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

VINDOLOR, LLC, Plaintiff v. BUC-EE'S, LTD, Defendant	Civil Action No.: 6:18-cv-00104 JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Vindolor, LLC ("Vindolor") hereby asserts the following claims for patent infringement against Defendant Buc-ee's, Ltd ("Defendant" or "Buc-ee's"), and alleges as follows:

THE PARTIES

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

2.   Defendant is a limited partnership organized and existing under the laws of Texas with its principal place of business at 327 FM 2004, Lake Jackson, Texas 77566.

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 4155 N General Bruce Dr, Temple, Texas 76501.

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 used 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.   The '391 Patent describes problems and shortcomings in the then-existing field of electronic personal identification. *See, e.g.,* '391 Patent at col. 1, l. 16 – col. 3, l. 33.

11.   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.

12.   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.* at col. 1, ll. 8-13.

13.   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.* at col. 1, l. 16 – col. 12, l. 39.

14.   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.* at col. 1, l. 16 – col. 12, l. 39.

15.   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.*

16.   As demonstrated by its frequent citation (over 250) by the United Stated Patent Office in other later-issued patents and reexaminations, the '391 Patent represents a fundamental technical improvement in the area of electronic identification systems. 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 Full-Text and Image Database – ref/6213391" ("**USPTO Patent Search**"),

available at http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&

u=%2Fnetahtml%2Fsearch-adv.htm&r=0&f=S&l=50&d=PALL&Query=ref/6213391.   (last

accessed April 9, 2018).

17.   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.

18.   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.

19.   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.

20.   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.

21.   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.

22.   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.

23.   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.

24.   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 does not preempt the field of its

invention or preclude the user of other 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.

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

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

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

28.   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.

29.   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.

30.   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).

31.   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 code generator 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 access code.

32.	There were 1,174 days from the time the '391 Patent was filed until the USPTO issued the notice of allowance for the '391 Patent on November 27, 2000.

33.	There were 1,308 days from the time the '391 Patent was filed until the USPTO issued the '391 Patent on April 10, 2001.

34.	Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 235 (Registers) and subclass 376 (Operational Analysis).

35.	Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 235 (Registers) and subclass 379 (Banking Systems).

36.	Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 235 (Registers) and subclass 380 (Credit or Identification Card Systems).

37.	Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 235 (Registers) and subclass 382 (Permitting Access).

38.	Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 235 (Registers) and subclass 382.5 (Changeable Authorization).

39.	Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 235 (Registers) and subclass 451 (Capacitive).

40.	Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 235 (Registers) and subclass 470 (With Scanning Of Record).

41.   Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 235 (Registers) and subclass 492 (Conductive).

42.   Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 902 (Electronic Funds Transfer) and subclass 2 (Protects Transmitted Data (*e.g.,* Encryption Or Decryption)).

43.   Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 902 (Electronic Funds Transfer) and subclass 3 (Evaluates Biometrics).

44.   Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 902 (Electronic Funds Transfer) and subclass 4 (Means To Read Data Stored On Identifier).

45.   Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 902 (Electronic Funds Transfer) and subclass 5 (And To Verify Identity Of User).

46.   Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 902 (Electronic Funds Transfer) and subclass 26 (Including Semiconductor Chip (*e.g.,* Smart Card)).

47.   Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 705 (Data Processing, Financial, Business Practice, Management, or Cost/Price Determination) and subclass 42 (Remote Banking (*e.g.,* Home Banking)).

48.   Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 705 (Data Processing, Financial, Business Practice, Management, or Cost/Price Determination) and subclass 43 (Including Automatic Teller Machine (i.e. ATM)).

49.   Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 705 (Data Processing, Financial, Business Practice, Management, or Cost/Price Determination) and subclass 44 (Requiring Authorization Or Authentication)).

50.   Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 713 (Electrical Computers And Digital Processing Systems: Support) and subclass 182 (System Access Control Based On User Identification By Cryptography).

51.   Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 713 (Electrical Computers And Digital Processing Systems: Support) and subclass 185 (Using Record Or Token).

52.   Prior to granting the '391 Patent, the USPTO Examiners conducted a search for prior patents and publications in class 713 (Electrical Computers And Digital Processing Systems: Support) and subclass 186 (Biometric Acquisition).

53.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 4,148,012 to Baump et al.

54.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 4,218,738 to Matyas et al.

55.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 4,264,782 to Konheim.

56.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 4,315,101 to Atella.

57.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 4,438,824 to Mueller-Schloer.

58.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 4,630,201 to White.

59.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 4,804,825 to Bitoh.

60.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 4,825,050 to Griffith et al.

61.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 4,827,518 to Feustal et al.

62.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 4,961,229 to Takahashi.

63.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 4,993,068 to Piosenka et al.

64.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 4,998,279 to Weiss.

65.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 5,151,684 to Johnsen.

66.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 5,276,444 to McNair.

67.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 5,313,556 to Parra.

68.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 5,386,103 to DeBan et al.

69.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 5,513,272 to Bogosian, Jr.

70.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 5,552,777 to Gokcebat et al.

71.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 5,581,630 to Bonneau, Jr.

72.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 5,594,493 to Nemirofsky.

73.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 5,623,552 to Lane.

74.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 5,793,027 to Baik.

75.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 5,815,658 to Kuriyama.

76.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 5,825,871 to Mark.

77.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 5,825,882 to Kowalski et al.

78.   Prior to granting the '391 Patent, the USPTO considered the disclosure of U.S. Patent No. 5,870,724 to Lowlor et al.

79.   Prior to granting the '391 Patent, the USPTO considered the disclosure of German Patent Document No. 3731773 (DE).

80.   Prior to granting the '391 Patent, the USPTO considered the disclosure of Japanese Patent Document No. 4-135293 (JP).

81.   Prior to granting the '391 Patent, the USPTO considered the disclosure of "High-Tech Building Security", Siuru, Bill, *Popular Electronics*, Dec. 1996, pp. 39–42, 46.

82.   Prior to granting the '391 Patent, the USPTO considered the disclosure of "Who Goes There?", Wyner, Peter, *Byte*, vol. 22, No. 6, Jun. 1997, pp. 70–80.

83.   Prior to granting the '391 Patent, the USPTO considered the disclosure of "No Place to Hide", Marsh, Ann, *Porhes*, Sep. 22, 1997, pp. 226–234.

84.   Prior to granting the '391 Patent, the USPTO considered the disclosure of "The Generation Gap", Vesley, Rebecca, *Wired*, Oct. 1997, pp. 53–56, 207.

85.   Prior to granting the '391 Patent, the USPTO considered the disclosure of Look. Forward, *Internet User Magazine*, Summer 1997, pp. 11, 12, 14, 21.

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

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

87.   Defendant has operated multiple retail establishments where it offered goods for sale to customers.

88.   Within its retail establishments, Defendant has operated near field communications ("NFC")-enabled point of sale terminals ("POS terminals") and has accepted payments using at least one of Microsoft Wallet, Wells Fargo Wallet, Masterpass, Samsung Pay, Android Pay, Google Pay, Google Wallet, Apple Pay, and PayPal mobile. See e.g., "Check out all the places where you can check out" ("**Check Out**"), *available at* https://www.apple.com/apple-pay/where-to-use/ (last accessed April 9, 2018).

89.   Prior to September 10, 2017, Defendant tested or used portable identification systems in the United States. Such devices include:

(a)   Window based phones and devices (*e.g.* the Microsoft Lumina 950, the Microsoft Lumina 640, and the Nokia Lumina 830) installed with the Microsoft Wallet App;

(b)   Android based phones and mobile devices (*e.g.* the Samsung Galaxy S6, the LG G4, the HTC One M9, the Motorola Droid Razr M, the Alcatel IDOL 4S, the ASUS PadFone 2, the Huawei Hero 9, the OnePlus 5, and the Pantech Discover p9090) installed with the PayPal Mobile App, the Wells Fargo Wallet App, the Masterpass App, the Google Wallet App, the Android Pay App, the Google Pay App, or the Samsung Pay App; and

(c)   Apple based phones and mobile devices (*e.g.* the Apple iPhone 6, and iPhone 6+) installed with the PayPal Mobile App, the Apple Wallet, or the Apple Pay App.

(collectively "Accused Infringing Devices").

90.   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. For example, there are additional manufacturers and/or models of Windows based mobile devices that were installed with the Microsoft Wallet App, also there are additional manufacturers and/or models of Android based mobile devices that were installed with the PayPal Mobile App, the Wells Fargo Wallet App, the Masterpass App, the Google Wallet App, the Android Pay App, the Google Pay App, or the Samsung Pay App, and there are additional models of Apple based mobile devices that were installed with the PayPal Mobile App, the Apple Wallet, and the Apple Pay App.

91.   Defendant has tested or used at least one of the Accused Infringing Devices in at least one of its retail establishments to process a payment for goods.

92.   Defendant has directed at least one of its employees to test or use at least one of the Accused Infringing Devices in at least one of its retail establishments to process a payment for goods.

93.   Defendant used NFC-enabled POS terminals within retail establishments to process credit transactions with the Accused Infringing Devices.

94.   The above described activities occurred prior to September 10, 2017.

95.   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.

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

97.   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: –

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

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

100.   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.

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

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

103.   As supported by the disclosures of Apple, the iPhone 6 is a portable identification system.
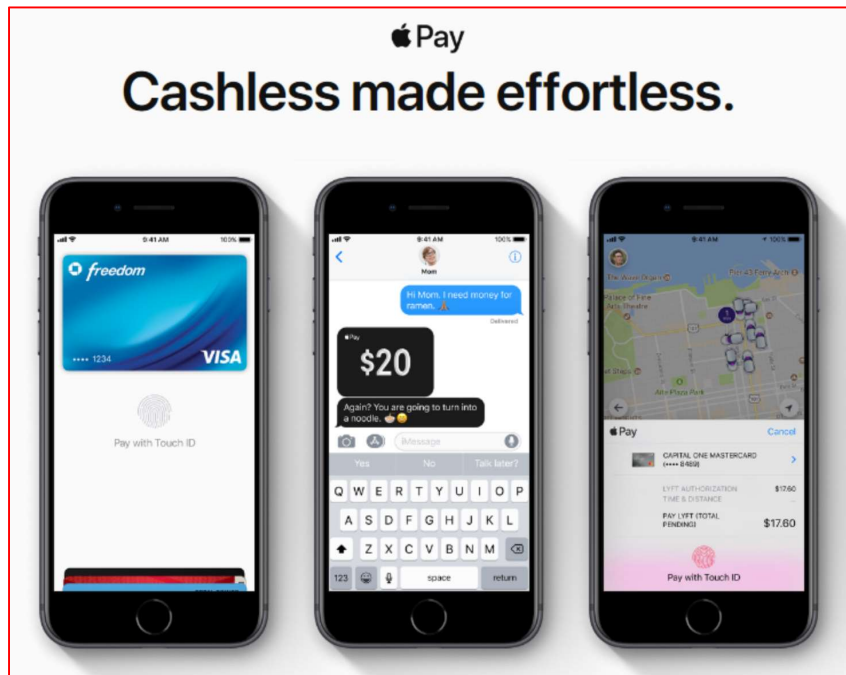
"Cashless   made   effortless"   ("**Cashless   Made   Effortless**"),   *available   at* https://www.apple.com/apple-pay/ (last accessed April 9, 2018).
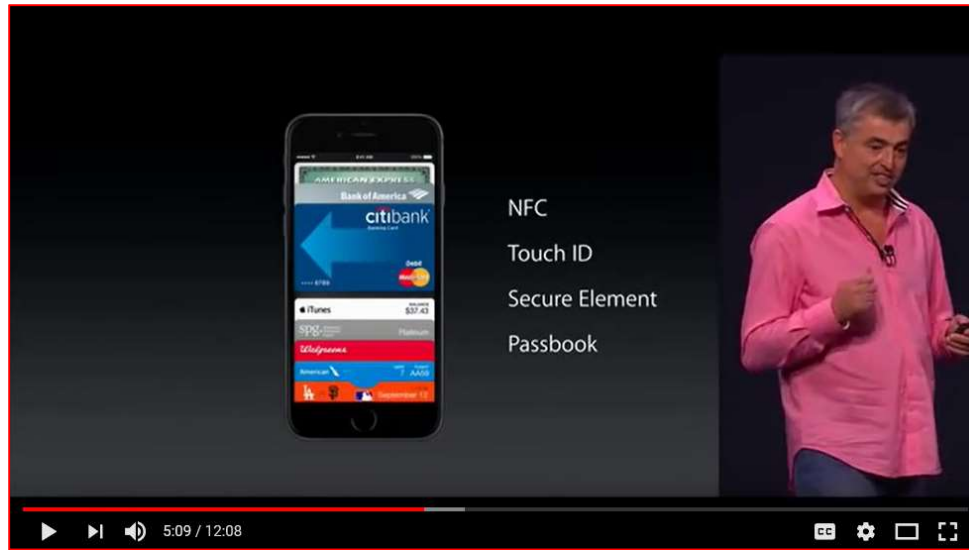
"Apple Pay Presentation (Sept 2014)" ("**Apple Pay Presentation**"), *available at*

https://www.youtube.com/watch?v=5ExcCyS1ZH8 (last accessed April 9, 2018).
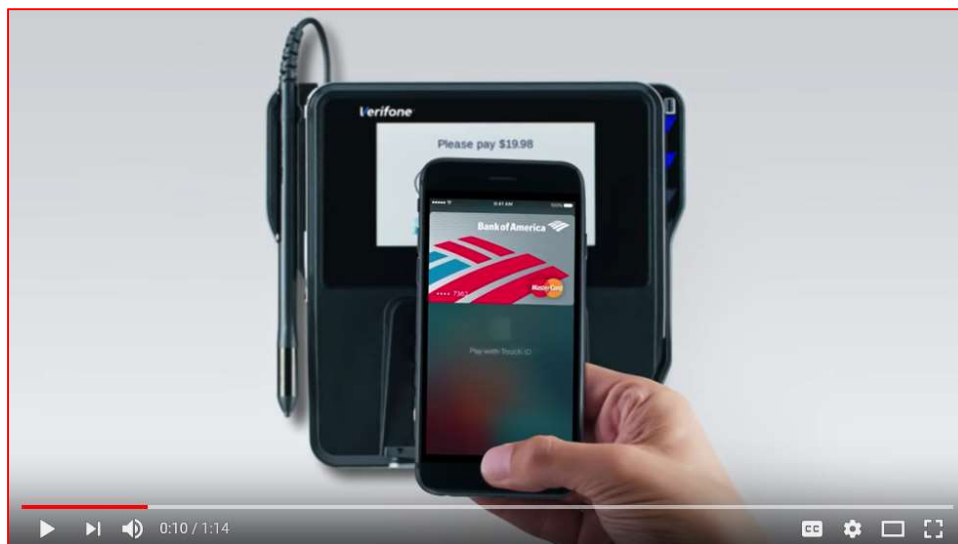
"iPhone – Guided Tour: Apple Pay" ("**iPhone – Guided Tour: Apple Pay**"), *available at*

https://www.youtube.com/watch?v=ez-2M3C_4wU (last accessed April 9, 2018).

"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 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 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.

Need help using Touch ID?
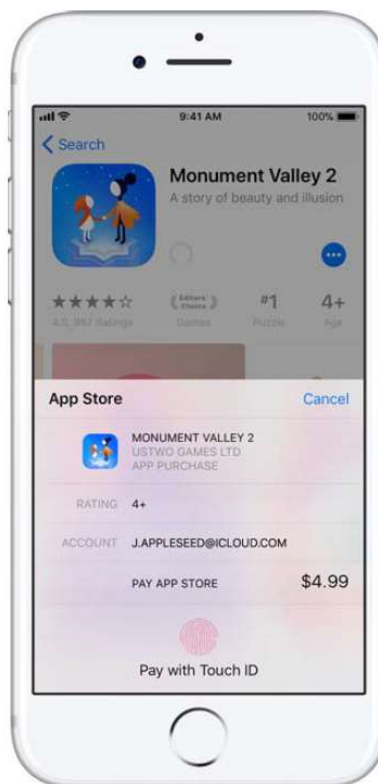
Use Touch ID.

Weight and Dimensions[2]

- Height: 5.44 inches (138.1 mm)
- Width: 2.64 inches (67.0 mm)
- Depth:0.27 inch (6.9 mm)
- Weight: 4.55 ounces (129 grams)

Technical Specifications.

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

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

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

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

107.   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.

Capacity[1]

- 16GB
- 32GB
- 64GB
- 128GB

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; –

108.   The iPhone 6 includes several inputs, including the Touch ID sensor and multiple wireless

radios (cellular, Wi-Fi, and NFC).

109.   The Touch ID sensor allows for the input of fingerprint images for processing into a

mathematical representation of a user's fingerprint.

110.   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.

111.   The NFC radio allows for communication with NFC-enabled credit card payment terminals

to receive data, including payment transaction details.

112.   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.

External Buttons and Connectors

- Home/Touch ID sensor
- Volume up/down
- Ring/silent
- On/off–Sleep/wake
- Microphone
- Lightning connector
- 3.5mm headphone jack
- Built–in speaker

Technical Specifications.

Sensors

- Touch ID
- Barometer
- Three-axis gyro
- Accelerometer
- Proximity sensor
- Ambient light sensor

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.

COMPLAINT FOR PATENT INFRINGEMENT 24

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; –

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

114.   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
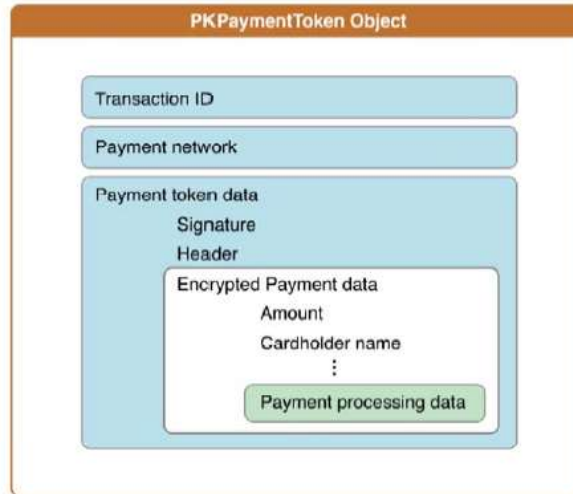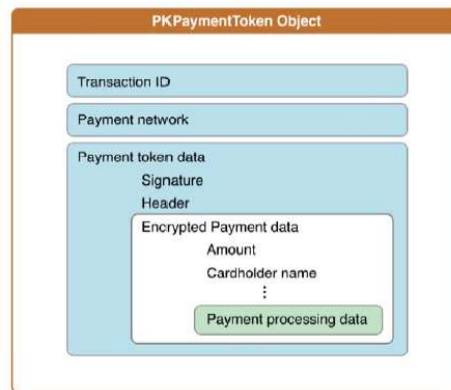
The Secure Element encrypts the token's payment data using either elliptic curve cryptography (ECC) or RSA encryption. The encryption algorithm is selected by the Secure Element based on the payment request. Most regions use ECC encryption. RSA is used only in regions where ECC encryption is unavailable 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; –*

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

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

COMPLAINT FOR PATENT INFRINGEMENT   28

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

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

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

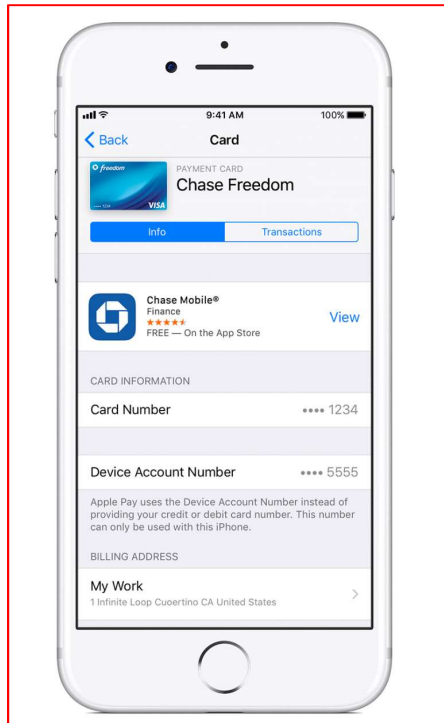120.   If there is not a match, the Apple Pay transaction is not authorized.

121.   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.

122.   This the Device Account Number is stored in the Secured Element.

123.   As supported by the disclosures of Apple, the Touch ID in combination with the Secure Enclave performs the function of determining user authorization or non-authorization by managing the authorization of Apple Pay based on matching a user's fingerprint data to registered fingerprint data, and the Touch ID and Secure Enclave are the same or equivalent structure to the disclosed verifying means, including the fingerprint scan and associated technology to perform biometric scanning.

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.

COMPLAINT FOR PATENT INFRINGEMENT   30

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.

COMPLAINT FOR PATENT INFRINGEMENT   31

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.

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.

> 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. –

124.   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.

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

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

127.   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.

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

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

130.   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.

131.   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.

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.

132.   The other Accused Infringing Devices operate in substantially the same manner.

"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).

How does Google Wallet/Android Pay work?

Google Wallet/Android Pay operates in two ways—card emulation with secure element (SE) and host-based card emulation. In card emulation with secure element, the device is placed on the NFC terminal and all the data read will be routed in SE, which is responsible for the communications with the NFC terminal. Once the transaction is done, the application can query the SE regarding the status and notify the user.
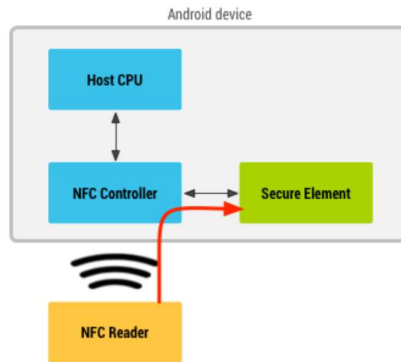
Card Emulation with a Secure Element (Source: *developer.android.com*)

"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).

Microsoft Wallet Details

How does it work?

The technology used for the new wallet is a form of near field communication (NFC) called host card emulation (HCE). Customers with debit and credit cards enrolled in Microsoft Wallet can make purchases at NFC-enabled terminals. This technology does not require access to a secure element embedded in the phone (like Apple Pay). Instead, card data is stored in the cloud.

The Microsoft Wallet provides security by using tokens for transactions, similar to Android Pay. Tokenization reduces risk for credit unions by replacing the PAN with a tokenized pseudo-PAN used in the payment system – all without impacting the acquiring side. Device profiles or passwords ensure transactions are initiated only by authorized user devices at recognized POS locations. User/device/account data is used to perform risk assessments for the transaction in real time through the client app and issuer back end.

Where can my members use Microsoft Wallet?

They can use Microsoft Wallet in stores where they see contactless terminals with either of these logos:

Which cards does Microsoft Wallet support?

Microsoft Wallet supports credit union credit and debit cards from MasterCard® and Visa®.

Which phones will support Microsoft Wallet?

The Lumia 650, 950 and 950 XL running Windows 10 Mobile. See the latest list of supported phones at www.microsoft.com/wallet
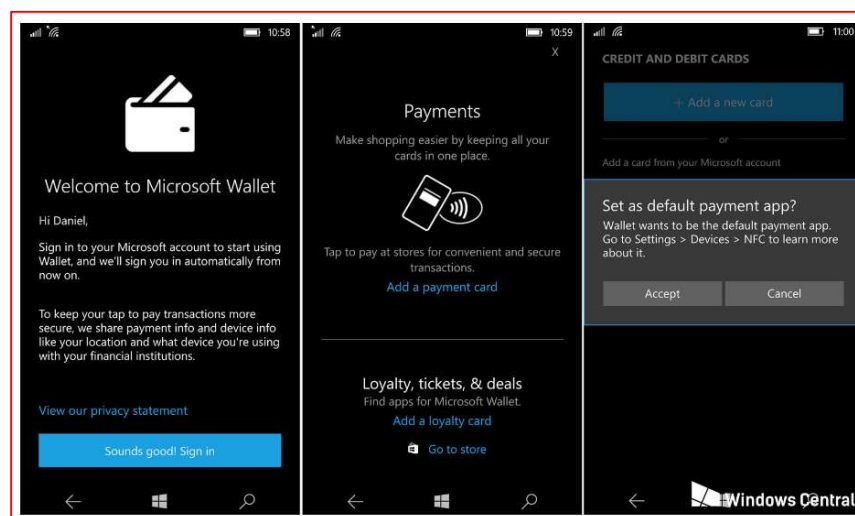
"Microsoft Wallet: FAQ" ("**Microsoft Wallet**"), at p. 3, *available at* https://www.co-opfs.org/media/microsoft_wallet_b2b_faq.pdf (last access April 4, 2018).

COMPLAINT FOR PATENT INFRINGEMENT   39
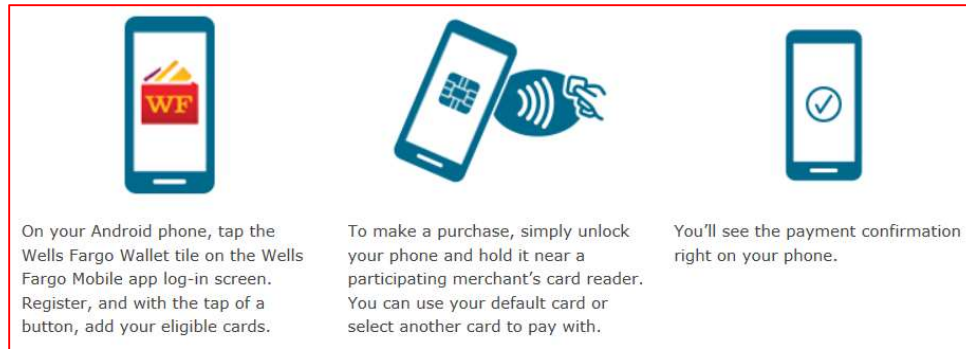
"Wells Fargo Wallet" ("**Wells Fargo Wallet**"), *available at* https://www.wellsfargo.com/

mobile-payments/wells-fargo-wallet/ (last accessed April 9, 2018).

Service	Supported Devices	How to Use	Number of Accepted Locations
Apple Pay	iPhone X, iPhone 8/8 Plus, 7/7 Plus, 6/6s, 6/6s Plus, SE, Apple Watch, iPad, iPad Air 2, iPad Pro, iPad Mini 3, 4, MacBook Pro with Touch Bar	Tap to pay with NFC at supported terminals	4 million
Google Pay (formerly known as Android Pay)	All NFC-enabled Android phones, tablets, watches running KitKat (4.4) or higher	Tap to pay with NFC at supported terminals	> 1.5 million
Samsung Pay	Galaxy Note 8, S8/S8+, S7/S7 Edge; S6/S6 Edge/S6 Edge+; Galaxy Note 5; Gear S2, S3 watches	Tap to pay with NFC at supported terminals, supports MST, EMV readers	> 30 million

"Mobile Wallets: Apple Pay vs Samsung Pay vs Google Pay" ("**Mobile Wallets**"), *available at*

https://www.tomsguide.com/us/mobile-wallet-guide,news-20666.html (last accessed April 9,

2018).

"NFC Tap to Pay is coming to Windows 10 Mobile with Microsoft Wallet 2.0" ("**NFC Tap to Pay**"), *available at* https://www.windowscentral.com/nfc-tap-pay-coming-windows-10-mobile (last accessed April 9, 2018).
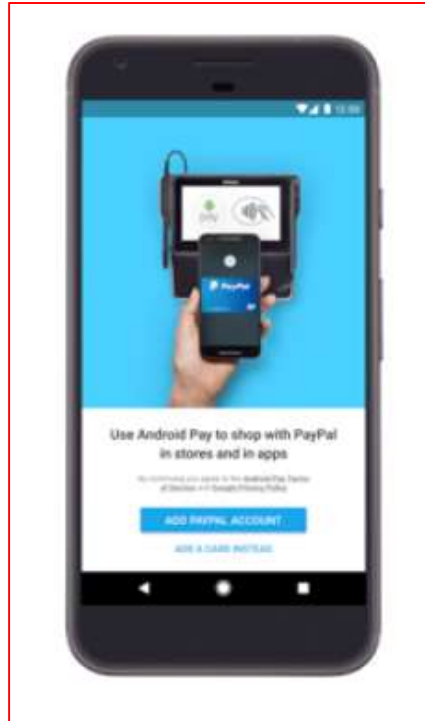
"PayPal teams up with Android Pay for mobile payment" ("**PayPal teams up with Android**"), *available at* https://techcrunch.com/2017/04/18/paypal-teams-up-with-android-pay-for-mobile-payments/ (last accessed April 9, 2018).

133.   In the operation and control of the POS terminal, Defendant exercised control of the Accused Infringing Devices by issuing commands from the POS terminal to the Accused Infringing Devices to initiate and control the generation of a response from the Accused Infringing Devices, which included an authorization code necessary to complete a credit transaction.

Benefits of Use

134.   In the operation and control of the POS terminal in conjunction with the Accused Infringing Devices, Defendant put the Accused Infringing Devices, as claimed in the '391 Patent, as a whole into service for its benefit.

135.   Defendant derived a direct and meaningful benefit from the use of the Accused Infringing Devices as claimed in the '391 Patent.

136.   Defendant derived a direct and meaningful benefit from the use of each and every element of the Accused Infringing Devices as claimed in the '391 Patent.

Credit card theft, fraud, and identity theft are serious concerns to retailers, including Defendant. Recently, the payment card systems for Home Depot, Target, Neiman Marcus, Panera Bread were breached. In the breaches, over 50,000,000 credit card numbers were stolen along with the credit card account owners' information, including address and name. Both Home Depot, Target, and their customers suffered great harm as a result of the breach of the payment credit card systems. As a result, Target agreed to pay $19 million to banks that issued MasterCards involved in the data breach. Target also agreed to pay $10 million to settle a class-action lawsuit related to the data breach. *See, e.g.,* "Case Study: The Home Depot Data Breach" ("**The Home Depot Data Breach**"), *available at* https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367 (last accessed April 9, 2018); "Anatomy of the Target data breach: Missed opportunities and lessons Learned" ("**Anatomy of the Target Data Breach**"), *available at* http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/ (last accessed April 9, 2018); "Target Paying $19 Million to MasterCard Banks Over Breach" ("**Target Paying $19 Million to MasterCard**"), *available at* http://fortune.com/2015/04/16/target-mastercard/ (last accessed April 9, 2018); "Target Offers $10

Million Settlement In Data Breach Lawsuit" ("**Target Offers $10 Million Settlement**"), *available at* https://www.npr.org/sections/thetwo-way/2015/03/19/394039055/target-offers-10-million-settlement-in-data-breach-lawsuit (last accessed April 9, 2018); "Panerabread.com Leaks Millions of Customer Records" ("**Panerabread.com Leaks Millions of Customer Records**"), *available at* https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/ (last accessed April 9, 2018); "Neiman Marcus Reports New Breach" ("Neiman Marcus Reports New Breach"), *available at* https://www.bankinfosecurity.com/new-neiman-marcus-breach-authentication-must-change-a-8843 (last accessed April 9, 2018); "5 million credit cards exposed in Saks and Lord & Taylor data breach" ("5 Million credit cards exposed"), *available at* https://nakedsecurity.sophos.com/2018/04/03/5-million-credit-cards-exposed-in-saks-and-lord-taylor-data-breach/ (last accessed April 9, 2018); "This Week In Credit Card News: A Record Number of Data Breaches; Starbucks Enters Credit Card Market" ("**A Record Number of Data Breaches**") ("The Identify Theft Resource Center reports the number of U.S. data breaches reached an all-time high in 2017. Data breaches totaled 1,579, up 45% from 2016. 55% hit the business sector…"), *available at* https://www.forbes.com/sites/billhardekopf/2018/02/02/this-week-in-credit-card-news-a-record-number-of-data-breaches-starbucks-enters-credit-card-market/#1c5af1a07346 (last accessed April 9, 2018); and "Equifax breach exposes data of 147.9 million U.S. consumers") ("**Equifax breach exposes data of 147.9 million**"), *available at* https://www.creditcards.com/credit-card-news/equifax-data-breach-143-million-id-theft.php (last accessed April 9, 2018);

137.   When retailers, including Defendant, processed payments using the Accused Infringing Devices, the retailer was able to avoid the data breach problem and liabilities suffered by Home Depot, Target, Neiman Marcus, Saks, Lord & Taylor, and others for transactions using the

Accused Infringing Devices because, during such transactions, the retailer never obtained the customers' credit card number. See, *e.g.,* "Unable to target Apple Pay, criminals unsurprisingly stick to bank fraud, identity theft" ("**Unable to Target Apple Pay**"), *available at* https://www.imore.com/unable-target-apple-pay-criminals-unsurprisingly-stick-fraud-identity-theft (last accessed April 9, 2018).

138.   Defendant obtained many benefits as a result of using the Accused Infringing Devices, including providing a simpler method for processing payments, providing a more secure transaction process, providing a greater privacy to its customers, lowering the risks of credit card breaches, providing a better customer experience, avoiding paying extra fees to banks or processors when using the Accused Infringing Devices, providing faster checkout times, achieving shorter checkout lines, and being able to have fewer required personnel during peak business hours. These benefits provide a direct competitive and monetary advantage to Defendant. "Explaining Apple Pay: Pros, Cons" ("**Explaining Apply Pay**"), *available at* https://www.practicalecommerce.com/Explaining-Apple-Pay-Pros-Cons (last accessed April 9, 2018); "All About Apple Pay" ("**All About Apple Pay**"), *available at* https://merchantservicesltd.com/apple-pay/ (last accessed April 9, 2018); "Apple Pay: 4 Reasons for Businesses to Adopt it (And 4 Reasons to Avoid it)" ("**Apple Pay; 4 Reasons for Business to Adopt it**"), *available at* https://www.businessnewsdaily.com/7295-apple-pay-4-reasons-for-businesses-to-adopt-it-and-4-reasons-to-avoid-it.html (last accessed April 9, 2018); "Apple Pay - What it Means for Retail" ("**Apple Pay - What it Means for Retail**"), *available at* https://www.trc-solutions.com/apple-pay-means-retail/ (last accessed April 9, 2018); and "About Apple Pay for Merchants" ("**About Apple Pay for Merchants**"), *available at* https://support.apple.com/en-us/HT204274 (last accessed April 9, 2018).
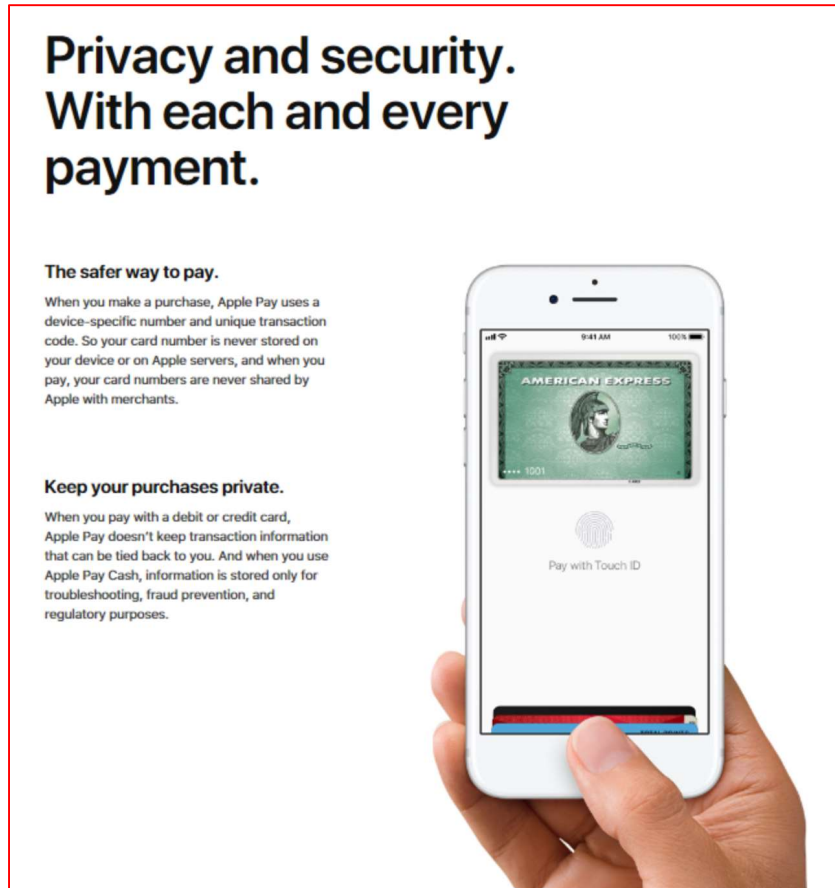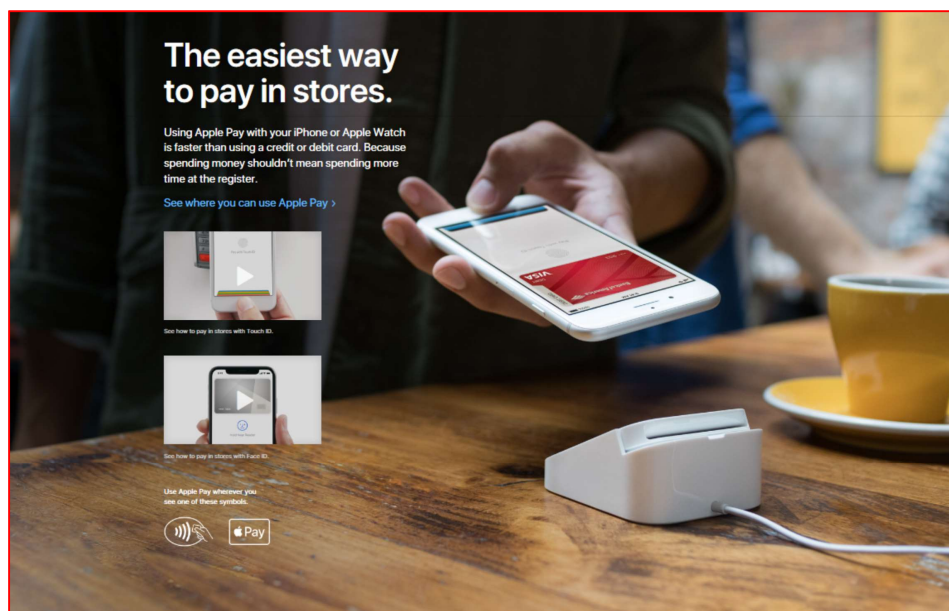
Cashless Made Effortless.

139.   With respect to operations involving a NFC-enabled POS terminal, the Accused Infringing

Devices emulated the behavior of a contactless credit card. When used, the process began when

the POS terminal operated by the Defendant transmitted commands to the Accused Infringing

Device. The Accused Infringing Device received the command and information relating to the

transaction. The Accused Infringing Device verified the identity of the authorized user and

generated the appropriate authorization code according to the instructions from the POS terminal.

The POS terminal then received the authorization code from the Accused Infringing Devices and

completed the transaction approval process by sending the authorization code to a servicing bank.

"An Introduction to NFC Standards" ("**Introduction to NFC Standards**"), *available at*

http://www.icma.com/ArticleArchives/StandardsOct12.pdf (last accessed April 9, 2018); "NFC

Standards" ("**NFC Standards**"), *available at* http://www.themobileknowledge.com/wp-content/uploads/2017/05/NFC-Standards.pdf (last accessed April 9, 2018); "NFC Essentials" ("**NFC Essestials**"), *available at* http://www.themobileknowledge.com/wp-content/uploads/2017/05/NFC-Essentials-v2.0.1.pdf (last accessed April 9, 2018); "Smart Card Technology FAQ" ("**Smart Card Technology**"), *available at* http://www.smartcardalliance.org/smart-cards-faq/ (last accessed April 9, 2018).

140.   The interchange of commands issued from the POS terminal to the Accused Infringing Devices and responses to the commands received from the Accused Infringing Devices to the POS terminal is specified, in part, according to the ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 18092, and ISO/IEC 21481 standards. *Id.*

Cashless Made Effortless.

141.   "Which is safer: Apple Pay or credit cards?" ("**Which is safer**"), *available at* https://www.youtube.com/watch?v=06ZWlNuaeMM&t=16s (last accessed April 9, 2018).
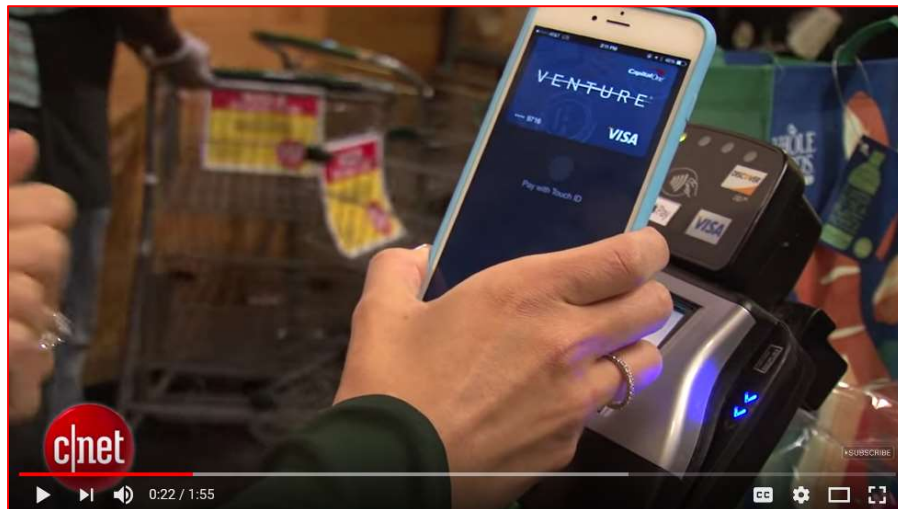
142.   "Apple Pay is the most secure way to pay, with a catch" ("**Apple Pay is the most secure way to pay**"), *available at* https://www.youtube.com/watch?v=9-f4rdSq2QY (last accessed April 9, 2018)

143.   When Defendant's customers purchased goods, Defendant directed and controlled the use of the Accused Infringing Devices in the process of completing credit transactions, including the timing and conditions of the use. In particular, the Defendant, with the use of the POS terminal,

initiated communications from the POS terminal to the Accused Infringing Devices with commands to initiate functions and operations within the device. This communication was timed to occur after determining the amount of sale for goods the customer wanted to purchase. Upon initiating communication, the Accused Infringing Devices verified the identity of the customer as an authorized person to approve the credit transaction. The Accused Infringing Devices then generated an authorization code and transmitted the authorization code to the Defendant. The Defendant then transmitted the authorization code to a bank servicing partner for final approval of the sale. Upon receiving approval from the bank servicing partner, the Defendant completed the sale with the customer. In this process, the Defendant conditioned the sale to the customer based on the customer using the Accused Infringing Device as directed by Defendant to verify the customer's identity. If the customer failed to verify their identity with the Accused Infringing Devices, the Defendant did not process the credit transaction using the Accused Infringing Device. Without the Defendant's actions, directions, and control, the Defendants' customers would not have been able to use the Accused Infringing Devices to purchase goods from the Defendant.

144.   Defendant has acted alone and in concert with others, including its customers, and is otherwise liable jointly, severally or otherwise for a right to relief related to or arising out of the same transaction, occurrence or series of transactions or occurrences related to using at least one of the Accused Infringing Devices.

145.   The Defendant received a benefit of a completed sales transaction upon the performance of using the Accused Infringing Devices.

146.   As described above, Defendant realizes several benefits from its use of the Accused Infringing Devices, including:

- providing simpler payments for its customers, which increased customer satisfaction and contributed to repeat business, increased customer referrals, and provided improved good will;

- more secure transactions, which reduced fraud and lowered transaction costs with credit servicing companies;

- providing greater privacy to its customers, which increased customer satisfaction, contributed to repeat business, increased customer referrals, and reduced liability as a result of data breaches;

- lower risks of credit card data breaches, which increased customer satisfaction and reduced liability to customers and banks as a result of credit card data breaches;

- better customer experience, which increased customer satisfaction, contributed to repeat business, and increased customer referrals;

- no extra fees from banks or processors, which allowed the Defendant to provide increased services with no additional price increase in goods to pay for the increased services;

- faster checkout times, which allowed the Defendant to provide services to more customers without increased costs, increased customer satisfaction, contributed to repeat business, increased customer referrals;

- shorter lines, which increased customer satisfaction, contributed to repeat business, and increased customer referrals; and

- less required personnel during peak business hours, which reduced labor costs for processing sales transactions (collectively "the Asserted Benefits").

See, e.g., **Explaining Apply Pay; All About Apple Pay; Apple Pay; 4 Reasons for Business to Adopt it; Apple Pay - What it Means for Retail; and About Apple Pay for Merchants.**

147.   Additionally, Defendant benefitted from the use of each and every element of the Accused Infringing Devices as claims in the '391 Patent.

148.   As non-limiting examples, set forth below (with claim language in italics) is a description of exemplary benefits to Defendant for each element of Claim 1 of the '391 Patent as a result of the use of the Accused Infringing Devices.

   1(a) A portable identification system comprising: –

149.   As described above, Defendant benefited from the use of the Accused Infringing Devices to complete a credit transaction for the sale of goods to customers by which the Defendant derived a profit. By use of the Accused Infringing Devices, Defendant received the Asserted Benefits. *Id.*

150.   The Defendant benefitted through the use of the Accused Infringing Devices because the Defendant did not need to verify its customers' personal identification through the use of an issued personal identification card (e.g. driver's license) in order to authorize use of a particular credit card.

151.   The Defendant benefitted through the use of the Accused Infringing Devices because the Defendant did not receive the customers' credit card number, thereby alleviating the Defendant from liability associated with data breaches, identity theft, fraud, and possible charge backs from the bank servicing the credit card transactions.

152.   The Defendant benefitted through the use of the Accused Infringing Devices because the Defendant was able to process sales transactions faster resulting in faster payment processing for customers, shorter checkout lines, reduced personnel during peak times, thereby increasing profitability while providing customers a more enjoyable shopping experience.

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

153.   The Defendant benefited from the use of a storage medium for storing electronic data in the Accused Infringing Devices. This storage medium allowed the Accused Infringing Devices to store incoming commands from the POS terminal, to store biometric or other distinctive information for the authorized credit card account holder, and to store generated access codes.

154.   Without the use of a storage medium in the Accused Infringing Devices, the Defendant would have been prohibited from processing a credit transaction to receive the Asserted Benefits.

155.   With the use of the storage medium in the Accused Infringing Devices, the other claimed elements in the Accused Infringing Devices were able to operate to authorize the credit transaction for the sale goods from the Defendant, thereby benefiting the Defendant.

156.   With the use of the storage medium, the Defendant was able to realize the Asserted Benefits.

1(c) one or more inputs; –

157.   The Defendant benefited from the use of one or more inputs in the Accused Infringing Devices. The one or more inputs (e.g. NFC radio receiver) allowed the Accused Infringing Devices to receive commands from the POS terminal to initiate and process credit transactions for the sale of goods from Defendant. Additional inputs (e.g. biometric fingerprint reader) allowed the Accused Infringing Devices to verify the identity of the authorized account holder to approve the transaction from the sale of goods from the Defendant.

158.   Without the use of the one or more inputs in the Accused Infringing Devices, the Defendant would have been prohibited from processing a credit transaction to receive the Asserted Benefits.

159.   With the use of the one or more inputs in the Accused Infringing Devices, the verification means element in the Accused Infringing Devices was able to operate to authorize the credit transaction for the sale goods from the Defendant, thereby benefiting the Defendant.

160.   With the use of the one or more inputs in the Accused Infringing Devices, the Defendant was able to prevent a fraudulent sales transaction, thereby benefiting the Defendant.

161.   With the use of the one or more inputs, the Defendant was able to realize the Asserted Benefits.

1(d) one or more outputs; –

162.   The Defendant benefited from the use of one or more outputs in the Accused Infringing Devices. The one or more outputs (e.g. NFC radio transmitter) allowed the Accused Infringing Devices to transmit responses to commands from the POS terminal to initiate and process credit transaction for the sale of goods from Defendant.

163.   The one or more outputs allowed the Accused Infringing Devices to transmit to the Defendant the generated access code need to approve and authorize the credit transaction for the sale of goods from the Defendant, thereby benefiting the Defendant.

164.   Without the use of the one or more outputs in the Accused Infringing Devices, the Defendant would have been prohibited from processing a credit transaction to receive the Asserted Benefits.

165.   With the use of the one or more outputs in the Accused Infringing Devices, the Defendant would not have been able to receive the appropriate authorization code to authorize and complete the credit transaction for the sale goods from the Defendant.

166.   With the use of the one or more outputs in the Accused Infringing Devices, the Defendant was able to prevent a fraudulent sales transaction, thereby benefiting the Defendant.

167.   With the use of the one or more outputs, the Defendant was able to realize the Asserted Benefits.

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 –

168.   The Defendant benefited from the use of the verifying means element in the Accused Infringing Devices. The verifying means element allowed the Accused Infringing Devices to identify the authorized account holder for the credit transaction for the sale of good from the Defendant.

169.   The verifying means element allowed the Accused Infringing Devices to generate an access code that was transmitted to the POS terminal that was required in order for Defendant to process the credit transaction for the sale of goods from the Defendant, thereby benefiting the Defendant.

170.   Without the use of the verifying means element in the Accused Infringing Devices, the Defendant would have been prohibited from processing a credit transaction to receive the Asserted Benefits.

171.   Without the use of the verifying means element in the Accused Infringing Devices, the Defendant would have not been able to receive the appropriate authorization code to authorize and complete the credit transaction for the sale goods from the Defendant.

172.   With the use of the verifying means element in the Accused Infringing Devices, the Defendant was able to prevent a fraudulent sales transaction, thereby benefiting the Defendant.

173.   With the use of the verifying means element, the Defendant was able to realize the Asserted Benefits.

> *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. –*

174.   The Defendant benefited from the use of the code generator in the Accused Infringing Devices. The code generator allowed the Accused Infringing Devices to generate an access code

that was transmitted to the POS terminal that was required in order for Defendant to process the credit transaction for the sale of goods from the Defendant identify the authorized account holder for the credit transaction for the sale of good from the Defendant.

175.   Without the use of the code generator in the Accused Infringing Devices, the Defendant would have been prohibited from processing a credit transaction to receive the Asserted Benefits.

176.   With the use of the code generator in the Accused Infringing Devices, the Defendant was able to receive the appropriate authorization code to authorize and complete the credit transaction for the sale goods from the Defendant, thereby benefiting the Defendant.

177.   With the use of the code generator in the Accused Infringing Devices, the Defendant was able to prevent a fraudulent sales transaction, thereby benefiting the Defendant.

178.   With the use of the code generator, the Defendant was able to realize the Asserted Benefits.

179.   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: April 9, 2018

Respectfully Submitted

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

THE MORT LAW FIRM, PLLC
106 E. Sixth Street, Suite 900
Austin, Texas 78701
Tel. (512) 865-7950

ATTORNEYS FOR PLAINTIFF