO Patent Application Search**"), http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=0&f=S&l=50&TERM1=6213391&FIELD1=&co1=AND&TERM2=&FIELD2=&d=PG01 (last accessed April 9, 2018).

23. These patents were issued to such companies as:

- Amazon Technologies, Inc.,
- American Express Travel Related Services Company, Inc.,
- Apple, Inc.,
- AT&T Corp.,
- Bell South Intellectual Property Corporation,
- Citicorp Development Center, Inc.,
- Exxonmobile Research & Engineering Company,
- First Data Corporation,

- First USA Bank, N.A.,
- Fujitsu Limited,
- International Business Machines Corporation,
- JP Morgan Chase Bank,
- Mastercard International, Inc.,
- Motorola, Inc.,
- Palm, Inc.,
- Securecard Technologies, Inc.,
- Sprint Communications Company, L.P.,
- The Western Union Company, and
- Visa U.S.A., Inc.

USPTO Patent Search.

24. The portable identification system of claim 1 of the '391 Patent includes a storage medium, one or more inputs, one or more outputs, a verifying means, and a code generator, all working together in a specific way to determine a user's authorization based on data derived from biometric or other distinctive characteristics of the user and then to generate an access code employing a code generating algorithm to generate one or more access codes based upon an identification profile wherein at least one of the generated access codes is an identification specific digital signature. The claimed system is directed to a specific, concrete, technological solution that improves personal identification for secure transactions.

25. The portable identification system of Claim 1 of the '391 Patent is tied to a "tangible machine" (a device with a storage medium, one or more inputs, one or more outputs, a verifying means, and a code generator, etc.) performing specific functions.

26. The portable identification system of Claim 1 of the '391 Patent covers security improvements to specific portable identification systems for authorizes user's using access codes that are an identification specific digital signature, and thus is fundamentally distinct from conventional methods and systems.

27. Viewed in light of the patent's specification, the '391 Patent claims are not directed to basic tools of scientific and technological work, nor are they directed to a fundamental economic practice. In particular, the use of a code generator after verifying and determining a user's authorization based on data derived from biometric or other distinctive characteristics of the user, as claimed, employing the code generating algorithm to generate one or more access codes based upon an identification profile wherein at least one of the generated access codes is an identification specific digital signature is not a basic tool of scientific or technological work, nor is it directed to a fundamental economic practice.

28. The '391 Patent claims are not directed to the use of an abstract mathematical formula on any general-purpose computer, or a purely conventional computer implementation of a mathematical formula, or generalized steps to be performed on a computer using conventional activity. In particular, the use of a code generator after verifying and determining a user's authorization based on data derived from biometric or other distinctive characteristics of the user, as claimed, employing the code generating algorithm to generate one or more access codes based upon an identification profile

wherein at least one of the generated access codes is an identification specific digital signature is not an abstract mathematical formula that is computed on any general-purpose computer, nor does it rely on a purely conventional computer implementation of an abstract mathematical formula, nor is it based on generalized steps to be performed on a computer using conventional activity.

29. The '391 Patent claims are not directed to a method of organizing human activity or to a fundamental economic practice long prevalent in our system of commerce. In particular, the use of a code generator after verifying and determining a user's authorization based on data derived from biometric or other distinctive characteristics of the user, as claimed, employing the code generating algorithm to generate one or more access codes based upon an identification profile wherein at least one of the generated access codes is an identification specific digital signature is not directed to a method of organizing human activity nor is it directed to a fundamental economic practice long prevalent in our system of commerce.

30. The inventions claimed in the '391 Patent do not take a well-known or established business method or process and apply it to a general-purpose computer. In particular, the use of a code generator after verifying and determining a user's authorization based on data derived from biometric or other distinctive characteristics of the user, as claimed, employing the code generating algorithm to generate one or more access codes based upon an identification profile wherein at least one of the generated access codes is an identification specific digital signature was not a well-known or established business method or process.

31. The '391 Patent was examined by Primary Examiner Karl D. Frech.

32. The '391 Patent was examined and approved for granting by Primary Examiner Michael G. Lee.

33. The '391 Patent was examined and approved for granting by Assistant Examiner Diane I. Lee.

34. On November 27, 2000, Examiner Diane I. Lee issued a notice of allowance for the '391 Patent, which is noted with her signature on the notice of allowance.

35. Supervisory Examiner Michael G. Lee approved the issuance of the notice of allowance for the '391 Patent, which is noted by his signature on the notice of allowance.

36. As stated in the notice of allowance:

> The following is an examiner's statement of reasons for allowance: Mueller discloses an apparatus for identity verification using a portable data card having a first memory as a storage medium for storing electronic data, a card reader as an input device for reading data from a portable data card storing electronic data such as a user information (such as name, public key, public network key, user reference feature, and etc.), a feature extractor as an additional input device for extracting biometric data or distinctive characteristics of the user such as a voice or fingerprints and introducing personal identification information into the storage medium, and wherein the data stored on the card and the extracted personal identification information are introduced into the storage medium for generating an identification profile for each user which is determined from input data, outputs device, the central processing device and the security service station as a verifying means for determining user authorization or non-authorization, a processing device of the terminal receives the reference feature data and the DES-key from the card are encrypted with a public network key to form a first cryptogram which serves as an identification profile and wherein the identification profile is determined from the input data the verifying means then determines whether the user is authorized or not authorized, and a random number generator employing at least one code generator algorithm for converting the DES-key of identification profile into a random access code. Mueller does not disclose the access code generated by the code generator is an identification specific digital signature profile which used to encode data for secure transmission.

> Lane discloses an identification card having an input device having fingerprint sensor for capturing the fingerprints of the user, a storage medium for storing the user's fingerprint information, a display and a speaker as output devices, a controller/authenticator for verifying an authorized user by a comparison with the stored fingerprints and the captured fingerprint, and upon a successful match, the output device provide a vidual [sic] indication with LED light and audibly indicating (i.e., with tone) that the obtained user information is authenticated. Land does not teaches [sic] the authenticated signal is an identification specific digital signature profile. In view of Muller and Lane, one of ordinary skill in the art would not have been motivated to modify the teachings of Muller and Lane in order to obtain a portable identification system having a generator employing the code generating algorithm to transform the access code into an identification specific digital signature profile when the determination of user is made, as set forth in the claims.

'391 Patent, Notice of Allowance and Issue Fee Due ("**Notice of Allowance**"), Paper 21 at pp. 2-3, Nov. 27, 2000, *available at* https://portal.uspto.gov/pair/view/BrowsePdfServlet?objectId=HUMTHFZEPXXIFW4&lang=DINO (last accessed April 9, 2018).

37. As noted in the Notice of Allowance, the portable identification system of claim 1 of the '391 Patent does not take existing information and organize it into a new form. In particular, the claimed system employs a code ***generator***, after verifying and determining a user's authorization based on data derived from biometric or other distinctive characteristics of the user, to ***generate an access code*** based on an identification profile wherein at least one of ***the generated access codes is an identification specific digital signature***. The system of Claim 1 generates the identification specific digital signature access code, not to organize it, but to more securely generate an identification specific access code. The generation of an

identification specific digital signature was not conventional with respect to portable electronic personal identification technology and systems.

38. In the process of reviewing the patentability of the '391 Patent, one or more examiners at the USPTO reviewed and considered the disclosure of:

- U.S. Patent No. 4,148,012 to Baump et al;
- U.S. Patent No. 4,218,738 to Matyas et al;
- U.S. Patent No. 4,264,782 to Konheim;
- U.S. Patent No. 4,315,101 to Atella;
- U.S. Patent No. 4,438,824 to Mueller-Schloer;
- U.S. Patent No. 4,630,201 to White;
- U.S. Patent No. 4,804,825 to Bitoh;
- U.S. Patent No. 4,825,050 to Griffith et al;
- U.S. Patent No. 4,827,518 to Feustal et al;
- U.S. Patent No. 4,961,229 to Takahashi;
- U.S. Patent No. 4,993,068 to Piosenka et al;
- U.S. Patent No. 4,998,279 to Weiss;
- U.S. Patent No. 5,151,684 to Johnsen;
- U.S. Patent No. 5,276,444 to McNair;
- U.S. Patent No. 5,313,556 to Parra;
- U.S. Patent No. 5,386,103 to DeBan et al;
- U.S. Patent No. 5,513,272 to Bogosian, Jr;
- U.S. Patent No. 5,552,777 to Gokcebat et al;
- U.S. Patent No. 5,581,630 to Bonneau, Jr;

- U.S. Patent No. 5,594,493 to Nemirofsky;
- U.S. Patent No. 5,623,552 to Lane;
- U.S. Patent No. 5,793,027 to Baik;
- U.S. Patent No. 5,815,658 to Kuriyama;
- U.S. Patent No. 5,825,871 to Mark;
- U.S. Patent No. 5,825,882 to Kowalski et al;
- U.S. Patent No. 5,870,724 to Lowlor et al;
- German Patent Document No. 3731773 (DE);
- Japanese Patent Document No. 4-135293 (JP);
- "High-Tech Building Security", Siuru, Bill, *Popular Electronics*, Dec. 1996, pp. 39–42, 46;
- "Who Goes There?", Wyner, Peter, *Byte*, vol. 22, No. 6, Jun. 1997, pp. 70–80;
- "No Place to Hide", Marsh, Ann, *Porhes*, Sep. 22, 1997, pp. 226–234;
- "The Generation Gap", Vesley, Rebecca, *Wired*, Oct. 1997, pp. 53–56, 207; and
- "Look. Forward", *Internet User Magazine*, Summer 1997, pp. 11, 12, 14, 21.

39. As noted by the United States Patents, foreign patent documents, and other publications cited by the '391 Patent, the claimed inventions of the '391 Patent do not preempt the field of its invention or preclude the user of other electronic personal identification systems. Instead, the claims of the '391 Patent cover very specific technologies used on specialized devices (*e.g.,* the use of a code generator after verifying and determining a user's authorization based on data derived from biometric or other

distinctive characteristics of the user, as claimed, employing the code generating algorithm to generate one or more access codes based upon an identification profile wherein at least one of the generated access codes is an identification specific digital signature) while leaving open other known or unknown technology for identifying a user.

40. Many means and methods exist for portable electronic personal identification not covered by the claims of the '391 Patent. The art cited by the Examiners in the examination of the '391 Patent all represent patentably distinct and in some instances prior art means and methods for electronic personal identification from those of the '391 Patent.

INFRINGEMENT OF U.S. PATENT NO. 6,213,391

41. Vindolor incorporates by reference and alleges all of the foregoing paragraphs of this Complaint as if fully set forth herein.

42. Prior to September 10, 2017, Defendant operated multiple retail establishments where it offered goods for sale to customers, including, but not limited to, Apple mobile devices and Samsung mobile devices (among others) (the "Accused Infringing Devices").

43. Prior to September 10, 2017, Defendant has sold the Accused Infringing Devices in the United States, including within this judicial district.

44. The Accused Infringing Devices are non-limiting examples that were identified based on publicly available information, and Vindolor reserves the right to identify additional infringing activities, products and services, including, for example, on the basis of information obtained during discovery.

45. The Accused Infringing Devices are portable devices that implement a portable identification system wherein the system comprises a storage medium for storing

electronic data; one or more inputs; one or more outputs; a verifying means for determining user authorization or non-authorization, said verifying means receiving data from at least one of said one or more inputs, which data is derived from biometric or other distinctive characteristics of the user, said verifying means generating an identification profile for each user, wherein said identification profile is determined from said data, and a code generator employing at least one code generating algorithm for generating one or more access codes based upon said identification profile wherein at least one of the said one or more access codes is an identification specific digital signature.

46. Defendant has infringed claims 1 and 2 of the '391 Patent in the United States by using, offering to sell, and selling without authority, the Accused Devices in violation of 35 U.S.C. § 271(a).

47. As just one non-limiting example, set forth below (with claim language in italics) is a description of infringement of exemplary Claim 1 of the '391 Patent in connection with an Apple iPhone 6 and the Apple Pay service. This description is based on publicly available information. Vindolor reserves the right to modify this description, including, for example, on the basis of information about the Accused Products that it obtains during discovery.

1(a) A portable identification system comprising: –

48. Defendant has used and has supported the Apple Pay service.

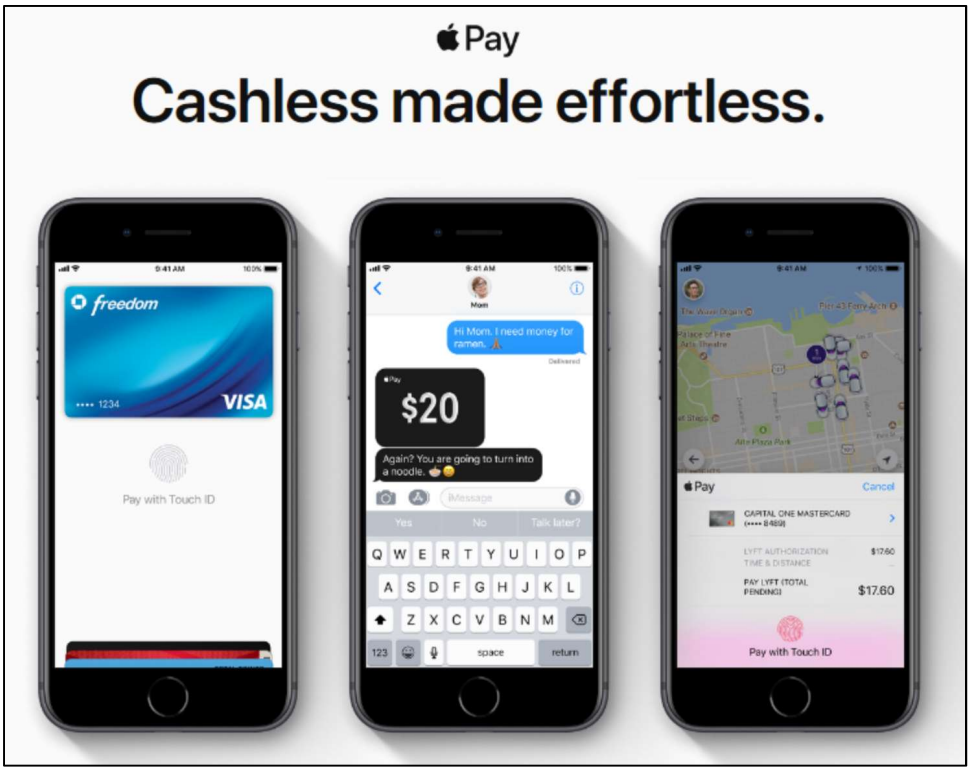
49. Defendant's customers have possessed Apple iPhones, such as the iPhone 6, that support the Apple Pay service.

50. With the iPhone 6 configured with a customer's credit card account, Defendant has initiated a credit card transaction with use of a NFC-enabled credit card payment terminal ("POS terminal") and a connection to a credit card processing server.

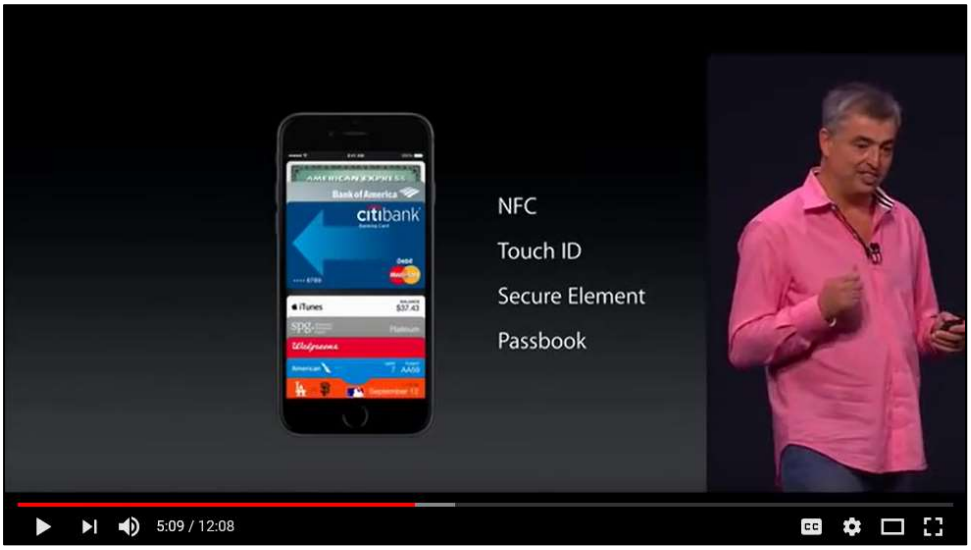
51. The iPhone 6 includes Touch ID, which provides biometric fingerprint identification, authorization, and verification for Apple Pay.

52. The iPhone 6 is a small, lightweight, portable, computing system.

53. As supported by the disclosures of Apple, the iPhone 6 is a portable identification system.

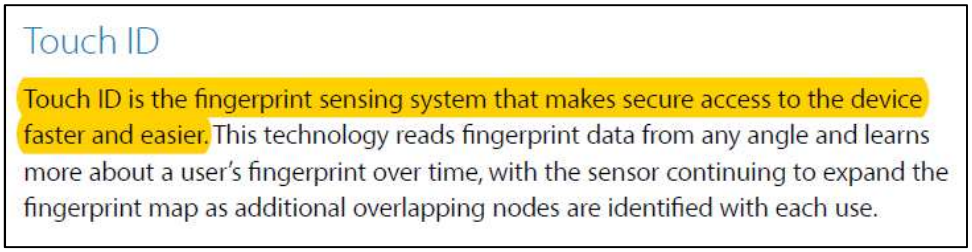


"Cashless made effortless" ("**Cashless Made Effortless**"), *available at* https://www.apple.com/apple-pay/ (last accessed April 9, 2018).



"Apple Pay Presentation (Sept 2014)" ("**Apple Pay Presentation**"), *available at* https://www.youtube.com/watch?v=5ExcCyS1ZH8 (last accessed April 9, 2018).

"iPhone – Guided Tour: Apple Pay" ("**iPhone – Guided Tour: Apple Pay**"), *available at* https://www.youtube.com/watch?v=ez-2M3C_4wU (last accessed April 9, 2018).



Touch ID

Touch ID is the fingerprint sensing system that makes secure access to the device faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use.

"iOS Security Guide," ("**iOS Security**"), *available at* https://www.apple.com/business/docs/iOS_Security_Guide.pdf, at 7 (last accessed April 9, 2018).

Use Touch ID for Apple Pay

With an iPhone 6 or iPhone 6 Plus or later, you can use Touch ID to make Apple Pay purchases in stores, within apps, and on websites in Safari. You can also use Touch ID on your iPhone to complete website purchases from your Mac. If you have an iPad Pro, iPad Air 2 or iPad Mini 3 or later, you can use Touch ID for Apple Pay purchases within apps and on websites in Safari.

"Use Touch ID on iPhone and iPad - Apple Support" ("**Use Touch ID**"), *available at* https://support.apple.com/en-us/HT201371 (last accessed April 9, 2018).

"iPhone 6 - Technical Specifications" ("**Technical Specifications**"), *available at* https://support.apple.com/kb/sp705?locale=en_US (last accessed April 9, 2018).

Touch ID

- Fingerprint identity sensor built into the Home button

Apple Pay

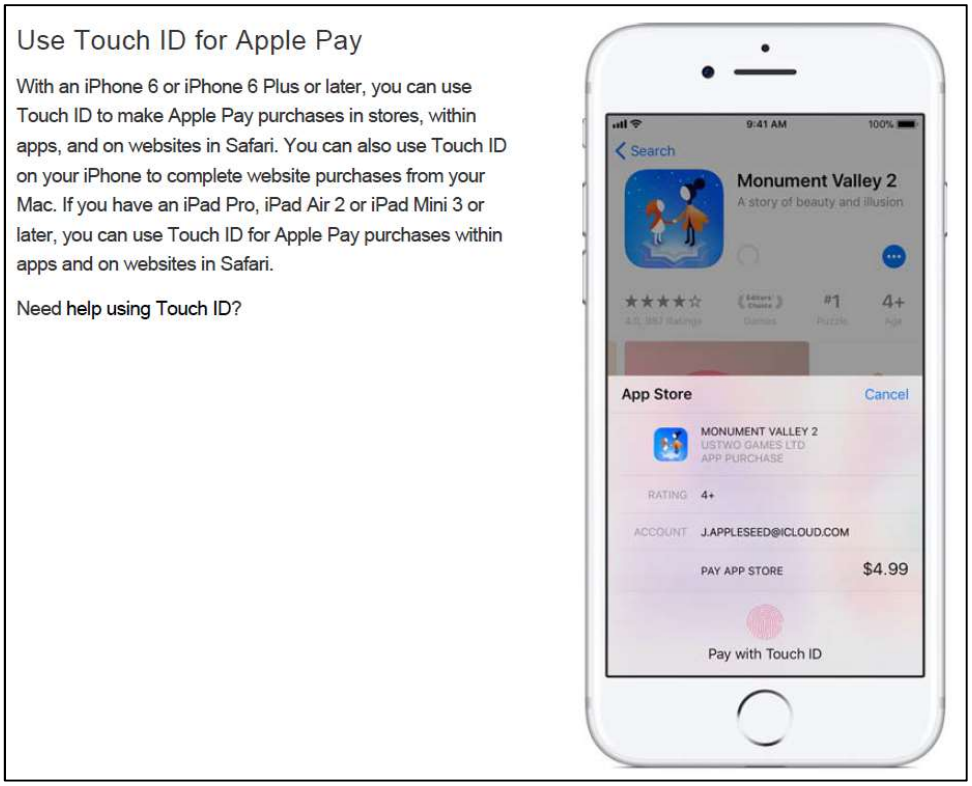
- Pay with your iPhone using Touch ID in stores and in apps

Id.

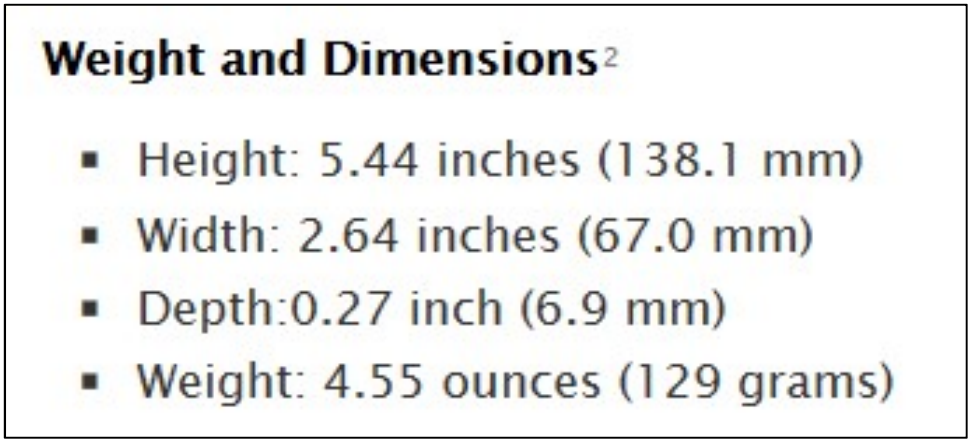
Touch ID

Touch ID is the fingerprint sensing system that makes secure access to the device faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use.

iOS Security at 7.



Use Touch ID.



Technical Specifications.

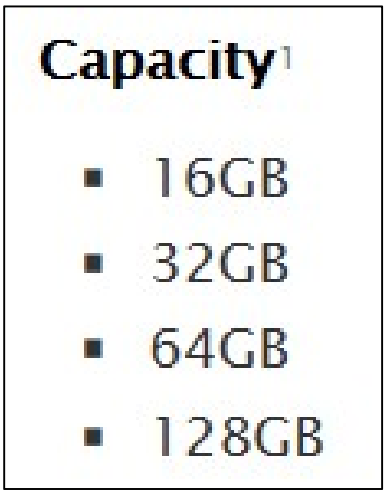
1(b) a storage medium for storing electronic data; –

54. The iPhone 6 includes multiple memories for storing electronic data.

55. Those memories include, RAM, flash memory, a Secure Enclave chip, and a Secure Element.

56. The Secure Enclave and Secure Element store enrolled fingerprint data and payment information, including the Device Account Number.

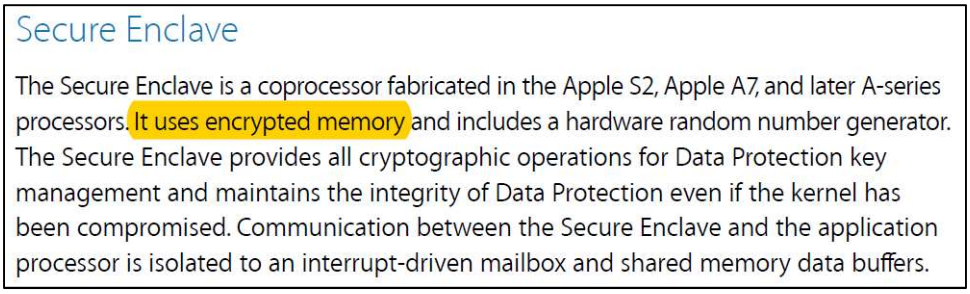
57. As supported by the disclosures of Apple, the enrolled fingerprint data and Device Account Number are electronic data, and the RAM, flash memory, Secure Enclave, and Secure Element, including associated memory circuitry, in the iPhone 6 are storage mediums for storing electronic data.



Technical Specifications.

> Once your card is approved, your bank or your bank's authorized service provider 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 unique to each transaction) to Apple. Apple can't decrypt it, but will add it to the Secure Element within your device. The Secure Element is an industry-standard, certified chip designed to store your payment information safely. The Device Account Number in the Secure Element is unique to your device and to each credit, debit, or prepaid card added. It's isolated from iOS and watchOS, never stored on Apple Pay servers, and never backed up to iCloud. Because this number is unique and different from usual credit, debit, or prepaid card numbers, your bank or issuer can prevent its use on a magnetic stripe card, over the phone, or on the web.

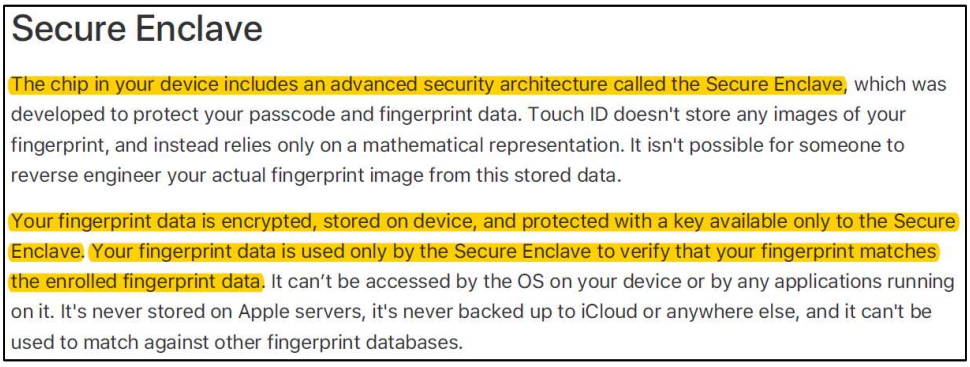
"Apple Pay security and privacy overview - Apple Support" (**"Apple Pay Security"**), *available at* https://support.apple.com/en-us/HT203027 (last accessed April 9, 2018).



Secure Enclave

The Secure Enclave is a coprocessor fabricated in the Apple S2, Apple A7, and later A-series processors. It uses encrypted memory and includes a hardware random number generator. The Secure Enclave provides all cryptographic operations for Data Protection key management and maintains the integrity of Data Protection even if the kernel has been compromised. Communication between the Secure Enclave and the application processor is isolated to an interrupt-driven mailbox and shared memory data buffers.

iOS Security at p. 7.



Secure Enclave

The chip in your device includes an advanced security architecture called the Secure Enclave, which was developed to protect your passcode and fingerprint data. Touch ID doesn't store any images of your fingerprint, and instead relies only on a mathematical representation. It isn't possible for someone to reverse engineer your actual fingerprint image from this stored data.

Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave. Your fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data. It can't be accessed by the OS on your device or by any applications running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases.

"About Touch ID advanced security technology" (**"About Touch ID"**), *available at* https://support.apple.com/en-us/ht204587 (last accessed April 9, 2018).

1(c) one or more inputs; –

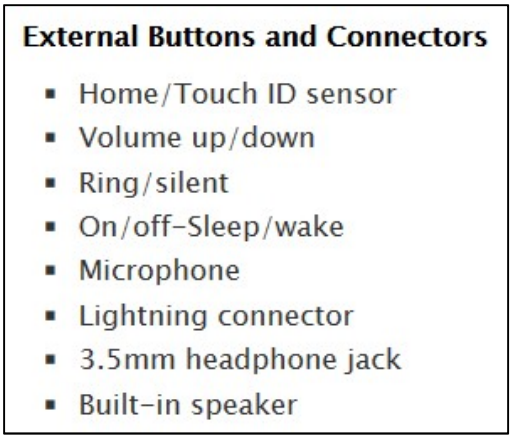
58. The iPhone 6 includes several inputs, including the Touch ID sensor and multiple wireless radios (cellular, Wi-Fi, and NFC).

59. The Touch ID sensor allows for the input of fingerprint images for processing into a mathematical representation of a user's fingerprint.

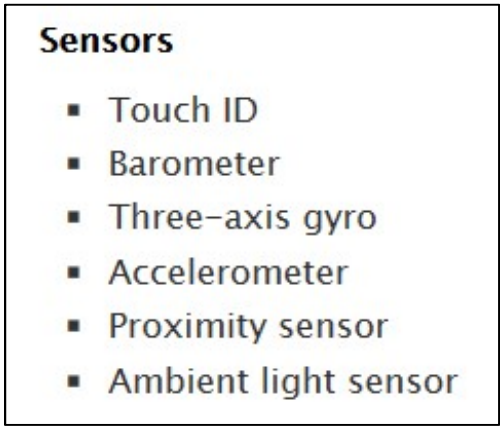
60. The cellular and Wi-Fi radios allow for communication with Apple to receive data, including a Device Account Number and cryptogram for use with Apple Pay.

61. The NFC radio allows for communication with NFC-enabled credit card payment terminals to receive data, including payment transaction details.

62. As supported by the disclosures of Apple, the touch ID sensor, cellular radio, Wi-Fi radio, and NFC radio associated with the iPhone 6 are inputs.



Technical Specifications.



Id.

Cellular and Wireless

- **Model A1549 (GSM)*/ Model A1522 (GSM)***
  - UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - GSM/EDGE (850, 900, 1800, 1900 MHz)
  - LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29)
- **Model A1549 (CDMA)*/ Model A1522 (CDMA)***
  - CDMA EV-DO Rev. A and Rev. B (800, 1700/2100, 1900, 2100 MHz)
  - UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - GSM/EDGE (850, 900, 1800, 1900 MHz)
  - LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29)

Model A1586*/ Model A1524*

- CDMA EV-DO Rev. A and Rev. B (800, 1700/2100, 1900, 2100 MHz)
- UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
- TD-SCDMA 1900 (F), 2000 (A)
- GSM/EDGE (850, 900, 1800, 1900 MHz)
- FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29)
- TD-LTE (Bands 38, 39, 40, 41)

- **All models**
  - 802.11a/b/g/n/ac Wi-Fi
  - Bluetooth 4.2 wireless technology
  - NFC

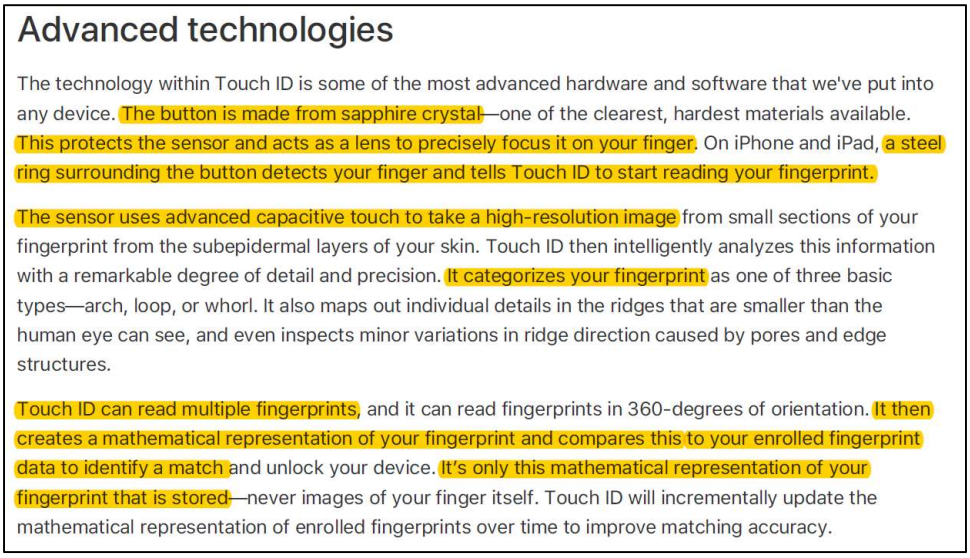
Id.

About Touch ID advanced security technology

Learn how Touch ID helps protect information on your iPhone, iPad, and MacBook Pro.

Much of our digital lives is stored on our Apple devices, and we recommend that you always use a passcode or password to help protect this important information and your privacy. Using Touch ID on your iPhone, iPad, and MacBook Pro is an easy way to use your fingerprint instead of a password for many common operations. With just a touch of your finger, the sensor quickly reads your fingerprint and automatically unlocks your device. You can use it to authorize purchases from the iTunes Store, App Store, and iBooks Store, as well as with Apple Pay. Developers can also allow you to use Touch ID to sign into their apps.

About Touch ID.



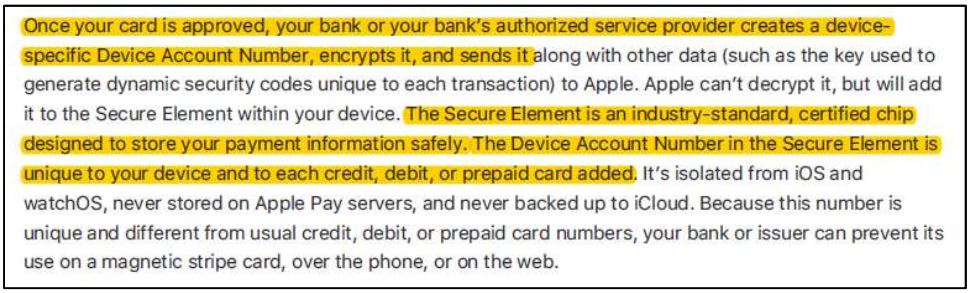
Advanced technologies

The technology within Touch ID is some of the most advanced hardware and software that we've put into any device. The button is made from sapphire crystal—one of the clearest, hardest materials available. This protects the sensor and acts as a lens to precisely focus it on your finger. On iPhone and iPad, a steel ring surrounding the button detects your finger and tells Touch ID to start reading your fingerprint.

The sensor uses advanced capacitive touch to take a high-resolution image from small sections of your fingerprint from the subepidermal layers of your skin. Touch ID then intelligently analyzes this information with a remarkable degree of detail and precision. It categorizes your fingerprint as one of three basic types—arch, loop, or whorl. It also maps out individual details in the ridges that are smaller than the human eye can see, and even inspects minor variations in ridge direction caused by pores and edge structures.

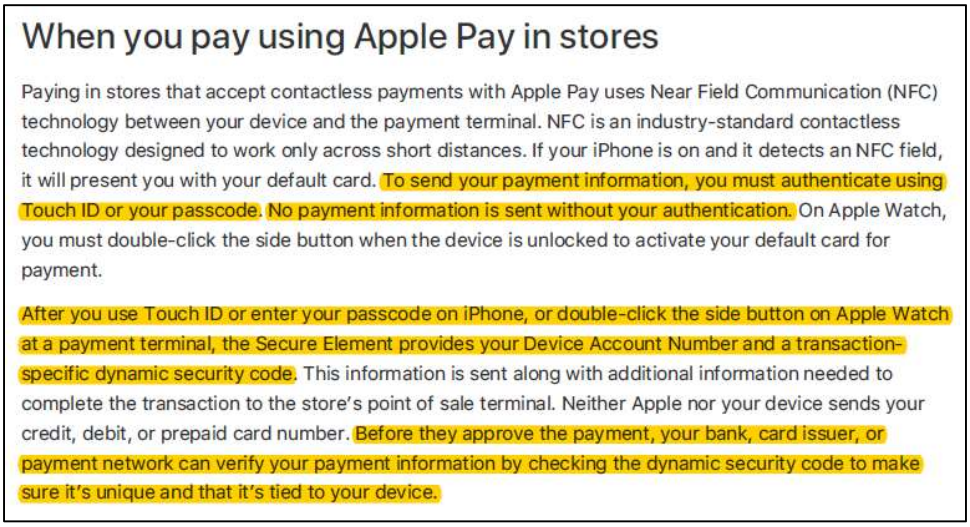
Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. It's only this mathematical representation of your fingerprint that is stored—never images of your finger itself. Touch ID will incrementally update the mathematical representation of enrolled fingerprints over time to improve matching accuracy.

Id.



Once your card is approved, your bank or your bank's authorized service provider 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 unique to each transaction) to Apple. Apple can't decrypt it, but will add it to the Secure Element within your device. The Secure Element is an industry-standard, certified chip designed to store your payment information safely. The Device Account Number in the Secure Element is unique to your device and to each credit, debit, or prepaid card added. It's isolated from iOS and watchOS, never stored on Apple Pay servers, and never backed up to iCloud. Because this number is unique and different from usual credit, debit, or prepaid card numbers, your bank or issuer can prevent its use on a magnetic stripe card, over the phone, or on the web.

Apple Pay Security.



When you pay using Apple Pay in stores

Paying in stores that accept contactless payments with Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard contactless technology designed to work only across short distances. If your iPhone is on and it detects an NFC field, it will present you with your default card. To send your payment information, you must authenticate using Touch ID or your passcode. No payment information is sent without your authentication. On Apple Watch, you must double-click the side button when the device is unlocked to activate your default card for payment.

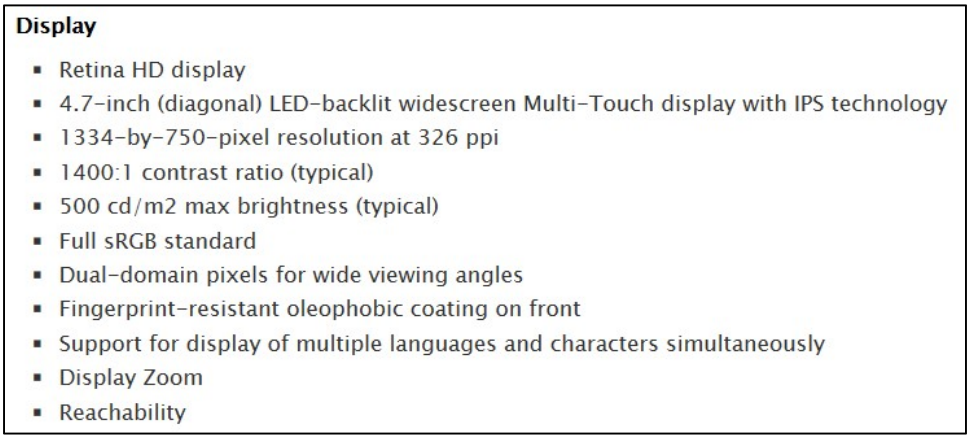
After you use Touch ID or enter your passcode on iPhone, or double-click the side button on Apple Watch at a payment terminal, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code. This information is sent along with additional information needed to complete the transaction to the store's point of sale terminal. Neither Apple nor your device sends your credit, debit, or prepaid card number. Before they approve the payment, your bank, card issuer, or payment network can verify your payment information by checking the dynamic security code to make sure it's unique and that it's tied to your device.

Id.

1(d) one or more outputs; –

63. The iPhone 6 includes several outputs, including a HD display, and multiple wireless radios (cellular, Wi-Fi, and NFC).

64. As supported by the disclosures of Apple, the HD Display, cellular radio, Wi-Fi radio, and NFC radio associated with the iPhone 6 are outputs.



Display

- Retina HD display
- 4.7-inch (diagonal) LED-backlit widescreen Multi-Touch display with IPS technology
- 1334-by-750-pixel resolution at 326 ppi
- 1400:1 contrast ratio (typical)
- 500 cd/m2 max brightness (typical)
- Full sRGB standard
- Dual-domain pixels for wide viewing angles
- Fingerprint-resistant oleophobic coating on front
- Support for display of multiple languages and characters simultaneously
- Display Zoom
- Reachability

Technical Specifications.

Cellular and Wireless

- **Model A1549 (GSM)*/ Model A1522 (GSM)***
  - UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - GSM/EDGE (850, 900, 1800, 1900 MHz)
  - LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29)
- **Model A1549 (CDMA)*/ Model A1522 (CDMA)***
  - CDMA EV-DO Rev. A and Rev. B (800, 1700/2100, 1900, 2100 MHz)
  - UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - GSM/EDGE (850, 900, 1800, 1900 MHz)
  - LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29)

Model A1586*/ Model A1524*

- CDMA EV-DO Rev. A and Rev. B (800, 1700/2100, 1900, 2100 MHz)
- UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
- TD-SCDMA 1900 (F), 2000 (A)
- GSM/EDGE (850, 900, 1800, 1900 MHz)
- FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29)
- TD-LTE (Bands 38, 39, 40, 41)

- **All models**
  - 802.11a/b/g/n/ac Wi-Fi
  - Bluetooth 4.2 wireless technology
  - NFC

Id.

Transaction-specific dynamic security code

All payment transactions originating from the payment applets include a transaction-specific dynamic security code along with a Device Account Number. This one-time code is computed using a counter that is incremented for each new transaction, and a key that's provisioned in the payment applet during personalization and is known by the payment network and/or the card issuer. Depending on the payment scheme, other data may also be used in the calculation of these codes, including the following:

- A random number generated by the payment applet
- Another random number generated by the terminal—in the case of an NFC transaction or
- Another random number generated by the server—in the case of transactions within apps

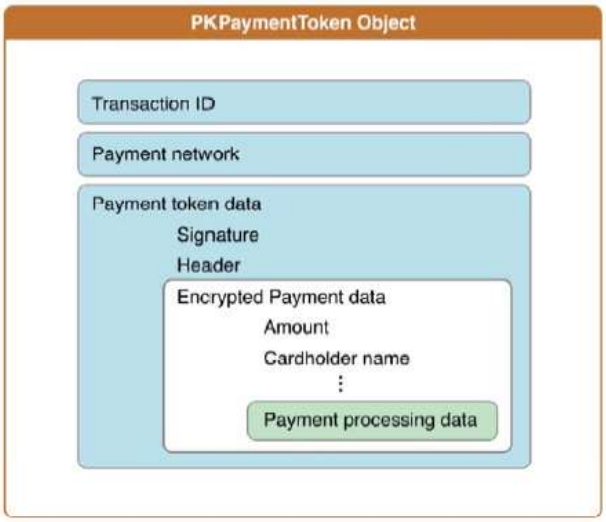
These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction. The length of these security codes may vary based on the type of transaction being done.

iOS Security at p. 38.

Payment Token Format Reference

A payment token is created by the Secure Element based on a payment request. The payment token has a nested structure, as shown in Figure 1-1.

Figure 1-1 Structure of a payment token



The Secure Element encrypts the token's payment data using either elliptic curve cryptography (ECC) or RSA encryption. The encryption algorithm is selected by the Secure Element based on the payment request. Most regions use ECC encryption. RSA is used only in regions where ECC encryption is unavailable due to regulatory concerns.

"Payment Token Format Reference" ("**Payment Token Format Reference**"), *available at* https://developer.apple.com/library/content/documentation/PassKit/Reference/PaymentTokenJSON/PaymentTokenJSON.html (last accessed April 9, 2018).

> *1(e) a verifying means for determining user authorization or non-authorization, said verifying means receiving data from at least one of said one or more inputs, which data is derived from biometric or other distinctive characteristics of the user, said verifying means generating an identification profile for each user, wherein said identification profile is determined from said data, and; –*

65. The iPhone 6 includes a Touch ID sensor, and a Secure Enclave.

66. When a user makes a purchase with Apple Pay using the iPhone 6, the user can use Touch ID to authorize the purchase.

67. In doing so, the Touch ID images the user's fingerprint.

68. The Secure Enclave chip then uses this fingerprint data and compares it to enrolled fingerprint data to identify a match.

69. If there is a match between the imaged fingerprint and the enrolled fingerprint data, the Secure Enclave authorizes the Apple Pay transaction.

70. If there is not a match, the Apple Pay transaction is not authorized.

71. When a user registers a credit card, the card issuer generates a Device Account Number, and sends it, along with other data, including a key used to generate dynamic security codes unique to each transaction to the iPhone registering the credit card.

72. The Device Account Number is stored in the Secured Element and represents a distinctive characteristic of the user.

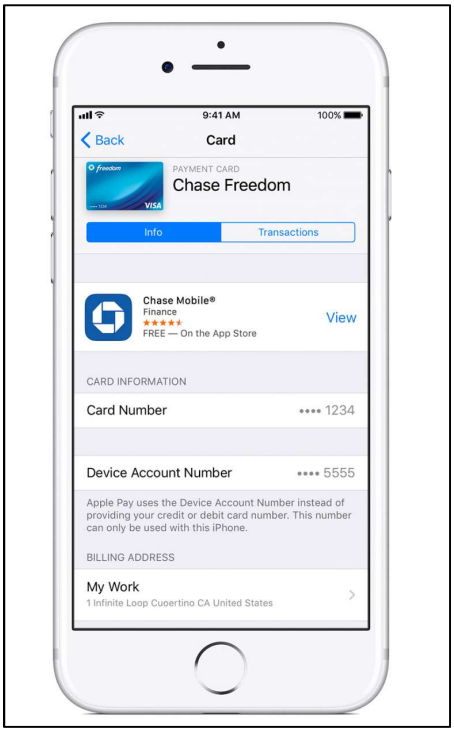
73. The Secure Enclave and Secure element generate an identification profile for the user, which includes the Device Account Number, in order for the code generator to generate an access code.

74. As supported by the disclosures of Apple, the Touch ID in combination with the Secure Enclave and Secure Element performs the function of determining user authorization or non-authorization, receiving data from at least one of said one or more inputs, which data is derived from biometric or other distinctive characteristics of the user, and generating an identification profile for each user, wherein said identification profile is determined from said data, and the Touch ID, Secure Enclave, and Secure Element are the same or equivalent structure to the disclosed verifying means, including

the fingerprint scan, comparator circuitry, data generating circuitry, and associated technology to perform biometric scanning, comparing of biometric information, and generating an identification profile.

About Apple Pay

Apple Pay offers an easy, secure, and private way to pay on iPhone, iPad, Apple Watch, and Mac. And now you can send and receive money with friends and family right in Messages.[1]



How secure is Apple Pay?

Apple Pay is safer than using a plastic credit, debit, or prepaid card. Every transaction on your iPhone, iPad, or Mac requires you to authenticate with Face ID, Touch ID, or your passcode. Your Apple Watch is protected by the passcode that only you know, and your passcode is required every time you put on your Apple Watch or when you pay using Apple Pay. Your card number and identity aren't shared with the merchant, and your actual card numbers aren't stored on your device or on Apple servers.

"About Apple Pay" ("**About Apple Pay**"), *available at* https://support.apple.com/en-us/HT201469 (last accessed April 9, 2018).

> The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user. Communication between the processor and the Touch ID sensor takes place over a serial peripheral interface bus. The processor forwards the data to the Secure Enclave but can't read it. It's encrypted and authenticated with a session key that is negotiated using the device's shared key that is provisioned for the Touch ID sensor and the Secure Enclave. The session key exchange uses AES key wrapping with both sides providing a random key that establishes the session key and uses AES-CCM transport encryption.

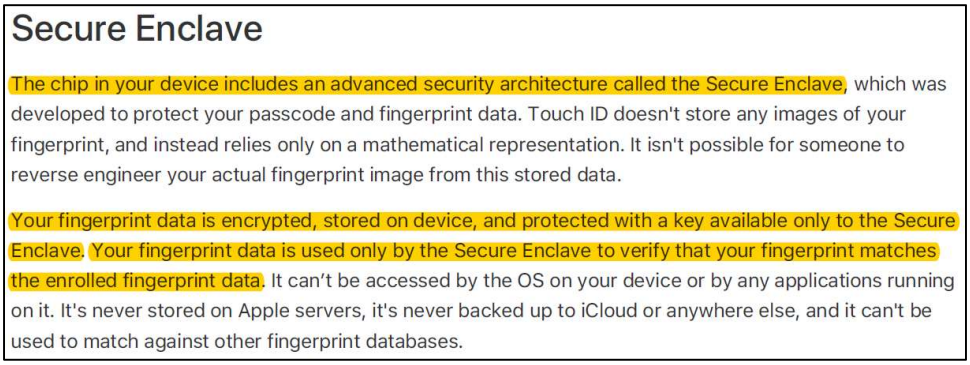
iOS Security at p. 7.

> ## About Touch ID advanced security technology
>
> Learn how Touch ID helps protect information on your iPhone, iPad, and MacBook Pro.
>
> Much of our digital lives is stored on our Apple devices, and we recommend that you always use a passcode or password to help protect this important information and your privacy. Using Touch ID on your iPhone, iPad, and MacBook Pro is an easy way to use your fingerprint instead of a password for many common operations. With just a touch of your finger, the sensor quickly reads your fingerprint and automatically unlocks your device. You can use it to authorize purchases from the iTunes Store, App Store, and iBooks Store, as well as with Apple Pay. Developers can also allow you to use Touch ID to sign into their apps.

About Touch ID.

> ## Advanced technologies
>
> The technology within Touch ID is some of the most advanced hardware and software that we've put into any device. The button is made from sapphire crystal—one of the clearest, hardest materials available. This protects the sensor and acts as a lens to precisely focus it on your finger. On iPhone and iPad, a steel ring surrounding the button detects your finger and tells Touch ID to start reading your fingerprint.
>
> The sensor uses advanced capacitive touch to take a high-resolution image from small sections of your fingerprint from the subepidermal layers of your skin. Touch ID then intelligently analyzes this information with a remarkable degree of detail and precision. It categorizes your fingerprint as one of three basic types—arch, loop, or whorl. It also maps out individual details in the ridges that are smaller than the human eye can see, and even inspects minor variations in ridge direction caused by pores and edge structures.
>
> Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. It's only this mathematical representation of your fingerprint that is stored—never images of your finger itself. Touch ID will incrementally update the mathematical representation of enrolled fingerprints over time to improve matching accuracy.

Id.

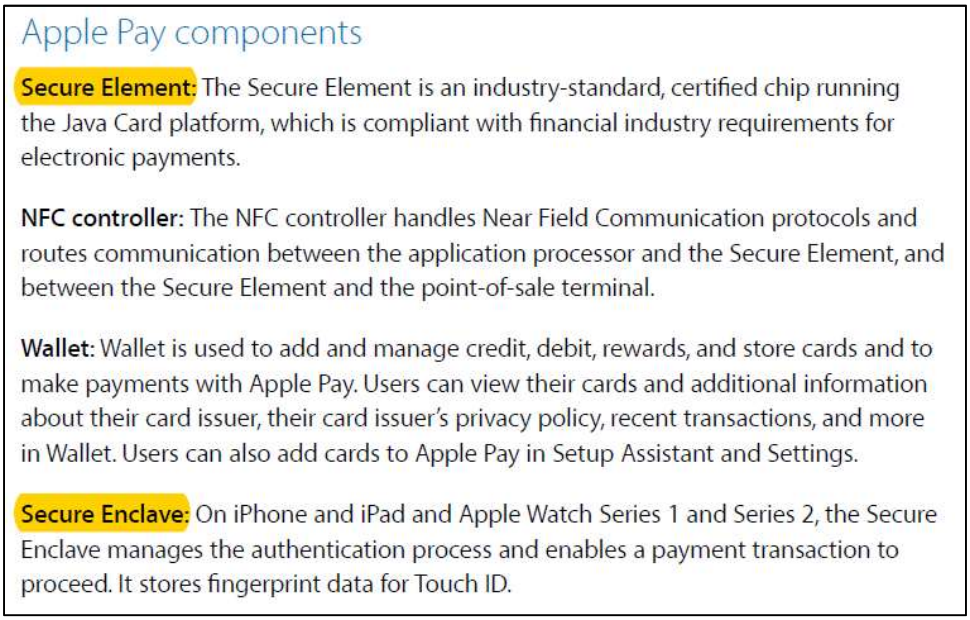


Secure Enclave

The chip in your device includes an advanced security architecture called the Secure Enclave, which was developed to protect your passcode and fingerprint data. Touch ID doesn't store any images of your fingerprint, and instead relies only on a mathematical representation. It isn't possible for someone to reverse engineer your actual fingerprint image from this stored data.

Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave. Your fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data. It can't be accessed by the OS on your device or by any applications running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases.

Id.



Apple Pay components

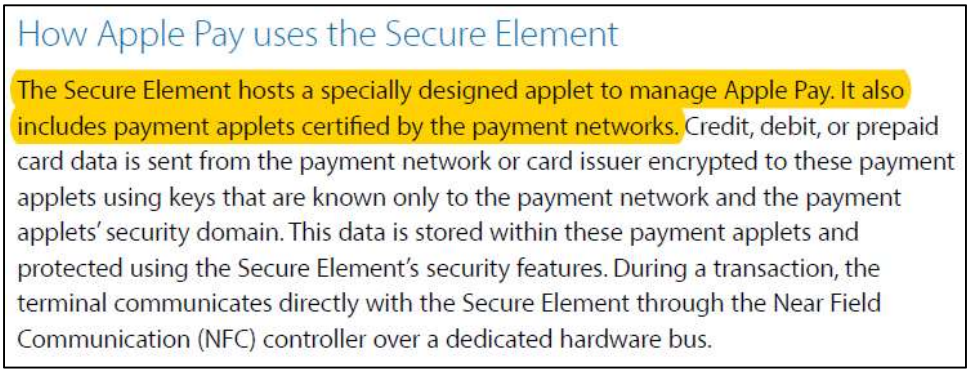
Secure Element: The Secure Element is an industry-standard, certified chip running the Java Card platform, which is compliant with financial industry requirements for electronic payments.

NFC controller: The NFC controller handles Near Field Communication protocols and routes communication between the application processor and the Secure Element, and between the Secure Element and the point-of-sale terminal.

Wallet: Wallet is used to add and manage credit, debit, rewards, and store cards and to make payments with Apple Pay. Users can view their cards and additional information about their card issuer, their card issuer's privacy policy, recent transactions, and more in Wallet. Users can also add cards to Apple Pay in Setup Assistant and Settings.

Secure Enclave: On iPhone and iPad and Apple Watch Series 1 and Series 2, the Secure Enclave manages the authentication process and enables a payment transaction to proceed. It stores fingerprint data for Touch ID.

iOS Security at p. 34.



How Apple Pay uses the Secure Element

The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes payment applets certified by the payment networks. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these payment applets using keys that are known only to the payment network and the payment applets' security domain. This data is stored within these payment applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the Near Field Communication (NFC) controller over a dedicated hardware bus.

Id.

> Once your card is approved, your bank or your bank's authorized service provider 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 unique to each transaction) to Apple. Apple can't decrypt it, but will add it to the Secure Element within your device. The Secure Element is an industry-standard, certified chip designed to store your payment information safely. The Device Account Number in the Secure Element is unique to your device and to each credit, debit, or prepaid card added. It's isolated from iOS and watchOS, never stored on Apple Pay servers, and never backed up to iCloud. Because this number is unique and different from usual credit, debit, or prepaid card numbers, your bank or issuer can prevent its use on a magnetic stripe card, over the phone, or on the web.

Apple Pay Security.

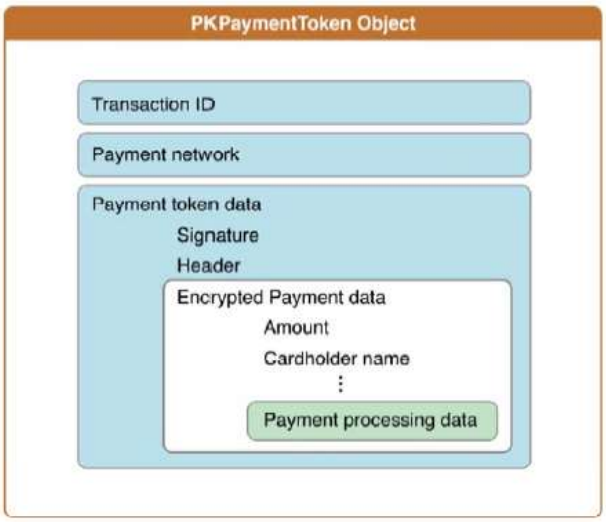
> ## When you pay using Apple Pay in stores
>
> Paying in stores that accept contactless payments with Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard contactless technology designed to work only across short distances. If your iPhone is on and it detects an NFC field, it will present you with your default card. To send your payment information, you must authenticate using Touch ID or your passcode. No payment information is sent without your authentication. On Apple Watch, you must double-click the side button when the device is unlocked to activate your default card for payment.
>
> After you use Touch ID or enter your passcode on iPhone, or double-click the side button on Apple Watch at a payment terminal, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code. This information is sent along with additional information needed to complete the transaction to the store's point of sale terminal. Neither Apple nor your device sends your credit, debit, or prepaid card number. Before they approve the payment, your bank, card issuer, or payment network can verify your payment information by checking the dynamic security code to make sure it's unique and that it's tied to your device.

Id.

Payment Token Format Reference

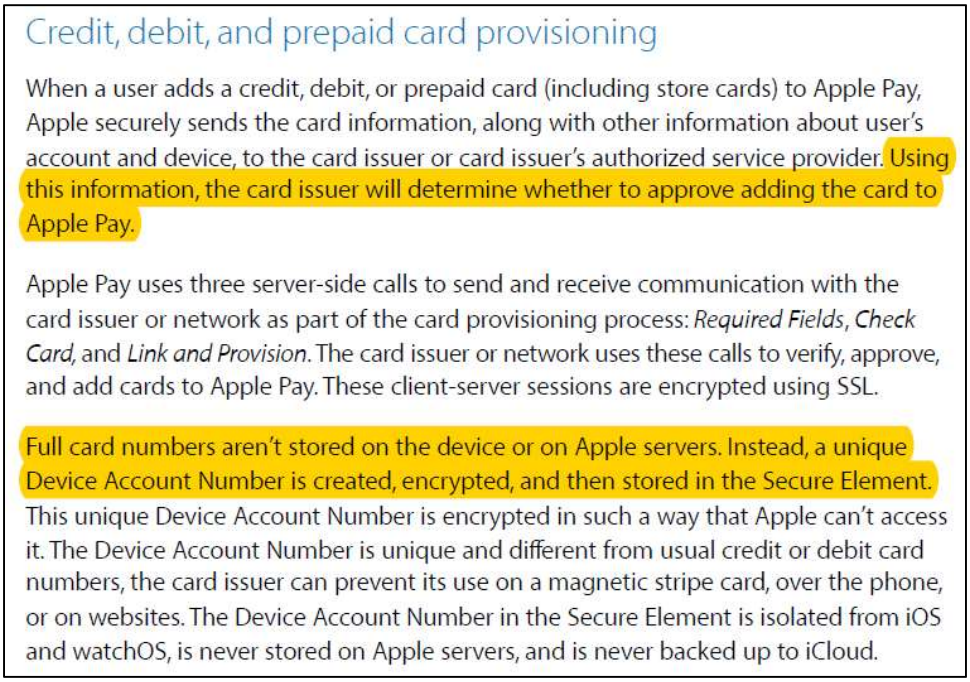
A payment token is created by the Secure Element based on a payment request. The payment token has a nested structure, as shown in Figure 1–1.

Figure 1–1 Structure of a payment token



The Secure Element encrypts the token's payment data using either elliptic curve cryptography (ECC) or RSA encryption. The encryption algorithm is selected by the Secure Element based on the payment request. Most regions use ECC encryption. RSA is used only in regions where ECC encryption is unavailable due to regulatory concerns.

Payment Token Format Reference.



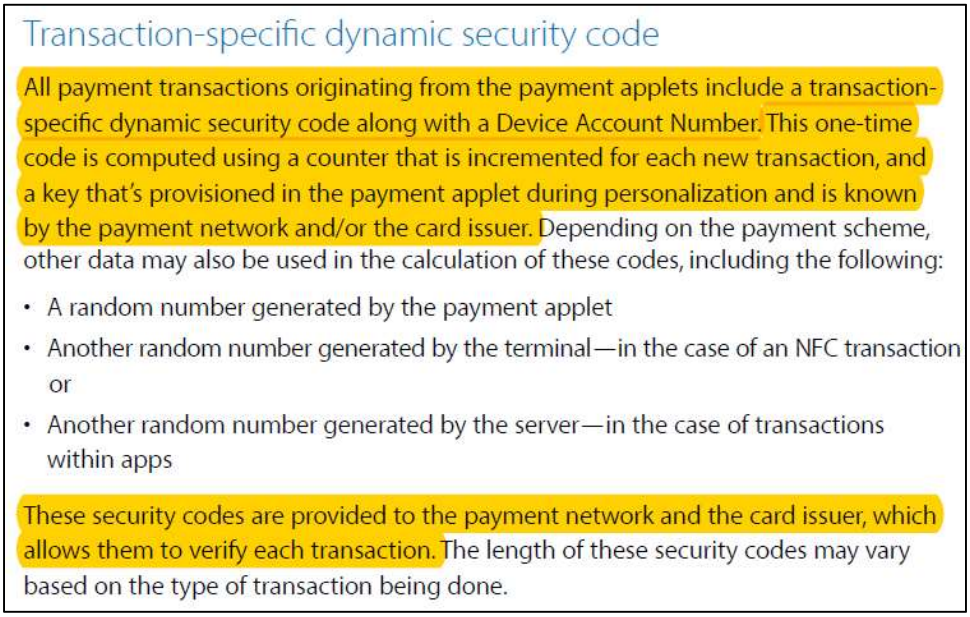
Credit, debit, and prepaid card provisioning

When a user adds a credit, debit, or prepaid card (including store cards) to Apple Pay, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer will determine whether to approve adding the card to Apple Pay.

Apple Pay uses three server-side calls to send and receive communication with the card issuer or network as part of the card provisioning process: *Required Fields*, *Check Card*, and *Link and Provision*. The card issuer or network uses these calls to verify, approve, and add cards to Apple Pay. These client-server sessions are encrypted using SSL.

Full card numbers aren't stored on the device or on Apple servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from 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 and watchOS, is never stored on Apple servers, and is never backed up to iCloud.

iOS Security at p. 35.



Transaction-specific dynamic security code

All payment transactions originating from the payment applets include a transaction-specific dynamic security code along with a Device Account Number. This one-time code is computed using a counter that is incremented for each new transaction, and a key that's provisioned in the payment applet during personalization and is known by the payment network and/or the card issuer. Depending on the payment scheme, other data may also be used in the calculation of these codes, including the following:

- A random number generated by the payment applet
- Another random number generated by the terminal—in the case of an NFC transaction or
- Another random number generated by the server—in the case of transactions within apps

These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction. The length of these security codes may vary based on the type of transaction being done.

Id. at p. 38.

> When the user authorizes a transaction, the Secure Enclave sends signed data about the type of authentication and details about the type of transaction (contactless or within apps) to the Secure Element, tied to an Authorization Random (AR) value. The AR is generated in the Secure Enclave when a user first provisions a credit card and is persisted while Apple Pay is enabled, protected by the Secure Enclave's encryption and anti-rollback mechanism. It is securely delivered to the Secure Element via the pairing key. On receipt of a new AR value, the Secure Element marks any previously added cards as deleted.

Id. at p. 37.

> *1(f) a code generator employing at least one code generating algorithm for generating one or more access codes based upon said identification profile wherein at least one of the said one or more access codes is an identification specific digital signature. –*

75. When a transaction is authorized by the owner of an iPhone 6, the Secure Enclave sends signed data about the type of authentication and details about the type of transaction to the Secure Element, tied to an Authorization Random ("AR") value.

76. The AR is generated in the Secure Enclave when the user first provisions a credit card and is persisted while Apply Pay is enabled.

77. All payment transactions originated from the iPhone 6 using Apple Pay include a transaction specific dynamic security code with a Device Account Number ("DAN").

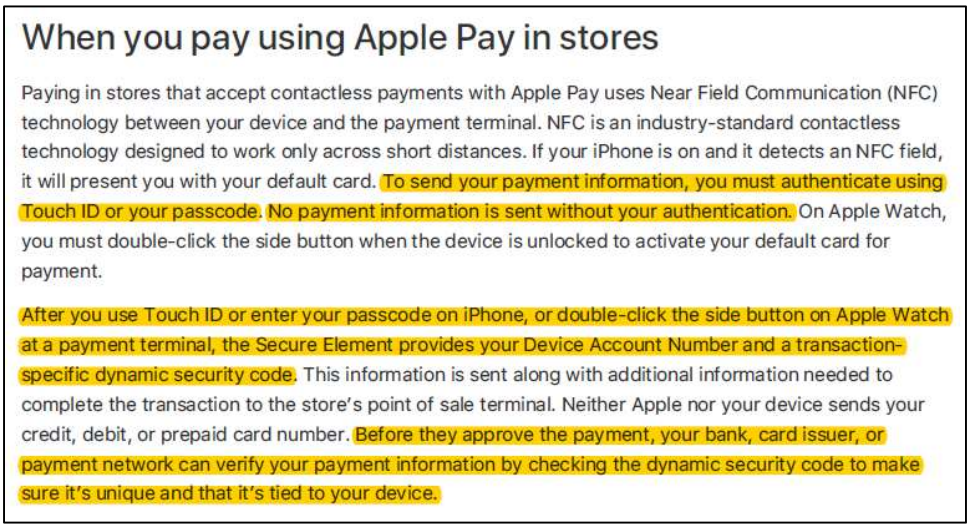
78. This dynamic security code is a one-time code and is computed using a counter that is incremented for each new transaction and a key that is provisioned in the payment applet during personalization and is known by the payment network and/or card issuer.

79. The AR generated by the Secure Enclave is used in the generation of these dynamic security codes.

80. A random number generated by the NFC POS terminal is also used in the generation of these dynamic security codes.

81. These dynamic security codes are provided to the payment network and the card issuer, which allows the payment network and card issuer to verify each transaction.

82. As supported by the disclosures of Apple, Secure Element is a code generator that employs a code generating algorithm for generating an access code based upon the user's identification profile, which includes the provisioned key. The dynamic security code is an identification specific digital signature.



When you pay using Apple Pay in stores

Paying in stores that accept contactless payments with Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard contactless technology designed to work only across short distances. If your iPhone is on and it detects an NFC field, it will present you with your default card. To send your payment information, you must authenticate using Touch ID or your passcode. No payment information is sent without your authentication. On Apple Watch, you must double-click the side button when the device is unlocked to activate your default card for payment.

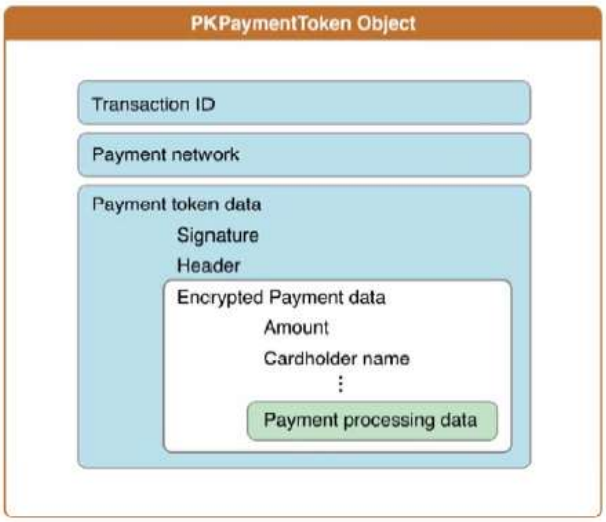
After you use Touch ID or enter your passcode on iPhone, or double-click the side button on Apple Watch at a payment terminal, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code. This information is sent along with additional information needed to complete the transaction to the store's point of sale terminal. Neither Apple nor your device sends your credit, debit, or prepaid card number. Before they approve the payment, your bank, card issuer, or payment network can verify your payment information by checking the dynamic security code to make sure it's unique and that it's tied to your device.

Apple Pay Security.

Payment Token Format Reference

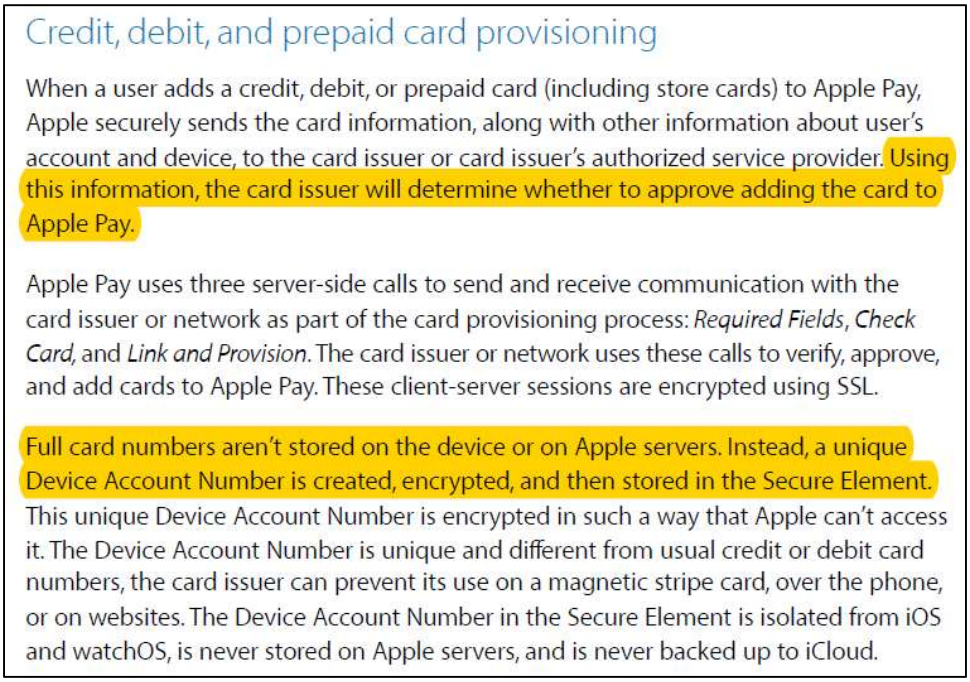
A payment token is created by the Secure Element based on a payment request. The payment token has a nested structure, as shown in Figure 1-1.

Figure 1-1 Structure of a payment token



The Secure Element encrypts the token's payment data using either elliptic curve cryptography (ECC) or RSA encryption. The encryption algorithm is selected by the Secure Element based on the payment request. Most regions use ECC encryption. RSA is used only in regions where ECC encryption is unavailable due to regulatory concerns.

Payment Token Format Reference.



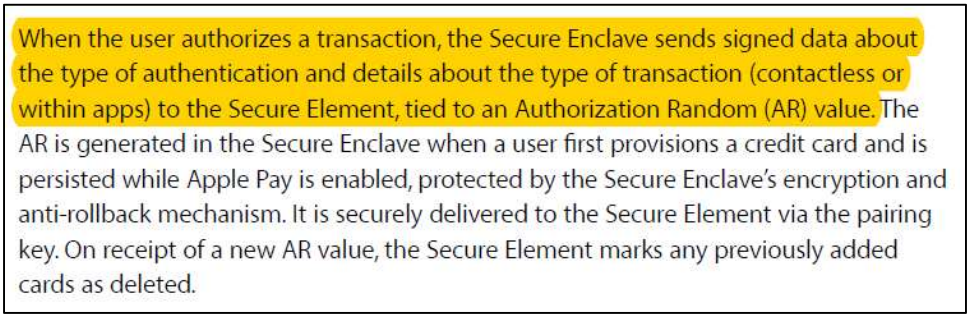
Credit, debit, and prepaid card provisioning

When a user adds a credit, debit, or prepaid card (including store cards) to Apple Pay, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer will determine whether to approve adding the card to Apple Pay.

Apple Pay uses three server-side calls to send and receive communication with the card issuer or network as part of the card provisioning process: *Required Fields*, *Check Card*, and *Link and Provision*. The card issuer or network uses these calls to verify, approve, and add cards to Apple Pay. These client-server sessions are encrypted using SSL.

Full card numbers aren't stored on the device or on Apple servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from 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 and watchOS, is never stored on Apple servers, and is never backed up to iCloud.

iOS Security at p. 35.



When the user authorizes a transaction, the Secure Enclave sends signed data about the type of authentication and details about the type of transaction (contactless or within apps) to the Secure Element, tied to an Authorization Random (AR) value. The AR is generated in the Secure Enclave when a user first provisions a credit card and is persisted while Apple Pay is enabled, protected by the Secure Enclave's encryption and anti-rollback mechanism. It is securely delivered to the Secure Element via the pairing key. On receipt of a new AR value, the Secure Element marks any previously added cards as deleted.

Id. at p. 37.

Transaction-specific dynamic security code

All payment transactions originating from the payment applets include a transaction-specific dynamic security code along with a Device Account Number. This one-time code is computed using a counter that is incremented for each new transaction, and a key that's provisioned in the payment applet during personalization and is known by the payment network and/or the card issuer. Depending on the payment scheme, other data may also be used in the calculation of these codes, including the following:

- A random number generated by the payment applet
- Another random number generated by the terminal—in the case of an NFC transaction or
- Another random number generated by the server—in the case of transactions within apps

These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction. The length of these security codes may vary based on the type of transaction being done.

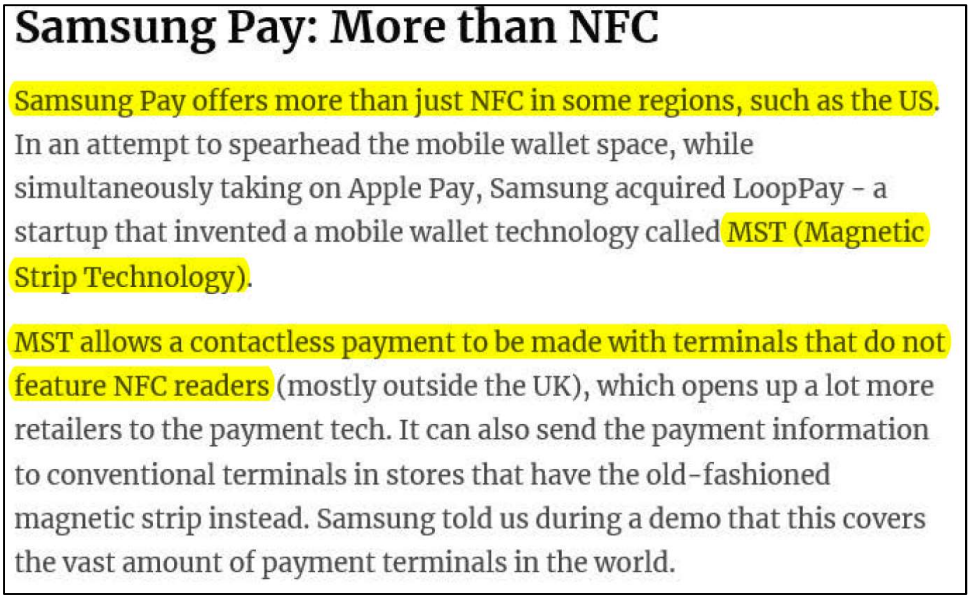
Id. at p. 38.

83. The other Accused Infringing Devices operate in substantially the same manner. See, e.g.

What is Samsung Pay, how does it work, and which banks support it?

Elyse Betters | 4 October 2017

POCKET-LINT

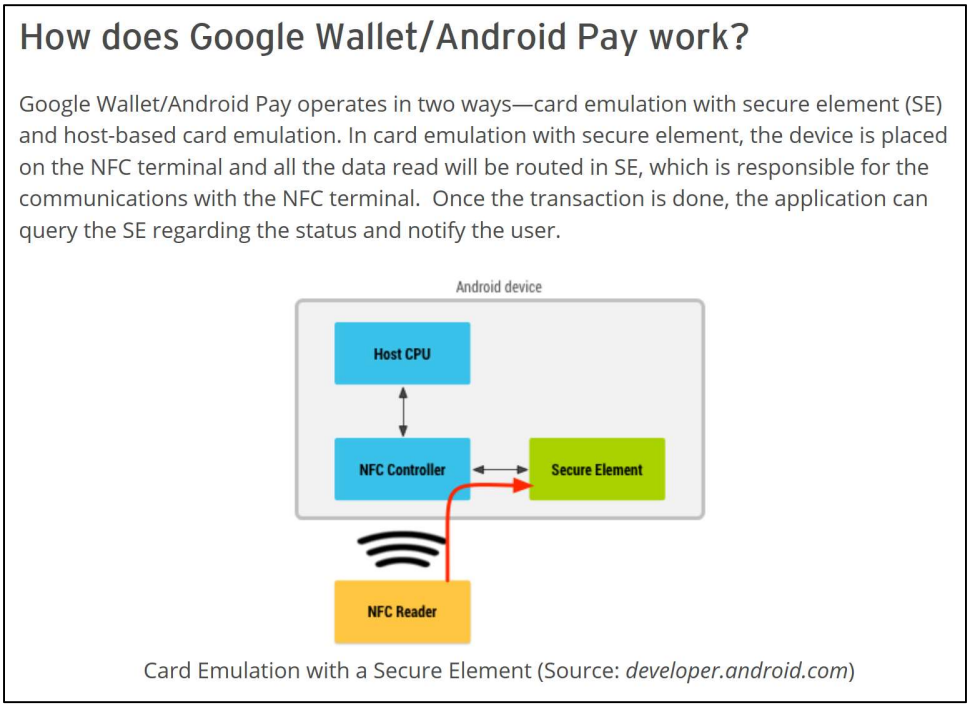


Samsung Pay: More than NFC

Samsung Pay offers more than just NFC in some regions, such as the US. In an attempt to spearhead the mobile wallet space, while simultaneously taking on Apple Pay, Samsung acquired LoopPay – a startup that invented a mobile wallet technology called MST (Magnetic Strip Technology).

MST allows a contactless payment to be made with terminals that do not feature NFC readers (mostly outside the UK), which opens up a lot more retailers to the payment tech. It can also send the payment information to conventional terminals in stores that have the old-fashioned magnetic strip instead. Samsung told us during a demo that this covers the vast amount of payment terminals in the world.

"What is Samsung Pay, how does it work, and which banks support it?" ("**What is Samsung Pay**") ("Just like Apple Pay, Samsung Pay uses tokenisation. Card payments are made secure by creating a number or token that replaces your card details. This token is stored within a secure element chip on your device, and when a payment is initiated, the token is passed to the retailer or merchant. The retailer therefore never has direct access to your card details."), *available at* https://www.pocket-lint.com/apps/news/samsung/132981-what-is-samsung-pay-how-does-it-work-and-which-banks-support-it (last accessed April 9, 2018).



"Mobile Payment Systems: How Android Pay Works" ("**How Android Pay Works**"), *available at* https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/mobile-payment-systems-android-pay (last accessed April 9, 2018).

DAMAGES

84. Vindolor has been damaged by Defendant's infringement of the '391 Patent.

PRAYER FOR RELIEF

Vindolor respectfully requests the Court enter judgment against Defendant:

1. declaring that Defendant has infringed the '391 Patent;
2. awarding Vindolor its damages suffered as a result of Defendant's infringement of the '391 Patent;
3. awarding Vindolor its costs, attorneys' fees, expenses, and interest; and
4. granting Vindolor such further relief as the Court finds appropriate.

JURY DEMAND

Vindolor demands trial by jury, Under Fed. R. Civ. P. 38.

Dated: May 30, 2019

Respectfully Submitted

/s/ Raymond W. Mort, III

Raymond W. Mort, III
Texas State Bar No. 00791308
raymort@austinlaw.com

THE MORT LAW FIRM, PLLC
100 Congress Ave, Suite 2000
Austin, Texas 78701
Tel/Fax: (512) 865-7950

ATTORNEYS FOR PLAINTIFF