IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

UNIVERSAL SECURE REGISTRY LLC, Plaintiff, v. APPLE INC., VISA INC., and VISA U.S.A., INC., Defendant.	)	C.A. No. _____ **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Universal Secure Registry LLC ("USR") hereby asserts the following claims for patent infringement against Defendants Apple Inc. ("Apple"), and Visa Inc. and Visa U.S.A. Inc. (collectively, "Visa," and with Apple, "Defendants"), and alleges as follows:

NATURE OF THE ACTION

1. This is a civil action for patent infringement under the patent laws of the United States, 35 U.S.C. § 1, *et seq.*

2. Defendants have infringed and continue to infringe, have contributed to and continue to contribute to infringement of, and have induced and continue to induce infringement of one or more claims of USR's U.S. Patent Nos. 8,577,813 ("the '813 patent"), 8,856,539 ("the '539 patent"), 9,100,826 ("the '826 patent"), and 9,530,137 ("the '137 patent") (collectively, the "Asserted Patents") at least by providing products, systems and services related to the Apple Pay service.

3. USR is the legal owner by assignment of the Asserted Patents, which were duly and legally issued by the United States Patent and Trademark Office ("USPTO"). USR seeks injunctive relief and monetary damages.

THE PARTIES

4. USR is a limited liability company organized and existing under the laws of the Commonwealth of Massachusetts with its principal place of business at 59 Sargent St. in Newton, Massachusetts.

5. Upon information and belief, Defendant Apple Inc. is a corporation organized and existing under the laws of the State of California with its principal place of business at 1 Infinite Loop, Cupertino, California.

6. Upon information and belief, Defendant Visa Inc. is a corporation organized and existing under the laws of the State of Delaware with its principal place of business at 900 Metro Center Boulevard in Foster City, California.

7. Upon information and belief, Defendant Visa U.S.A. Inc. is a corporation organized and existing under the laws of the State of Delaware with its principal place of business at 900 Metro Center Boulevard in Foster City, California.

8. Upon information and belief, each of the Defendants directly and/or indirectly imports, develops, designs, manufactures, distributes, markets, offers to sell and/or sells infringing products and services in the United States, including in the District of Delaware, and otherwise purposefully directs infringing activities to this District in connection with providing the Apple Pay service.

9. Upon information and belief and as further explained below, Defendants have been and are acting in concert and are 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 the making, using, importing into the United States, offering for sale or selling of at least one infringing product, process, or service in this District in connection with

providing the Apple Pay service. In addition, this action involves questions of law and fact that are common to all Defendants.

JURISDICTION AND VENUE

10. This is a civil action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq*.

11. This Court has subject matter jurisdiction over the matters asserted herein under 28 U.S.C. §§ 1331 and 1338(a).

12. Apple is subject to this Court's personal jurisdiction. Apple has infringed USR's patents in Delaware by, among other things, engaging in infringing conduct within and directed at or from this District. For example, Apple has purposefully and voluntarily placed one or more of its infringing products, as described below, into the stream of commerce with the expectation that these infringing products will be used in this District. These infringing products have been and continue to be used in this District.

13. Apple employs individuals and operates a retail store at 125 Christiana Mall in Newark, Delaware in this District. Upon information and belief, this store sells more infringing iPhones than any other Apple retail location, and sells and/or supports the second-most volume of infringing products out of any Apple retail location. *See* "Apple's (AAPL) Delaware Store Claims Title for Selling Most iPhones," *available at* http://abcnews.go.com/Business/apples-delaware-store-claims-title-selling-iphones/story?id=20650009.

14. Customers use the infringing Apple Pay service with their Apple devices at a large number of retailers with locations within this District, including Ace Hardware, Chevron, Dunkin' Donuts, KFC, Macy's, McDonald's, Starbucks, and Subway. *See* "Apple Pay: Where to Use," *available at* https://www.apple.com/apple-pay/where-to-use/.

15. Apple has also repeatedly availed itself of the jurisdiction of this Court by filing complaints for patent infringement in this District (*see, e.g., Apple Inc. v. HTC Corp. et al*, C.A. No. 11-611-GMS; *Apple Inc. v. HTC Corp. et al*, C.A. No. 10-544-GMS; *Apple Inc. v. HTC Corp. et al*, C.A. No. 10-167-GMS; *Apple Inc. v. HTC Corp. et al*, C.A. No. 10-166-GMS; *Apple Inc. v. Atico Int'l USA Inc. et al*, C.A. No. 8-283-GMS).

16. Visa is subject to this Court's personal jurisdiction. Visa Inc. and Visa U.S.A. Inc. are corporations organized and existing under the laws of the State of Delaware. Visa has infringed USR's patents in Delaware by, among other things, engaging in infringing conduct within and directed at/or from this District. For example, Visa has purposefully and voluntarily placed one or more of its infringing products, as described below, into the stream of commerce with the expectation that these infringing products will be used in this District. These infringing products have been and continue to be used in this District.

17. Visa employs individuals and is actively hiring individuals for positions located in Wilmington, Delaware, within this District. *See, e.g.*, "Careers at Visa," *available at* https://usa.visa.com/careers.html (last accessed May 19, 2017).

18. Customers use the infringing Apple Pay service with their Visa payment cards at a large number of retailers with locations within this District, including Ace Hardware, Chevron, Dunkin' Donuts, KFC, Macy's, McDonald's, Starbucks, and Subway. *See* "Apple Pay: Where to Use," *available at* https://www.apple.com/apple-pay/where-to-use/.

19. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391 and 1400 at least because, as discussed above, Visa is incorporated in this District and Apple has a regular and established place of business in this District, each Defendant is subject to personal jurisdiction in this District, each Defendant regularly conducts business in this District, and each

Defendant has committed and continues to commit acts of direct and indirect patent infringement complained of herein within this District.

USR'S HISTORY AND PATENTED TECHNOLOGY

20. USR was founded by Dr. Kenneth P. Weiss, the current Chairman and CEO of USR and a recognized expert in the fields of information systems security and identity authentication, especially computer-based multifactor identity authentication. Before starting USR, Dr. Weiss founded and served for many years as the CTO and Chairman of the Board of Security Dynamics Technologies Inc., now RSA Security LLC, a part of Dell Technologies. At Security Dynamics, Dr. Weiss invented the SecurID tokens and their underlying algorithm: technology that became a leading form of personal identity authentication for computer security and electronic commerce. Dr. Weiss' SecurID technology is being used by more than 150 million people, more than 90% of Fortune 500 companies, and corporations, consumers, governments, and banks in more than 30 countries. His technology has been used by all three branches of the United States government, including the Defense Department, the Treasury Department, the Senate, and the White House.

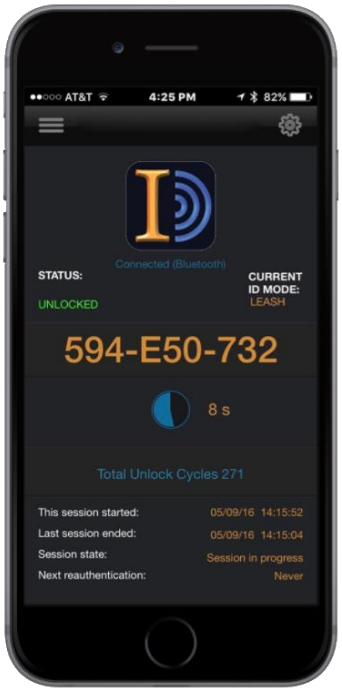
21. In connection with his work at USR, Dr. Weiss has developed and continues to develop innovative technological solutions for identity authentication, computer security, and digital and mobile payment security. USR's patented innovations allow a user to securely authenticate his or her identity using technology built into a personal electronic device combined with the user's own secret and/or biometric information. Such authentication is secure, useful, and convenient across a variety of contexts.

22. Applied to payment card transactions (for example, those involving credit, debit, charge, prepaid, gift, or rewards card accounts), USR's technology offers a state-of-the-art processing solution that is both highly secure and highly convenient. USR's patented technology

can allow a user to employ an electronic device, such as a smartphone, as an "electronic wallet" capable of interacting with point-of-sale devices (or directly with webpages and other digital storefronts) to safely and securely authorize payments from one or more payment accounts.

23. USR's patented technology enables users to conduct highly secure transactions from their mobile phones, laptop computers, and other electronic devices with a simple click, touch, and/or other biometric input. Using aspects of USR's technology, the user device does not store or send any sensitive information, such as personal account information or payment card details, that, if compromised, could be used for fraudulent purposes. Instead, the user device locally generates and sends data including a cryptographic value used for authentication. A new cryptographic value is generated each time a transaction occurs, and the value is verified by the payment processor before the transaction is approved. Using additional aspects of USR's technology, the user device will require the user to authenticate himself or herself via entry of secret information (e.g., a pin) and/or biometric information (e.g., a fingerprint) before the user device will carry out a payment. As a result, even if the user device is lost or stolen or the one-time cryptographic value is intercepted, neither the user device nor the value can be used to make a fraudulent purchase. Hence, the novel technology described and claimed in the Asserted Patents is safe, private, and convenient.

24. Today, USR actively develops and markets a line of security applications and products leveraging its patented technology. For example, USR's licensed "USR ID" application has been touted "the most secure personal proxy in the world" and utilizes three-factor authentication to automatically lock and unlock an authorized user's computer as the user walks to and from her computer. A sample image of the USR ID application running on an iPhone is shown below:



25. The '813 patent, granted by the USPTO on November 5, 2013, is entitled "Universal Secure Registry." Dr. Weiss is the sole named inventor. USR is the original and current owner by assignment of the '813 patent. A true and correct copy of the '813 patent is attached hereto as Exhibit A.

26. The '539 patent, granted by the USPTO on October 7, 2014, is entitled "Universal Secure Registry." Dr. Weiss is the sole named inventor. USR is the original and current owner by assignment of the '539 patent. A true and correct copy of the '539 patent is attached hereto as Exhibit B.

27. The '826 patent, granted by the USPTO on August 14, 2015, is entitled "Method and Apparatus for Secure Access Payment and Identification." Dr. Weiss is the sole named inventor. USR is the original and current owner by assignment of the '826 patent. A true and correct copy of the '826 patent is attached hereto as Exhibit C.

28. The '137 patent, granted by the USPTO on December 27, 2016, is entitled "Method and Apparatus for Secure Access Payment and Identification." Dr. Weiss is the sole

named inventor. USR is the original and current owner by assignment of the '137 patent. A true and correct copy of the '137 patent is attached hereto as Exhibit D.

ACTS GIVING RISE TO THIS ACTION

29. At the iPhone 6 launch event in September of 2014, Apple CEO Tim Cook explained: "[p]ayments is a huge business. Every day between credit and debit we spend $12 billion. That's over $4 trillion a year and that's just in the United States. And this business is comprised of over 200 million transactions a day." For decades, in a typical transaction, a customer would slide his or her card through a point-of-sale ("POS") device at a merchant checkout location, and the POS device would read information such as card number and expiration date from a magnetic strip on the back of the card. That information would pass through a card network, such as Visa or MasterCard networks, and ultimately to the issuing bank for transaction approval (or disapproval).

30. The traditional magnetic strip lacks adequate security and is highly susceptible to fraud. In an attempt to reduce fraud, a consortium of payment-card companies introduced the "EMV chip" into payment cards, which made them more difficult to copy. But cards with the EMV chip, too, are insecure. For example, an EMV chip does not prevent a nefarious actor from carrying out unauthorized transactions using a stolen card, or from intercepting and fraudulently using card information that is transmitted during an ordinary transaction.

31. Thus, the need existed for technology that would allow consumers to make payment-card transactions conveniently and with a high-degree of security. Recognizing very early on—long before Apple, Visa, and others in the payment industry—that mobile phones and other personal electronic devices provided an optimal platform to meet this need, Dr. Weiss developed and patented superior technology using such devices to provide a mobile, efficient,

and highly secure system for making payment-card transactions. Dr. Weiss was the first in this space, and the secure payment technology that he developed is the core of Apple Pay.

32. Recognizing the enormous promise of his technology, Dr. Weiss and USR sought to partner with both and Apple and Visa to develop a commercial implementation. To that end, Dr. Weiss and USR disclosed their patented technology to Apple and Visa a number of years before the development and release of Apple Pay.

33. In 2010, USR sent Apple a series of letters describing USR's patented technology. On July 14, 2010, USR sent Apple a letter seeking to partner with Apple to jointly develop a payment-card solution that "is integrated with and centers around a software-modified payment phone." In another letter sent to Apple on September 7, 2010, USR further elaborated that its patented technology, which employed smart mobile devices for secure financial transactions, "eliminates the need for account numbers or any sensitive or private information to be stored in or transmitted from a smart mobile device." That letter also explained that one of USR's allowed patent applications "employ[s] a biometric for identity authentication on a smart phone." On September 21, 2010, USR sent Apple another letter touting the potential benefit of incorporating USR's technology into the iPhone platform, and describing USR's growing patent portfolio.

34. Around the same time, USR pursued a partnership with Visa Inc. In mid-2010, Dr. Weiss and USR engaged in a series of confidential discussions with senior representatives of Visa, including then-Chairman and CEO, Joseph Saunders, and then-Global Head of Strategy and Corporate Development, Oliver Jenkyn. During these discussions, USR made detailed presentations of USR's patented technology under protection of a Non-Disclosure Agreement.

35. Neither Apple nor Visa ever partnered with USR. Instead, they partnered with each other and with other payment networks and banks to incorporate USR's patented technology

into a service called Apple Pay, which works in conjunction with Apple products, like iPhones, iPads, Apple watches, and various Mac computers. Upon information and belief, Apple and Visa began working together on Apple Pay at least as early as January 2013, and Visa dedicated approximately 1,000 people towards the development project with Apple.

36. On September 9, 2014, Apple publicly launched Apple Pay in its keynote address introducing the iPhone 6. In this address, Apple touted the same benefits that USR had introduced to Apple and Visa in 2010. For instance, just as USR disclosed to Apple and Visa that its patented technology eliminated the need to store or transmit payment-card account numbers, Apple bragged to its users that with Apple Pay, "the credit card isn't stored on the device." Since then, Apple Pay's growth has been explosive.

37. Defendant Visa operates the world's largest payment processing network called VisaNet. Upon information and belief, VisaNet is capable of handling more than 24,000 transaction messages per second and processes more than 150 million transactions every day. Upon information and belief, Visa teamed with Apple to develop and incorporate the Apple Pay service into Apple's iOS devices, enabling users to employ their Visa cards as a part of Apple Pay transactions processed using the Visa Token Service, a digital and mobile payment service developed in conjunction with Apple Pay. On information and belief, since Apple Pay launched in 2014, Visa has supported and processed all Apple Pay transactions made with Visa cards.

38. Many Delaware-based banks issue US-branded payment cards. Upon information and belief, Apple Pay supports these payment cards and most partner-branded Visa payment cards. Not only do these third-party banks issue payment cards that support Apple Pay, they also authorize and facilitate financial transactions made using Apple Pay. Upon information and

belief, these same Delaware-based banks have agreements with Defendants regarding the processing and support of financial transactions made through Apple Pay.

39. Upon information and belief, at least the following Apple devices support Apple Pay and infringe one or more claims of the Asserted Patents literally and/or under the doctrine of equivalents: Apple iPhone 7, iPhone 7 Plus, iPhone 6s, iPhone 6s Plus, iPhone 6, iPhone 6 Plus, iPhone SE, iPhone 5, 5s and 5c (paired with Apple Watch), iPad (5th generation), iPad Pro (12.9-inch), iPad pro (9.7-inch), iPad Air 2, iPad mini 4, iPad mini 3, Apple Watch Series 2, Apple Watch Series 1, Apple Watch (1st generation), MacBook Pro with Touch ID, and all Mac models introduced in 2012 or later (with an Apple Pay-enabled iPhone or Apple Watch) (collectively, "Accused Apple Devices"). *See* "Apple Pay is compatible with these devices," *available at* https://support.apple.com/en-us/KM207105. Each of the Accused Apple Devices alone, or in combination with one or more other Apple devices, and the Visa payment processing network, the Visa Token Service, and associated Apple and Visa backend servers and systems supporting Apple Pay transactions (collectively, the "Accused Products"), practices USR's patented technology described and claimed in the Asserted Patents.

40. In short, Defendants have made extensive use of USR's patented technologies, including the technology described and claimed in the Asserted Patents. USR has no choice but to defend its proprietary and patented technology. USR thus requests that this Court award it damages sufficient to compensate for Defendants' infringement of the Asserted Patents, find this case exceptional and award USR its attorneys' fees and costs, and grant an injunction against Defendants to prevent ongoing infringement of the Asserted Patents.

COUNT I: INFRINGEMENT OF U.S. PATENT NO. 8,577,813

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

42. Defendants have directly infringed and are currently directly infringing the '813 patent by making, using, selling, offering for sale, and/or importing into the United States, without authority, products, methods, equipment, and/or services that practice one or more claims of the '813 patent in connection with the Apple Pay service, including but not limited to the Apple iPhone 7, iPhone 7 Plus, iPhone 6s, iPhone 6s Plus, iPhone 6, iPhone 6 Plus, iPhone SE, iPhone 5, 5s and 5c (paired with Apple Watch), Apple Watch Series 2, Apple Watch Series 1, Apple Watch (1st generation), and all other Apple products that support the Apple Pay service for in-store purchases; the Visa payment processing network, Visa Token Service, and other Visa servers and/or systems that process Apple Pay transactions and/or otherwise support the Apple Pay service for in-store purchases; and other Apple and Visa activities, products and/or systems that process Apple Pay transactions and/or otherwise support the Apple Pay service for in-store purchases (collectively, "the '813 Accused Products"). The '813 Accused Products are non-limiting examples that were identified based on publicly available information, and USR reserves the right to identify additional infringing activities, products and services, including, for example, on the basis of information obtained during discovery.

43. 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 '813 patent in connection with an Apple iPhone 7, the Visa payment processing network, and the Visa Token Service. This description is based on publicly available information. USR reserves the right to modify this description, including, for example, on the basis of information about the '813 Accused Products that it obtains during discovery.

1(a) *An electronic ID device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction, comprising:* – Apple and

Visa make, use, sell, offer for sale, and/or import products, servers and services that support the Apple Pay service. As an example, Apple sells the iPhone 7 supporting Apple Pay, and Visa processes Apple Pay transactions using Visa cards and the iPhone 7. *See, e.g.*, "iPhone 7 Tech Specs" ("iPhone 7 Tech Specs"), *available at* http://www.apple.com/iphone-7/specs/ ("Apple Pay - Pay with your iPhone using Touch ID in stores, within apps, and on the web"). The iPhone 7 comprises an electronic ID device that is configured to allow a user to select any one of a plurality of accounts (e.g., credit, debit, prepaid, and store card accounts) associated with the user to employ in a financial transaction (e.g., to pay for a purchase at a store using Apple Pay). For example, the iPhone 7 is configured to maintain up to eight credit, debit, prepaid, and store card accounts as a part of Apple Pay on the iPhone 7. *See, e.g.*, "Set up Apple Pay on your iPhone, iPad, Apple Watch, or Mac" ("Set up Apple Pay"), *available at* https://support.apple.com/en-us/HT204506 ("Get started by adding your credit, debit, or prepaid cards to your iPhone . . . . You can add up to eight cards on any device."). In connection with setting up and using a default or Automatic Selection card and/or selecting a card at the time of purchase, the iPhone 7 is configured to allow a user to select one of multiple accounts to employ as a part of an Apple Pay transaction at a store. *See, e.g.*, "Using Apple Pay in stores, and within apps and websites" ("Using Apple Pay"), *available at* https://support.apple.com/en-us/HT201239 ("**Pay with iPhone** - To use your default card, rest your finger on Touch ID and hold your iPhone within an inch of the contactless reader until you see Done and a checkmark on the display. . . . To switch cards on your iPhone, hold your device near the reader without resting your finger on Touch ID. When your default card appears, tap it, then tap the one that you want to use. Rest your finger on Touch ID to pay. . . . **Use a rewards card** - At participating stores, you can receive or redeem rewards using Apple Pay. Just add your rewards card to Wallet and use it when you pay with Apple Pay.

If you want your rewards card to appear automatically in a store, go to the card, tap [], then turn on Automatic Selection."); "iOS Security Guide" ("iOS Security"), *available at* https://www.apple.com/business/docs/iOS_Security_Guide.pdf, at 34 ("**Wallet:** Wallet is used to add and manage credit, debit, rewards, and store cards and to make payments with Apple Pay."), 38 ("**Contactless payments with Apple Pay -** If iPhone is on and detects an NFC field, it will present the user with the relevant credit, debit, prepaid card, or the default card, which is managed in Settings. The user can also go to the Wallet app and choose a credit or debit card, or when the device is locked, double-click the Home button."); "Apple Pay Available to Millions of Visa Cardholders" ("Apple Pay for Visa Cardholders"), *available at* http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1978656 ("**How to Make a Payment with Apple Pay** - Visa cardholders can make in store purchases . . . by holding the phone in front of a contactless reader and placing their fingertip on the Touch ID to authorize the payment."); "Visa and Apple Opening a New Era of Payments on Mobile Devices" ("Visa and Apple Opening a New Era"), *available at* http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1965351 ("Thanks to a new capability called Visa Token Service, participating financial institutions in the U.S. . . . will be able to add Visa debit and credit cards to Apple Pay, Apple's new payment service, and enable their customers to make easy and secure purchases at select U.S. merchants both in stores and in apps.").

Pictures showing an iPhone allowing a user to select a card account to employ in an Apple Pay transaction are shown below.

1(b) *a biometric sensor configured to receive a biometric input provided by the user; –* The electronic ID device of an iPhone 7 comprises a biometric sensor (e.g., a Touch ID fingerprint sensor) configured to receive a biometric input (e.g., fingerprint data) provided by the user in connection with unlocking the iPhone 7 and/or authorizing an Apple Pay transaction using Touch ID. *See, e.g.*, iPhone 7 Tech Specs ("Touch ID - Fingerprint sensor built into the new Home button"); iOS Security Guide, at 7-8 ("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. . . . 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. . . . The fingerprint sensor is active only when the capacitive steel ring that surrounds the Home button detects the touch of a finger, which triggers the advanced imaging array to scan the finger and send the scan to the Secure Enclave."); Using Apple Pay

("**Pay with iPhone** - To use your default card, rest your finger on Touch ID and hold your iPhone within an inch of the contactless reader until you see Done and a checkmark on the display. . . . To switch cards on your iPhone, hold your device near the reader without resting your finger on Touch ID. When your default card appears, tap it, then tap the one that you want to use. Rest your finger on Touch ID to pay.").

A picture identifying the Touch ID sensor on an iPhone 7 is shown below.

1(c) *a user interface configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts*; – The electronic ID device of an iPhone 7 comprises a user interface configured to receive a user input including secret information known to the user (e.g., a passcode) in connection with unlocking the iPhone 7 and/or authorizing an Apple Pay transaction and, as described above, to receive identifying information concerning an account selected by the user from the plurality of accounts (e.g., a credit, debit, prepaid, and/or store card account to be used as part of an Apple Pay transaction at a store). See 1(a), *supra*; *see also, e.g.*, iPhone 7 Tech Specs ("**Display** . . . Multi-Touch display"); iOS Security Guide, at 7 ("To use Touch ID, users must set up their device so that a passcode is required to unlock it. When Touch ID scans and recognizes an enrolled fingerprint, the device unlocks without asking for the device

passcode. The passcode can always be used instead of Touch ID, and it's still required under the following circumstances . . . ."), 12 ("**Passcodes** . . . iOS supports six-digit, four-digit, and arbitrary-length alphanumeric passcodes. In addition to unlocking the device, a passcode provides entropy for certain encryption keys."), 37 ("**Payment authorization -** On devices that have a Secure Enclave, the Secure Element will only allow a payment to be made after it receives authorization from the Secure Enclave. On iPhone or iPad, this involves confirming the user has authenticated with Touch ID or the device passcode. Touch ID is the default method if available but the passcode can be used at any time instead of Touch ID."); "Apple Pay security and privacy overview" ("Apple Pay Security"), *available at* https://support.apple.com/en-us/HT203027 ("**When you pay using Apple Pay in stores**. . . . To send your payment information, you must authenticate using Touch ID or your passcode.").

A picture identifying the user interface on an iPhone 7 is shown below.

1(d) *a communication interface configured to communicate with a secure registry;* – The electronic ID device of an iPhone 7 comprises a communication interface (e.g., a Near Field Communication (NFC) interface) configured to communicate with a secure registry (e.g., the Visa payment processing network, the Visa Token Service, and/or a payment processing system operated by another payment network and/or card issuer) in connection with an Apple Pay

transaction at a store. *See* 1(a), *supra*; *see also, e.g.*, iPhone 7 Tech Specs ("**Wireless** . . . NFC"); iOS Security Guide, at 34 ("**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."), 35 ("**How Apple Pay uses the NFC controller -** As the gateway to the Secure Element, the NFC controller ensures that all contactless payment transactions are conducted using a point-of-sale terminal that is in close proximity with the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. Once payment is authorized by the card holder using Touch ID or passcode, . . . contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field."), 38 ("**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. . . . These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction."); Apple Pay Security ("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. . . . After you use Touch ID or enter your passcode on iPhone, . . . 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. . . . Before they approve the payment, your bank 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 for Visa Cardholders ("**How to Make a Payment with Apple Pay** - Visa cardholders can make in store purchases . . . by holding the phone in front of a contactless reader and placing their fingertip on the Touch ID to authorize the payment. More than 220,000 merchant locations in the U.S. have installed contactless readers."); "Visa and Apple Opening a New Era ("Thanks to a new capability called Visa Token Service, participating financial institutions in the U.S. . . . will be able to add Visa debit and credit cards to Apple Pay, Apple's new payment service, and enable their customers to make easy and secure purchases at select U.S. merchants both in stores and in apps."); "Visa Token Service Guide" ("Visa Token Service"), *available at* https://developer.visa.com/products/vts/guides ("**Transaction Processing** - Transaction processing is the process of using a token to complete a purchase. The consumer initiates a purchase on a web site, with a mobile phone at a retail store, or within a merchant application. The merchant submits a token and use case-specific dynamic security information (such as a cryptogram) in place of the PAN to its acquirer. The acquirer passes the token and its security information to the payment network as if it were a PAN. Visa detects the token and validates that the circumstances of the transaction are consistent with the domain restrictions defined for the token. If the token is authentic, Visa exchanges it for the corresponding PAN that is securely stored in Visa's Token Vault, and passes both the PAN and the token to the issuer for an authorization decision.").

1(e) *a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface and the communication interface, the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least one of the biometric input and the secret information,* – The electronic ID device of an iPhone 7 comprises a processor (e.g., one or more processors within

the iPhone 7) coupled to the biometric sensor (e.g., the Touch ID sensor) to receive information concerning the biometric input (e.g., fingerprint data), to the user interface, and to the communication interface (e.g., the NFC interface). The processor is programmed to activate the electronic ID device (e.g., such that it may perform an Apple Pay transaction) based on successful authentication by the electronic ID device of at least one of the biometric input (e.g., fingerprint data) and the secret information (e.g., passcode), both of which may be used to authenticate the user in connection with an Apple Pay transaction at a store. *See* 1(b) and 1(c), *supra*; *see also, e.g.*, iPhone 7 Tech Specs ("**Chip** . . . A10 Fusion chip with 64-bit architecture"); iOS Security Guide, at 7 ("**Secure Enclave -** The Secure Enclave is a coprocessor fabricated in the Apple S2, Apple A7, and later A-series processors. . . . 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. . . . To use Touch ID, users must set up their device so that a passcode is required to unlock it. When Touch ID scans and recognizes an enrolled fingerprint, the device unlocks without asking for the device passcode. The passcode can always be used instead of Touch ID, and it's still required under the following circumstances . . . ."), 12 ("**Passcodes** . . . iOS supports six-digit, four-digit, and arbitrary-length alphanumeric passcodes. In addition to unlocking the device, a passcode provides entropy for certain encryption keys."), 34-35 ("**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. . . . **Secure Enclave**: . . . the Secure Enclave manages the authentication process

and enables a payment transaction to proceed. It stores fingerprint data for Touch ID. . . . The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes payment applets certified by the payment networks. . . . During a transaction, the terminal communicates directly with the Secure Element through the Near Field Communication (NFC) controller over a dedicated hardware bus. . . . As the gateway to the Secure Element, the NFC controller ensures that all contactless payment transactions are conducted using a point-of-sale terminal that is in close proximity with the device. . . . Once payment is authorized by the card holder using Touch ID or passcode, . . . contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field."), 37 ("**Payment authorization** - On devices that have a Secure Enclave, the Secure Element will only allow a payment to be made after it receives authorization from the Secure Enclave. On iPhone or iPad, this involves confirming the user has authenticated with Touch ID or the device passcode. Touch ID is the default method if available but the passcode can be used at any time instead of Touch ID. . . . 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. . . . Using the pairing key and its copy of the current AR value, the Secure Element verifies the authorization received from the Secure Enclave before enabling the payment applet for a contactless payment."); Apple Pay Security ("**When you pay using Apple Pay in stores**. . . . To send your payment information, you must authenticate using Touch ID or your passcode.").

A picture showing a processor on the iPhone receiving a biometric input in connection with an Apple Pay transaction is shown below.

1(f) *the processor also being programmed such that once the electronic ID device is activated the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, information associated with at least a portion of the biometric input, and the secret information, and to communicate the encrypted authentication information via the communication interface to the secure registry; and*

– The processor of the electronic ID device of an iPhone 7 is also programmed such that once the electronic ID device is activated following successful authentication of the user, the processor is configured to generate a non-predictable value (e.g., a random number and/or counter) and to generate encrypted authentication information (e.g., a transaction-specific dynamic security code and/or other encrypted payment data) from the non-predictable value, information associated with at least a portion of the biometric input, and the secret information. The processor is also configured to communicate the encrypted authentication information via the communication interface (e.g., the NFC interface) to the secure registry (e.g., the Visa payment processing network, the Visa Token Service, and/or a payment processing system operated by another

payment network and/or card issuer) in connection with an Apple Pay transaction at a store. *See* 1(a)-1(e), *supra*; *see also, e.g.*, iOS Security Guide, at 7 ("To use Touch ID, users must set up their device so that a passcode is required to unlock it. When Touch ID scans and recognizes an enrolled fingerprint, the device unlocks without asking for the device passcode. The passcode can always be used instead of Touch ID, and it's still required under the following circumstances . . . ."), 34-35 ("**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. . . . The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes payment applets certified by the payment networks. . . . During a transaction, the terminal communicates directly with the Secure Element through the Near Field Communication (NFC) controller over a dedicated hardware bus. . . . As the gateway to the Secure Element, the NFC controller ensures that all contactless payment transactions are conducted using a point-of-sale terminal that is in close proximity with the device. . . . Once payment is authorized by the card holder using Touch ID or passcode, . . . contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field."), 37 ("**Payment authorization** - On devices that have a Secure Enclave, the Secure Element will only allow a payment to be made after it receives authorization from the Secure Enclave. On iPhone or iPad, this involves confirming the user has authenticated with Touch ID or the device passcode. Touch ID is the default method if available but the passcode can be used at any time instead of Touch ID. . . . 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. . . . Using the pairing key and its copy of the current AR

value, the Secure Element verifies the authorization received from the Secure Enclave before enabling the payment applet for a contactless payment."), 38 ("**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 . . . . These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction.. . . . Next, the user must authenticate using Touch ID or their passcode before payment information is transmitted. . . . Once the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment."); 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. . . . To send your payment information, you must authenticate using Touch ID or your passcode. . . . After you use Touch ID or enter your passcode on iPhone, . . . 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. . . . Before they approve the payment, your bank 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 for Visa Cardholders ("**How to Make a Payment with Apple Pay** - Visa cardholders can make in store purchases . . . by holding the phone in front of a

contactless reader and placing their fingertip on the Touch ID to authorize the payment. More than 220,000 merchant locations in the U.S. have installed contactless readers."); Visa and Apple Opening a New Era ("Thanks to a new capability called Visa Token Service, participating financial institutions in the U.S. . . . will be able to add Visa debit and credit cards to Apple Pay, Apple's new payment service, and enable their customers to make easy and secure purchases at select U.S. merchants both in stores and in apps."); Visa Token Service ("**Transaction Processing -** Transaction processing is the process of using a token to complete a purchase. The consumer initiates a purchase on a web site, with a mobile phone at a retail store, or within a merchant application. The merchant submits a token and use case-specific dynamic security information (such as a cryptogram) in place of the PAN to its acquirer. The acquirer passes the token and its security information to the payment network as if it were a PAN. Visa detects the token and validates that the circumstances of the transaction are consistent with the domain restrictions defined for the token. If the token is authentic, Visa exchanges it for the corresponding PAN that is securely stored in Visa's Token Vault, and passes both the PAN and the token to the issuer for an authorization decision.").

1(g) *wherein the communication interface is configured to wirelessly transmit the encrypted authentication information to a point-of-sale (POS) device,* – The communication interface (e.g., the NFC interface) of the electronic ID device of an iPhone 7 is configured to wirelessly transmit the encrypted authentication information (e.g., the transaction-specific dynamic security code and/or other encrypted payment data) to a store's point-of-sale (POS) device in connection with an Apple Pay transaction. *See* 1(d)-1(f), *supra*; *see also, e.g.*, iOS Security Guide, at 34-35 ("**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. . . . The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes payment applets certified by the payment networks. . . . During a transaction, the terminal communicates directly with the Secure Element through the Near Field Communication (NFC) controller over a dedicated hardware bus. . . . As the gateway to the Secure Element, the NFC controller ensures that all contactless payment transactions are conducted using a point-of-sale terminal that is in close proximity with the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. . . . Once payment is authorized by the card holder using Touch ID or passcode, . . . contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field."), 38 ("**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. . . . These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction.. . . . Once the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment."); 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. . . . After you use Touch ID or enter your passcode on iPhone, . . . 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."); Apple Pay for Visa Cardholders ("**How to Make a Payment with Apple Pay** - Visa cardholders can make in store purchases . . . by holding the phone in front of a contactless reader and placing their

fingertip on the Touch ID to authorize the payment. More than 220,000 merchant locations in the U.S. have installed contactless readers.").

1(h) *and wherein the secure registry is configured to receive at least a portion of the encrypted authentication information from the POS device.* – The secure registry (e.g., the Visa payment processing network, the Visa Token Service, and/or a payment processing system operated by another payment network and/or card issuer) is configured to receive at least a portion of the encrypted authentication information (e.g., the transaction-specific dynamic security code and/or other encrypted payment data) from the store's POS device in connection with an Apple Pay transaction. *See* 1(d)-1(g), *supra*; *see also, e.g.*, iOS Security Guide, at 34-35 ("Payment transactions are between the user, the merchant, and the card issuer. . . . **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. . . . During a transaction, the terminal communicates directly with the Secure Element through the Near Field Communication (NFC) controller over a dedicated hardware bus. . . . As the gateway to the Secure Element, the NFC controller ensures that all contactless payment transactions are conducted using a point-of-sale terminal that is in close proximity with the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. . . . Once payment is authorized by the card holder using Touch ID or passcode, . . . contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field."), 38 ("**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. . . . These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction.. . . . Once the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment."); Apple Pay Security ("Payment transactions are between you, the merchant, . . . and your bank. . . . **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. . . . After you use Touch ID or enter your passcode on iPhone, . . . 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. . . . Before they approve the payment, your bank 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 for Visa Cardholders ("**How to Make a Payment with Apple Pay** - Visa cardholders can make in store purchases . . . by holding the phone in front of a contactless reader and placing their fingertip on the Touch ID to authorize the payment. More than 220,000 merchant locations in the U.S. have installed contactless readers."); Visa and Apple Opening a New Era ("Thanks to a new capability called Visa Token Service, participating financial institutions in the U.S. . . . will be able to add Visa debit and credit cards to Apple Pay, Apple's new payment service, and enable their customers to make easy and secure purchases at select U.S. merchants both in stores and in apps."); Visa Token Service ("**Transaction Processing -** Transaction processing is the process of using a token to complete a purchase. The consumer initiates a purchase on a web site, with a mobile

phone at a retail store, or within a merchant application. The merchant submits a token and use case-specific dynamic security information (such as a cryptogram) in place of the PAN to its acquirer. The acquirer passes the token and its security information to the payment network as if it were a PAN. Visa detects the token and validates that the circumstances of the transaction are consistent with the domain restrictions defined for the token. If the token is authentic, Visa exchanges it for the corresponding PAN that is securely stored in Visa's Token Vault, and passes both the PAN and the token to the issuer for an authorization decision.").

44. To the extent necessary for direct infringement of any claim of the '813 patent by Apple and/or Visa, Apple and Visa are engaged in a joint enterprise with respect to the Apple Pay service such that the acts of one are attributable to the other. On information and belief, Apple and Visa worked together to develop and implement the Apple Pay service, and they offer Apple Pay to users pursuant to contractual agreement, with a common purpose to "accelerate adoption of mobile payments" using Visa cards together with the Apple Pay service, a shared pecuniary interest in that purpose, and equal control over the direction of the enterprise. *See* "Visa and Apple Opening a New Era of Payments on Mobile Devices," *available at* http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1965351&highlight. According to Visa executive Jim McCarthy, "It was obvious that the Apple environment was going to be the launch partner" for using electronic devices to make touchless mobile payments without transmitting customer account information to and from merchants. *See* "American Express and Visa Love Apple Pay. Will Consumers?" *available at* https://www.bloomberg.com/news/articles/2014-10-23/apple-pay-partners-with-american-express-visa-card-networks. On information and belief, Visa dedicated 1,000 personnel to developing the Apple Pay service. *See* "Banks Did it Apple's Way in Payments by

Mobile," *available at* https://dealbook.nytimes.com/2014/09/11/banks-did-it-apples-way-in-payments-by-mobile/?_r=0.

45. To the extent necessary to direct infringement of any claim of the '813 patent by Apple, Apple is also engaged in a joint enterprise tied to the Apple Pay service with other payment networks, whose acts are attributable to Apple. On information and belief, Apple and other payment networks worked together to develop and implement the Apple Pay service, and they offer Apple Pay to users pursuant to contractual agreement, with a common purpose that their cards be used with the Apple Pay service, a shared pecuniary interest in that purpose, and equal control over the direction of the enterprise. *See* "American Express and Visa Love Apple Pay. Will Consumers?" *available at* https://www.bloomberg.com/news/articles/2014-10-23/apple-pay-partners-with-american-express-visa-card-networks; "Banks Did it Apple's Way in Payments by Mobile," *available at* https://dealbook.nytimes.com/2014/09/11/banks-did-it-apples-way-in-payments-by-mobile/?_r=0.

46. To the extent necessary to direct infringement of any claim of the '813 patent by Apple and/or Visa, the acts of card issuers tied to the Apple Pay service are attributable to Apple and, for transactions involving Visa cards, to Visa. On information and belief, Apple and Visa condition participation in the Apple Pay service (and receipt of revenue and other benefits therefrom) upon performance of claimed steps of '813 patent claims associated with processing Apple Pay transaction requests, and they establish the manner and timing of that performance. *See*, *e.g.*, "Apple Pay participating banks in Canada and the United States," *available at* https://support.apple.com/en-us/HT204916; "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides.

47. To the extent necessary to direct infringement of any claim of the '813 patent by Apple and/or Visa, the acts of end-users of Apple devices tied to the Apple Pay service are attributable to Apple and, for transactions involving Visa cards, to Visa. On information and belief, Apple and Visa condition participation in the Apple Pay service (and receipt of benefits therefrom) upon performance of claimed steps of '813 patent claims associated with processing Apple Pay transaction requests, and they establish the manner and timing of that performance. *See, e.g.*, "Apple Pay," *available at* http://www.apple.com/apple-pay/; "Using Apple Pay in stores, and within apps and websites," *available at* https://support.apple.com/en-us/HT201239; "Apple Pay," *available at* https://usa.visa.com/pay-with-visa/featured-technologies/apple-pay.html.

48. At least as early as the filing and service of this Complaint, Apple is also indirectly infringing the '813 patent.

49. Apple has actual knowledge of USR's rights in the '813 patent and details of Apple's infringement of the '813 patent based on at least the filing and service of this Complaint.

50. Apple manufactures, uses, imports, offers for sale, and/or sells the '813 Accused Products with knowledge of or willful blindness to the fact that its actions will induce Apple's partners and end users to infringe the '813 patent. When used to conduct and/or process an Apple Pay transaction, the '813 Accused Products perform all of the steps of one or more claims of the '813 patent. Apple induces others to infringe the '813 patent in violation of 35 U.S.C. § 271 by encouraging and facilitating others to practice the '813 patent's inventions for performing secure financial transactions. Apple enables others to infringe the '813 patent by incorporating software and hardware supporting Apple Pay into the '813 Accused Products, by publishing information about infringing aspects of its Apple Pay service, and by providing its

partners with software, instruction, and transactional data used to process Apple Pay transactions.

51. Apple actively and knowingly induces end users to infringe the '813 patent by teaching and encouraging end users to use Apple Pay in an infringing manner, with the specific intent to cause the infringing acts. For example, Apple induces users to select and control access to accounts for use in point-of-sale Apple Pay transactions and to generate authentication information in connection with point-of-sale Apple Pay transactions in ways that infringe claims of the '813 patent. Apple's website advertises the Apple Pay service to end users as follows: "Make secure purchases in stores, in apps, and now on the web." *See, e.g.*, "Apple Pay," *available at* http://www.apple.com/apple-pay/. The same site includes an instructional video showing users how to use Apple Pay at a point of sale. *Id.* Another page on Apple's website further explains to users how to use Apple Pay. *See, e.g.*, "Using Apple Pay in stores, and within apps and websites," *available at* https://support.apple.com/en-us/HT201239. When end users used the Apple Pay service to conduct transactions in the manner Apple instructs, they infringe one or more claims of the '813 patent.

52. Apple actively and knowingly induces Visa and other partners to infringe the '813 patent by adding payment cards to Apple devices and sending Apple Pay transaction requests to Visa and other partners' servers for processing, thereby inducing Visa and other partners to process Apple Pay transactions in an infringing manner, with the specific intent to cause the infringing acts. Apple induces Visa and other partners to receive and process authentication information and to control access to user accounts as part of processing Apple Pay transactions in ways that infringe claims of the '813 patent. *See, e.g.*, "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides; "Apple Pay," *available at*

https://usa.visa.com/pay-with-visa/featured-technologies/apple-pay.html; "American Express and Visa Love Apple Pay. Will Consumers?" *available at* https://www.bloomberg.com/news/articles/2014-10-23/apple-pay-partners-with-american-express-visa-card-networks; "Banks Did it Apple's Way in Payments by Mobile," *available at* https://dealbook.nytimes.com/2014/09/11/banks-did-it-apples-way-in-payments-by-mobile/?_r=0.

53. Apple contributes to the infringement of the '813 patent in violation of 35 U.S.C. § 271. Apple knows that infringing components of the '813 Accused Products are especially made or especially adapted for use in the infringement of the '813 patent. The infringing components of these products are not staple articles or commodities of commerce suitable for substantial non-infringing use, and the infringing components of these products are a material part of the invention of the '813 patent. The '813 Accused Products contain infringing components, such as software enabling the use of the Apple Pay service and one or more processors specially configured to generate authentication information and supporting Apple Pay transactions. These hardware and/or software components that Apple provides are separable from Apple's products, a material part of the patented invention, and have no substantial non-infringing use. Accordingly, Apple is also contributing to the direct infringement of the '813 patent by the end users and by Visa.

54. At least as early as the filing and service of this Complaint, Visa is also indirectly infringing the '813 patent.

55. Visa has actual knowledge of USR's rights in the '813 patent and details of Visa's infringement of the '813 patent based on at least the filing and service of this Complaint.

56. Visa manufactures, uses, imports, offers for sale, and/or sells the '813 Accused Products with knowledge of or willful blindness to the fact that its actions will induce Visa's partners and end users to infringe the '813 patent. When used to conduct and/or process an Apple Pay transaction, the '813 Accused Products perform all of the steps of one or more claims of the '813 patent. Visa induces others to infringe the '813 patent in violation of 35 U.S.C. § 271 by encouraging and facilitating others to practice the '813 patent's inventions for performing secure financial transactions. Visa enables others to infringe the '813 patent by enrolling Visa cards in the Apple Pay service, providing the Visa Token service, providing instructions for how to use Apple Pay, and processing Apple Pay transactions.

57. Visa actively and knowingly induces end users to infringe the '813 patent by teaching and encouraging end users to use Apple Pay in an infringing manner, with the specific intent to cause the infringing acts. For example, Visa induces users to select and control access to accounts for use in point-of-sale Apple Pay transactions and to generate authentication information in connection with point-of-sale Apple Pay transactions in ways that infringe claims of the '813 patent. Visa's website advertises the Apple Pay service to end users as follows: "Visa with Apple Pay: a simple, secure way to pay. Learn how to start using your Visa card on Apple Pay today." *See, e.g.*, "Apple Pay," *available at* https://usa.visa.com/pay-with-visa/featured-technologies/apple-pay.html. The same site includes an instructional video and other information showing users how to use Apple Pay. *Id.* When end users use the Apple Pay service to conduct transactions in the manner Visa instructs, they infringe one or more claims of the '813 patent.

58. Visa actively and knowingly induces Apple and other partners to infringe the '813 patent by enrolling Visa cards in the Apple Pay service and processing Apple Pay transaction

requests from Apple devices, thereby enabling Apple's devices to carry out Apple Pay transactions in an infringing manner, with the specific intent to cause the infringing acts. Visa induces Apple to control access to accounts for use in point-of-sale Apple Pay transactions and to generate authentication information in connection with point-of-sale Apple Pay transactions in ways that infringe claims of the '813 patent. Visa also induces other partners to receive and process authentication information and to control access to user accounts as part of processing Apple Pay transactions in ways that infringe claims of the '813 patent. *See, e.g.*, "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides.

59. Visa also contributes to the infringement of the '813 patent in violation of 35 U.S.C. § 271. Visa knows that infringing components of the '813 Accused Products are especially made or especially adapted for use in the infringement of the '813 patent. The infringing components of these products are not staple articles or commodities of commerce suitable for substantial non-infringing use, and the infringing components of these products are a material part of the invention of the '813 patent. Visa provides "a unique digital identifier called a token," which is a 16-digit sequence of numbers formatted just like a payment-card number. *See* "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides. This "token" is used by Apple Pay; Visa also provides components used to generate a transaction-specific dynamic security code used by Apple Pay, and provides programming and/or servers that process Apple Pay transactions. The components Visa provides are separable from the '813 Accused Products, a material part of the patented invention, and have no substantial non-infringing use. Accordingly, Visa is also contributing to the direct infringement of the '813 patent by the end users and by Apple.

60. Defendants' infringement has caused, and is continuing to cause, damage and irreparable injury to USR, and USR will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

61. USR is entitled to injunctive relief and damages in accordance with 35 U.S.C. §§ 271, 281, 283, and 284.

62. This is an exceptional case. USR is entitled to attorneys' fees and costs under 35 U.S.C. § 285 as a result of the infringement of the '813 patent by Defendants.

COUNT II: INFRINGEMENT OF U.S. PATENT NO. 8,856,539

63. USR incorporates by reference and realleges foregoing paragraphs 1-40 of this Complaint as if fully set forth herein.

64. Defendants have directly infringed and are currently directly infringing the '539 patent by making, using, selling, offering for sale, and/or importing into the United States, without authority, products, methods, equipment, and/or services that practice one or more claims of the '539 patent in connection with the Apple Pay service, including but not limited to the Visa payment processing network, Visa Token Service, other Visa servers and/or systems that process Apple Pay transactions and/or otherwise support the Apple Pay service, and other Apple and Visa activities, products and/or systems that process Apple Pay transactions and/or otherwise support the Apple Pay service (collectively, "the '539 Accused Products"). The '539 Accused Products are non-limiting examples that were identified based on publicly available information, and USR reserves the right to identify additional infringing activities, products and services, including, for example, on the basis of information obtained during discovery.

65. As just one non-limiting example, set forth below (with claim language in italics) is a description of infringement of exemplary claim 22 of the '539 patent in connection with the Visa payment processing network and Visa Token Service. This description is based on publicly

available information. USR reserves the right to modify this description, including, for example, on the basis of information about the '539 Accused Products that it obtains during discovery.

22(a) *A method for providing information to a provider to enable transactions between the provider and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code, the method comprising*; – Apple and Visa make, use, sell, offer for sale, and/or import servers and systems that process Apple Pay transactions, and practice a method for providing information to a provider to enable transactions between the provider and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code. As one example, Visa's Token Service (VTS) "replaces sensitive account information, such as the 16-digit primary account number, with a unique digital identifier called a token. The token allows payments to be processed without exposing actual account details that could potentially be compromised. Issuers, merchants, and wallet providers can deliver secure mobile payment applications, gain access to third-party digital payment experiences, or securely maintain cards on file in order to offer their customers safe ways to shop online and with mobile devices.

Visa Token Service provides the payment ecosystem with a flexible and scalable way to securely provision and manage digital credentials (tokens) across remote (e-Commerce and m-Commerce) and mobile contactless form factors. In order for payment tokens to provide improved protection against misuse, the token is limited to use in a specific domain, such as token requester, mobile device, merchant, transaction type, or channel. These capabilities are made available and complemented through a common set of Visa APIs.

The Token Service APIs currently available on Visa Developer provide the tokenization services needed by merchants or wallet providers who want to tokenize their card-

on-file repositories and/or obtain a token for a single online purchase and then use those tokens in standard e-Commerce purchases." *See* "What is the Visa Token Service?," *available at* https://developer.visa.com/products/vts.

The time-varying multicharacter code may include, for example, the token provisioned by VTS and/or a time varying, one-time-use code, or cryptogram: "A consumer enrolls their Visa account with a digital payment service provider (such as an online retailer or mobile wallet) by providing their primary account number (PAN), security code, and other account information. The digital payment service provider requests a payment token from Visa for the enrolled account. Depending on the use case, Visa may share the token request with the issuing bank. With the account issuer's approval, Visa replaces the consumer's PAN with the token. Visa then shares the token with the digital payment service provider for online and mobile (NFC) payment use. A payment token can be limited to a specific mobile device, e-Commerce merchant, or number of purchase transactions before expiring." *See also* "Obtaining Cryptograms," *available at* https://developer.visa.com/products/vts/guides#obtaining _cryptograms ("When a provisioned token is submitted in an e-commerce payment in lieu of a PAN, it must be accompanied by a one-time-use cryptogram called a Token Authentication Verification Value (TAVV). The Get Payment Data With Token API can be used to request a TAVV for use with a specific provisioned token. The TAVV value is generated using the provisioned token and additional transaction data; its calculation and format may vary by use case."). *See* "How Does It Work?," *available at* https://developer.visa.com/products/vts. "For individual e-commerce purchases, you (or your acquirer or payment gateway) will need to request a new TAVV each time the token is used." *See* "Obtaining Cryptograms," *available at* https://developer.visa.com/products/vts/guides.

22(b) *receiving a transaction request including at least the time-varying multicharacter code for an entity on whose behalf a transaction is to take place and an indication of the provider requesting the transaction;* – Visa's payment processing network, which includes the Visa Token Service, receives a transaction request including at least the time-varying multicharacter code for an entity on whose behalf a transaction is to take place and an indication of the provider requesting the transaction. For example, a user of the Apple Pay service passes a token (including the provisioned Device Account Number) along with a transaction-specific dynamic security code (also called a one-time-use cryptogram or Token Authentication Verification Value (TAVV)). *See* "Transaction Processing," *available at* https://developer.visa.com/products/vts/guides ("Transaction processing is the process of using a token to complete a purchase. The consumer initiates a purchase on a web site, with a mobile phone at a retail store, or within a merchant application. The merchant submits a token and use case-specific dynamic security information (such as a cryptogram) in place of the PAN to its acquirer. The acquirer passes the token and its security information to the payment network as if it were a PAN.

Visa detects the token and validates that the circumstances of the transaction are consistent with the domain restrictions defined for the token. If the token is authentic, Visa exchanges it for the corresponding PAN that is securely stored in Visa's Token Vault, and passes both the PAN and the token to the issuer for an authorization decision. The issuer (or its processor) approves or declines the transaction and returns the response to Visa. Visa exchanges the PAN for its token and sends the response with the token back to the acquirer and on to the merchant.")

See also iOS Security Guide, at 38 ("**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 . . . . These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction.. . . . Next, the user must authenticate using Touch ID or their passcode before payment information is transmitted. . . . Once the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment."); Apple Pay Security ("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. . . . After you use Touch ID or enter your passcode on iPhone, . . . 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. . . . Before they approve the payment, your bank 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.").

22(c) *mapping the time-varying multicharacter code to an identity of the entity using the time-varying multicharacter code;* – Visa's payment processing network, which includes the

Visa Token Service, maps the time-varying multicharacter code to an identity of the entity using the time-varying multicharacter code. As an example, the token (including the provisioned Device Account Number) along with a transaction-specific dynamic security code (also called a one-time-use cryptogram or Token Authentication Verification Value (TAVV)) are verified and then used to lookup the personal account number (PAN) associated with the Apple Pay service user using the provisioned token and dynamic security code. *See* "Transaction Processing," *available at* https://developer.visa.com/products/vts/guides ("The acquirer passes the token and its security information to the payment network as if it were a PAN. Visa detects the token and validates that the circumstances of the transaction are consistent with the domain restrictions defined for the token. If the token is authentic, Visa exchanges it for the corresponding PAN that is securely stored in Visa's Token Vault, and passes both the PAN and the token to the issuer for an authorization decision."). *See also* "How Does It Work?," *available at* https://developer.visa.com/products/vts ("Visa Token Vault.... Links tokens to a cardholder's PAN for payment processing"; "Token Transaction Processing: Visa Token Service and VisaNet conduct token-to-PAN mapping, cryptogram validation, domain restriction check and velocity checking (cloud-based payments tokens)"). *See* 22(a)-(b), *supra*.

22(d) *determining compliance with any access restrictions for the provider to secure data of the entity for completing the transaction based at least in part on the indication of the provider and the time-varying multicharacter code of the transaction request;* – Visa's payment processing network, which includes the Visa Token Service, determines compliance with any access restrictions for the provider to secure data of the entity for completing the transaction based at least in part on the indication of the provider and the time-varying multicharacter code of the transaction request. As an example, domain restrictions stored in the Visa Token Vault are

accessed and evaluated to determined compliance. The domain restrictions are provisioned as part of the token containing the Device Account Number and/or the transaction-specific dynamic security code (also called a one-time-use cryptogram or Token Authentication Verification Value (TAVV)). *See* "Token Provisioning," *available at* https://developer.visa.com/products/vts/guides ("A key characteristic of tokens is that they are always accompanied by domain restrictions, a set of rules that define how and when a token can be used for a payment. The domain restrictions vary depending upon the purpose for which the token is being requested. Domain restrictions could limit a token to be used with a specific device, a specific channel (contactless v. e-commerce), or a specific merchant or token requestor. Tokens may be limited to a specific number of transactions, a specific duration (time to live), or a specific transaction amount. A token may need to be accompanied by a cryptogram that must travel to the network with it. These domain restrictions are set as part of the provisioning process and are stored with the token in the Visa Token Vault."); *see also* "Transaction Processing," *available at* https://developer.visa.com/products/vts/guides ("Visa detects the token and validates that the circumstances of the transaction are consistent with the domain restrictions defined for the token. If the token is authentic, Visa exchanges it for the corresponding PAN that is securely stored in Visa's Token Vault, and passes both the PAN and the token to the issuer for an authorization decision. The issuer (or its processor) approves or declines the transaction and returns the response to Visa. Visa exchanges the PAN for its token and sends the response with the token back to the acquirer and on to the merchant."). *See also* "How Does It Work?," *available at* https://developer.visa.com/products/vts ("Token Transaction Processing: Visa Token Service and VisaNet conduct token-to-PAN mapping, cryptogram validation, domain restriction check and velocity checking (cloud-based payments tokens)"). *See* 22(a)-(c), *supra*.

22(e) *accessing information of the entity required to perform the transaction based on the determined compliance with any access restrictions for the provider, the information including account identifying information;* – Visa's payment processing network, which includes the Visa Token Service, accesses information of the entity required to perform the transaction based on the determined compliance with any access restrictions for the provider, the information including account identifying information. As an example, if the domain restrictions are satisfied, one or more of the personal account number (PAN), security code, and other account information is accessed from the Visa Token Vault. *See* "Token Provisioning," *available at* https://developer.visa.com/products/vts ("A consumer enrolls their Visa account with a digital payment service provider (such as an online retailer or mobile wallet) by providing their primary account number (PAN), security code, and other account information. The digital payment service provider requests a payment token from Visa for the enrolled account. Depending on the use case, Visa may share the token request with the issuing bank. With the account issuer's approval, Visa replaces the consumer's PAN with the token. Visa then shares the token with the digital payment service provider for online and mobile (NFC) payment use. A payment token can be limited to a specific mobile device, e-Commerce merchant, or number of purchase transactions before expiring.") *See also* "Token Provisioning," *available at* https://developer.visa.com/products/vts/guides ("A key characteristic of tokens is that they are always accompanied by domain restrictions, a set of rules that define how and when a token can be used for a payment. The domain restrictions vary depending upon the purpose for which the token is being requested. Domain restrictions could limit a token to be used with a specific device, a specific channel (contactless v. e-commerce), or a specific merchant or token requestor. Tokens may be limited to a specific number of transactions, a specific duration (time to live), or

a specific transaction amount. A token may need to be accompanied by a cryptogram that must travel to the network with it. These domain restrictions are set as part of the provisioning process and are stored with the token in the Visa Token Vault."); *see also* "Transaction Processing," *available at* https://developer.visa.com/products/vts/guides ("Visa detects the token and validates that the circumstances of the transaction are consistent with the domain restrictions defined for the token. If the token is authentic, Visa exchanges it for the corresponding PAN that is securely stored in Visa's Token Vault, and passes both the PAN and the token to the issuer for an authorization decision. The issuer (or its processor) approves or declines the transaction and returns the response to Visa. Visa exchanges the PAN for its token and sends the response with the token back to the acquirer and on to the merchant."). *See also* "How Does It Work?," *available at* https://developer.visa.com/products/vts ("Token Transaction Processing: Visa Token Service and VisaNet conduct token-to-PAN mapping, cryptogram validation, domain restriction check and velocity checking (cloud-based payments tokens)"). *See* 22(a)-(d), *supra*.

22(f) *providing the account identifying information to a third party without providing the account identifying information to the provider to enable or deny the transaction;* – Visa's payment processing network, which includes the Visa Token Service, provides the account identifying information to a third party without providing the account identifying information to the provider to enable or deny the transaction. As an example, one or more of the personal account number (PAN), security code, and other account information may be provided to the issuing bank or institution (or in some instances to a processor acting on the back or institution's behalf) in order to approve or decline the transaction. *See* "Transaction Processing," *available at* https://developer.visa.com/products/vts/guides ("Visa detects the token and validates that the circumstances of the transaction are consistent with the domain restrictions defined for the token.

If the token is authentic, Visa exchanges it for the corresponding PAN that is securely stored in Visa's Token Vault, and passes both the PAN and the token to the issuer for an authorization decision. The issuer (or its processor) approves or declines the transaction and returns the response to Visa. Visa exchanges the PAN for its token and sends the response with the token back to the acquirer and on to the merchant."). *See* 22(a)-(e), *supra*.

22(g) *enabling or denying the provider to perform the transaction without the provider's knowledge of the account identifying information* – Visa's payment processing network, which includes the Visa Token Service, enables or denies the provider to perform the transaction without the provider's knowledge of the account identifying information. As one example, Visa sends a response from the issuer (or processor) back to the acquirer and on to the merchant with the token. The response indicates whether the transaction was approved or declined and permits the provider (e.g., a merchant, website, or application that accepts Apple Pay transactions) to perform the transaction without the provider's knowledge of the PAN. *See* "Transaction Processing," *available at* https://developer.visa.com/products/vts/guides ("Visa detects the token and validates that the circumstances of the transaction are consistent with the domain restrictions defined for the token. If the token is authentic, Visa exchanges it for the corresponding PAN that is securely stored in Visa's Token Vault, and passes both the PAN and the token to the issuer for an authorization decision. The issuer (or its processor) approves or declines the transaction and returns the response to Visa. Visa exchanges the PAN for its token and sends the response with the token back to the acquirer and on to the merchant."). *See also* "What is the Visa Token Service?,) *available at* https://developer.visa.com/products/vts ("The Visa Token Service (VTS), a new security technology from Visa, replaces sensitive account information, such as the 16-digit primary account number, with a unique digital identifier called a *token*. The token allows

payments to be processed without exposing actual account details that could potentially be compromised. Issuers, merchants, and wallet providers can deliver secure mobile payment applications, gain access to third-party digital payment experiences, or securely maintain cards on file in order to offer their customers safe ways to shop online and with mobile devices.")

See also "Apple Pay security and privacy overview," *available at* https://support.apple.com/en-us/HT203027 ("Apple doesn't store or have access to the credit, debit, or prepaid card numbers you added to Apple Pay. Apple Pay only stores a portion of your actual card numbers and a portion of your Device Account Numbers, along with a card description, to help you manage your cards…. 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 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.")

See also iOS Security Guide, at 33 ("Full card numbers are not 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.), 34-35 ("Payment

transactions are between the user, the merchant, and the card issuer. . . . **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. . . . During a transaction, the terminal communicates directly with the Secure Element through the Near Field Communication (NFC) controller over a dedicated hardware bus. . . . As the gateway to the Secure Element, the NFC controller ensures that all contactless payment transactions are conducted using a point-of-sale terminal that is in close proximity with the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. . . . Once payment is authorized by the card holder using Touch ID or passcode, . . . contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field."), 38 ("**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. . . . These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction.. . . . Once the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment."); Apple Pay Security ("Payment transactions are between you, the merchant, . . . and your bank. . . . **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. . . . After you use Touch ID or enter your passcode on iPhone, . . . 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. . . . Before they approve the payment, your bank 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 for Visa Cardholders ("**How to Make a Payment with Apple Pay** - Visa cardholders can make in store purchases . . . by holding the phone in front of a contactless reader and placing their fingertip on the Touch ID to authorize the payment. More than 220,000 merchant locations in the U.S. have installed contactless readers."); Visa and Apple Opening a New Era ("Thanks to a new capability called Visa Token Service, participating financial institutions in the U.S. . . . will be able to add Visa debit and credit cards to Apple Pay, Apple's new payment service, and enable their customers to make easy and secure purchases at select U.S. merchants both in stores and in apps."). *See also* 10(a)-10(f), *supra*.

66. To the extent necessary to direct infringement of any claim of the '539 patent by Apple and/or Visa, Apple and Visa are engaged in a joint enterprise with respect to the Apple Pay service such that the acts of one are attributable to the other. On information and belief, Apple and Visa worked together to develop and implement the Apple Pay service, and they offer Apple Pay to users pursuant to contractual agreement, with a common purpose to "accelerate adoption of mobile payments" using Visa cards together with the Apple Pay service, a shared pecuniary interest in that purpose, and equal control over the direction of the enterprise. *See* "Visa and Apple Opening a New Era of Payments on Mobile Devices," *available at* http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1965351&highlight. According to Visa executive Jim McCarthy, "It was obvious that the Apple environment was going to be the launch partner" for using electronic

devices to make touchless mobile payments without transmitting customer account information to and from merchants. *See* "American Express and Visa Love Apple Pay. Will Consumers?" *available at* https://www.bloomberg.com/news/articles/2014-10-23/apple-pay-partners-with-american-express-visa-card-networks. On information and belief, Visa dedicated 1,000 personnel to developing the Apple Pay service. *See* "Banks Did it Apple's Way in Payments by Mobile," *available at* https://dealbook.nytimes.com/2014/09/11/banks-did-it-apples-way-in-payments-by-mobile/?_r=0.

67. To the extent necessary to direct infringement of any claim of the '539 patent by Apple, Apple is also engaged in a joint enterprise tied to the Apple Pay service with other payment networks, whose acts are attributable to Apple. On information and belief, Apple and other payment networks worked together to develop and implement the Apple Pay service, and they offer Apple Pay to users pursuant to contractual agreement, with a common purpose that their cards be used with the Apple Pay service, a shared pecuniary interest in that purpose, and equal control over the direction of the enterprise. *See* "American Express and Visa Love Apple Pay. Will Consumers?" *available at* https://www.bloomberg.com/news/articles/2014-10-23/apple-pay-partners-with-american-express-visa-card-networks; "Banks Did it Apple's Way in Payments by Mobile," *available at* https://dealbook.nytimes.com/2014/09/11/banks-did-it-apples-way-in-payments-by-mobile/?_r=0.

68. To the extent necessary to direct infringement of any claim of the '539 patent by Apple and/or Visa, the acts of card issuers tied to the Apple Pay service are attributable to Apple and, for transactions involving Visa cards, to Visa. On information and belief, Apple and Visa condition participation in the Apple Pay service (and receipt of revenue and other benefits therefrom) upon performance of claimed steps of '539 patent claims associated with processing

Apple Pay transaction requests, and they establish the manner and timing of that performance. *See, e.g.*, "Apple Pay participating banks in Canada and the United States," *available at* https://support.apple.com/en-us/HT204916; "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides.

69. At least as early as the filing and service of this Complaint, Apple is also indirectly infringing the '539 patent.

70. Apple has actual knowledge of USR's rights in the '539 patent and details of Apple's infringement of the '539 patent based on at least the filing and service of this Complaint.

71. Apple manufactures, uses, imports, offers for sale, and/or sells the '539 Accused Products with knowledge of or willful blindness to the fact that its actions will induce Apple's partners and end users to infringe the '539 patent. When used to conduct and/or process an Apple Pay transaction, the '539 Accused Products perform all of the steps of one or more claims of the '539 patent. Apple induces others to infringe the '539 patent in violation of 35 U.S.C. § 271 by encouraging and facilitating others to practice the '539 patent's inventions for performing secure financial transactions. Apple enables others to infringe the '539 patent by incorporating both software and hardware into the '539 Accused Products enabling others to conduct and/or process transactions with Apple Pay, and by publishing information about infringing aspects of its Apple Pay service.

72. Apple actively and knowingly induces Visa and other payment processors and card issuers to infringe the '539 patent by adding payment cards to Apple devices and sending Apple Pay transaction requests and multicharacter codes to their servers for processing, thereby inducing Visa and other partners to process Apple Pay transactions in an infringing manner, with the specific intent to cause the infringing acts. Visa and other partners authenticate users and

provide information to merchants to enable Apple Pay transactions between merchants and users in a manner that infringes claims of the '539 patent. *See, e.g.*, "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides; "Apple Pay," *available at* https://usa.visa.com/pay-with-visa/featured-technologies/apple-pay.html; "American Express and Visa Love Apple Pay. Will Consumers?" *available at* https://www.bloomberg.com/news/articles/2014-10-23/apple-pay-partners-with-american-express-visa-card-networks; "Banks Did it Apple's Way in Payments by Mobile," *available at* https://dealbook.nytimes.com/2014/09/11/banks-did-it-apples-way-in-payments-by-mobile/?_r=0.

73. Apple contributes to the infringement of the '539 patent in violation of 35 U.S.C. § 271. Apple knows that infringing components of the '539 Accused Products are especially made or especially adapted for use in the infringement of the '539 patent. The infringing components of these products are not staple articles or commodities of commerce suitable for substantial non-infringing use, and the infringing components of these products are a material part of the invention of the '539 patent. The '539 Accused Products contain infringing components, such as software enabling the use of the Apple Pay service and one or more processors specially configured to generate transaction requests and multicharacter codes and supporting Apple Pay transactions. These hardware and/or software components that Apple provides are separable from Apple's products, a material part of the patented invention, and have no substantial non-infringing use. Accordingly, Apple is also contributing to the direct infringement of the '539 patent by Visa and other payment processors.

74. At least as early as the filing and service of this Complaint, Visa is also indirectly infringing the '539 patent.

75. Visa has actual knowledge of USR's rights in the '539 patent and details of Visa's infringement of the '539 patent based on at least the filing and service of this Complaint.

76. Visa manufactures, uses, imports, offers for sale, and/or sells the '539 Accused Products with knowledge of or willful blindness to the fact that its actions will induce Visa's partners and end users to infringe the '539 patent. When used to conduct and/or process an Apple Pay transaction, the '539 Accused Products perform all of the steps of one or more claims of the '539 patent. Visa induces others to infringe the '539 patent in violation of 35 U.S.C. § 271 by encouraging and facilitating others to practice the '539 patent's inventions for performing secure financial transactions. Visa enables others to infringe the '539 patent by enrolling Visa cards in the Apple Pay service, providing the Visa Token service, providing instructions for how to use Apple Pay, and processing Apple Pay transactions.

77. Visa actively and knowingly induces Apple and other partners to infringe the '539 patent by enrolling Visa cards in the Apple Pay service and processing Apple Pay transaction requests from Apple devices, thereby enabling Apple devices and servers and other partners' servers to carry out Apple Pay transactions in an infringing manner, with the specific intent to cause the infringing acts. Apple and other partners authenticate users and provide information to merchants to enable Apple Pay transactions between merchants and users (e.g., for purchases within Apps or on websites) in a manner that infringes claims of the '539 patent. *See, e.g.*, "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides.

78. Visa also contributes to the infringement of the '539 patent in violation of 35 U.S.C. § 271. Visa knows that infringing components of the '539 Accused Products are especially made or especially adapted for use in the infringement of the '539 patent. The

infringing components of these products are not staple articles or commodities of commerce suitable for substantial non-infringing use, and the infringing components of these products are a material part of the invention of the '539 patent. Visa provides "a unique digital identifier called a token," which is a 16-digit sequence of numbers formatted just like a payment-card number. *See* "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides. This "token" is used by Apple Pay; Visa also provides components used to generate a transaction-specific dynamic security code used by Apple Pay, and provides programmed servers that process Apple Pay transactions. The components Visa provides are separable from the '539 Accused Products, a material part of the patented invention, and have no substantial non-infringing use. Accordingly, Visa is also contributing to the direct infringement of the '539 patent by Apple.

79. Defendants' infringement has caused, and is continuing to cause, damage and irreparable injury to USR, and USR will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

80. USR is entitled to injunctive relief and damages in accordance with 35 U.S.C. §§ 271, 281, 283, and 284.

81. This is an exceptional case. USR is entitled to attorneys' fees and costs under 35 U.S.C. § 285 as a result of the infringement of the '539 patent by Defendants.

COUNT III: INFRINGEMENT OF U.S. PATENT NO. 9,100,826

82. USR incorporates by reference and realleges foregoing paragraphs 1-40 of this Complaint as if fully set forth herein.

83. Defendants have directly infringed and are currently directly infringing the '826 patent by making, using, selling, offering for sale, and/or importing into the United States, without authority, products, methods, equipment, and/or services that practice one or more

claims of the '826 patent in connection with the Apple Pay service, including but not limited to the iPhone 7, iPhone 7 Plus, iPhone 6s, iPhone 6s Plus, iPhone 6, iPhone 6 Plus, iPhone SE, iPhone 5, 5s and 5c (paired with Apple Watch), iPad (5th generation), iPad Pro (12.9-inch), iPad pro (9.7-inch), iPad Air 2, iPad mini 4, iPad mini 3, Apple Watch Series 2, Apple Watch Series 1, Apple Watch (1st generation), MacBook Pro with Touch ID, all other Mac models introduced in 2012 or later (with an Apple Pay-enabled iPhone or Apple Watch), and all other Apple products that support the Apple Pay service; the Visa payment processing network, Visa Token Service, and other Visa servers and/or systems that process Apple Pay transactions and/or otherwise support the Apple Pay service; and other Apple and Visa activities, products and/or systems that process Apple Pay transactions and/or otherwise support the Apple Pay service (collectively, "the '826 Accused Products"). The '826 Accused Products are non-limiting examples that were identified based on publicly available information, and USR reserves the right to identify additional infringing activities, products and services, including, for example, on the basis of information obtained during discovery.

84. As just one non-limiting example, set forth below (with claim language in italics) is a description of infringement of exemplary claim 10 of the '826 patent in connection with an Apple iPhone 7, the Visa payment processing network, and the Visa Token Service. This description is based on publicly available information. USR reserves the right to modify this description, including, for example, on the basis of information about the '826 Accused Products that it obtains during discovery.

10(a) *A computer implemented method of authenticating an identity of a first entity, comprising acts of;* – Apple and Visa make, use, sell, offer for sale, and/or import products, servers, and systems that support the Apple Pay service and practice a computer implemented

method of authenticating an identity of a first entity when using the Apple Pay service. As an example, Apple sells the iPhone 7, and Visa processes Apple Pay transactions using Visa cards and the iPhone 7. *See, e.g.*, "iPhone 7 Tech Specs" ("iPhone 7 Tech Specs"), *available at* http://www.apple.com/iphone-7/specs/ ("Apple Pay - Pay with your iPhone using Touch ID in stores, within apps, and on the web"). *See also* "Using Apple Pay in stores, and within apps and websites" ("HT201239"), *available at* https://support.apple.com/en-us/HT201239. The identity of a first entity (e.g., an Apple Pay user) is authenticated as described in more detail below.

Defendants Apple and Visa make, use sell, offer for sale, and/or import many devices, components, servers, and systems that also practice a computer implemented method of authenticating an identity of a first entity when supporting and enabling Apple Pay transactions. As an example, and as discussed above, Visa teamed with Apple in September 2014 to incorporate a mobile wallet feature into Apple's iPhone models, enabling users to more readily use their Visa cards with the Apple Pay service. Since 2014, Apple's backend servers and Visa's payment processing network, VisaNet, including Visa's Token Service, have supported and processed transactions made using Apple Pay, including billions of Apple Pay transactions made in the United States. Each transaction carried out using Apple's backend servers and Visa's payment processing network performs a computer implemented method of authenticating an identity of a first entity. *See* "Shaping the future of mobile payments," *available at* https://usa.visa.com/partner-with-us/payment-technology/apple-pay.html ("Visa Token Service helps secure Apple Pay by replacing credit card numbers with a digital account identifier that is stored securely on users' devices."). *See also* "Apple Pay Available to Millions of Visa Cardholders" ("Apple Pay for Visa Cardholders"), *available at* http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1978656

("**How to Make a Payment with Apple Pay** - Visa cardholders can make in store purchases . . . by holding the phone in front of a contactless reader and placing their fingertip on the Touch ID to authorize the payment. More than 220,000 merchant locations in the U.S. have installed contactless readers."); "Visa and Apple Opening a New Era of Payments on Mobile Devices" ("Visa and Apple Opening a New Era"), *available at* http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1965351 ("Thanks to a new capability called Visa Token Service, participating financial institutions in the U.S. . . . will be able to add Visa debit and credit cards to Apple Pay, Apple's new payment service, and enable their customers to make easy and secure purchases at select U.S. merchants both in stores and in apps.").

A flow chart showing the steps in a typical Apple Pay transaction flow is shown below.

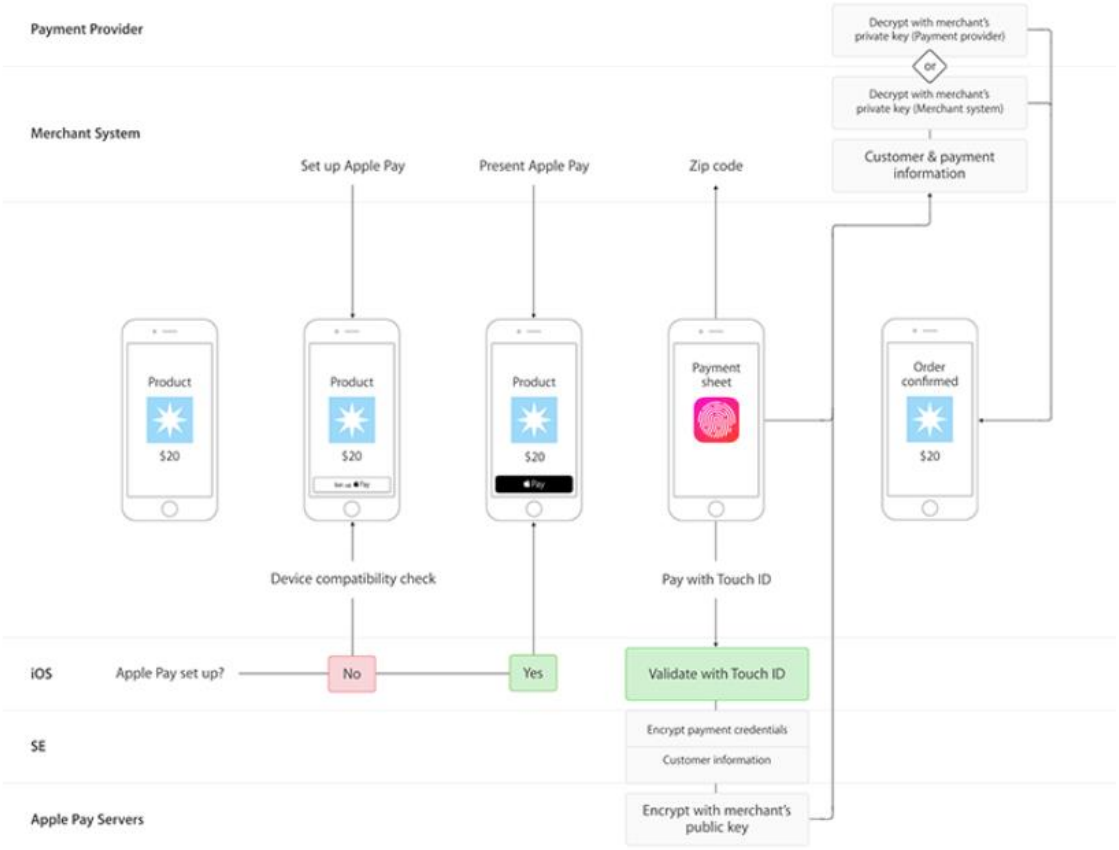


Figure 2: Payment Flow

See "Getting Started with Apple Pay," *available at* https://developer.apple.com/apple-pay/get-started/. Both Apple Pay servers and the payment provider act in concert to authenticate an identity of a first entity when using the Apple Pay service.

10(b) *authenticating, with a first handheld device, a user of the first handheld device as the first entity based on authentication information;* – Apple's iPhone 7 authenticates a user of the first handheld device as the first entity based on authentication information, which can include fingerprint data and/or a passcode. *See, e.g.*, iPhone 7 Tech Specs ("Touch ID - Fingerprint sensor built into the new Home button"); iOS Security Guide, at 7-8 ("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. . . . 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. . . . The fingerprint sensor is active only when the capacitive steel ring that surrounds the Home button detects the touch of a finger, which triggers the advanced imaging array to scan the finger and send the scan to the Secure Enclave."); Using Apple Pay ("**Pay with iPhone** - To use your default card, rest your finger on Touch ID and hold your iPhone within an inch of the contactless reader until you see Done and a checkmark on the display. . . . To switch cards on your iPhone, hold your device near the reader without resting your finger on Touch ID. When your default card appears, tap it, then tap the one that you want to use. Rest your finger on Touch ID to pay.").

A picture identifying the Touch ID sensor used to authenticate a user of an iPhone 7 is shown below.

See also iOS Security Guide, at 7 ("To use Touch ID, users must set up their device so that a passcode is required to unlock it. When Touch ID scans and recognizes an enrolled fingerprint, the device unlocks without asking for the device passcode. The passcode can always be used instead of Touch ID, and it's still required under the following circumstances . . . ."), 12

("**Passcodes** . . . iOS supports six-digit, four-digit, and arbitrary-length alphanumeric passcodes. In addition to unlocking the device, a passcode provides entropy for certain encryption keys."), 37 ("**Payment authorization -** On devices that have a Secure Enclave, the Secure Element will only allow a payment to be made after it receives authorization from the Secure Enclave. On iPhone or iPad, this involves confirming the user has authenticated with Touch ID or the device passcode. Touch ID is the default method if available but the passcode can be used at any time instead of Touch ID."); "Apple Pay security and privacy overview" ("Apple Pay Security"), *available at* https://support.apple.com/en-us/HT203027 ("**When you pay using Apple Pay in stores**. . . . To send your payment information, you must authenticate using Touch ID or your passcode.").

10(c) *retrieving or receiving first biometric* information *of the user of the first handheld device;* – As described above, the iPhone 7 includes a fingerprint sensing system known as Touch ID that retrieving or receiving biometric information (e.g., fingerprint data) of the user of the first handheld device. *See* 1(a)-(b), *supra*.

10(d) *determining a first authentication information from the first biometric information;* – The Secure Element and/or Secure Enclave within the iPhone 7 determines first authentication information (for example, in the form of a Device Account Number and/or a transaction-specific dynamic security code) from the biometric information. *See* "Apple Pay security and privacy overview," *available at* https://support.apple.com/en-us/HT203027 ("To send your payment information, you must authenticate using Touch ID or your passcode. No payment information is sent without your authentication…. 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 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."). *See also* iOS Security Guide, at 34 ("**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."), 35 ("**How Apple Pay uses the NFC controller -** As the gateway to the Secure Element, the NFC controller ensures that all contactless payment transactions are conducted using a point-of-sale terminal that is in close proximity with the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. Once payment is authorized by the card holder using Touch ID or passcode, . . . contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field."), 38 ("**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 . . . . These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction.. . . . Next, the user must authenticate using Touch ID or their passcode before payment information is transmitted. . . . Once the user authenticates, the Device Account

Number and a transaction-specific dynamic security code are used when processing the payment."); Apple Pay Security ("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. . . . After you use Touch ID or enter your passcode on iPhone, . . . 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. . . . Before they approve the payment, your bank 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.").

10(e) *receiving with a second device, the first authentication information of the first entity wirelessly transmitted from the first handheld device;* – The iPhone 7 wirelessly transmits (for example, using Near Field Communication (NFC), Wi-Fi, Bluetooth, and/or a Cellular Network transceiver) the authentication information to one or more servers or systems associated with the Visa payment processing network (sometimes via an intermediary POS terminal), which receive the authentication information. *See* iOS Security Guide, at 34 ("**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."), 35 ("**How Apple Pay uses the NFC controller -** As the gateway to the Secure Element, the NFC controller ensures that all contactless payment transactions are conducted using a point-of-sale terminal that is in close proximity with the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless

transactions. Once payment is authorized by the card holder using Touch ID or passcode, . . . contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field."), 38 ("**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 . . . . These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction.. . . . Next, the user must authenticate using Touch ID or their passcode before payment information is transmitted. . . . Once the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment."); Apple Pay Security ("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. . . . After you use Touch ID or enter your passcode on iPhone, . . . 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. . . . Before they approve the payment, your bank 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 for Visa Cardholders ("**How to**

Make a Payment with Apple Pay - Visa cardholders can make in store purchases . . . by holding the phone in front of a contactless reader and placing their fingertip on the Touch ID to authorize the payment. More than 220,000 merchant locations in the U.S. have installed contactless readers."); Visa and Apple Opening a New Era ("Thanks to a new capability called Visa Token Service, participating financial institutions in the U.S. . . . will be able to add Visa debit and credit cards to Apple Pay, Apple's new payment service, and enable their customers to make easy and secure purchases at select U.S. merchants both in stores and in apps.").

10(f) *retrieving or receiving respective second authentication information for the user of the first handheld device;* – One or more Visa and/or Apple backend servers or systems associated with the Visa payment processing network retrieve or receive respective second authentication information (the other one of a Device Account Number and/or a transaction-specific dynamic security code) for the user of the first handheld device. *See* 10(a)-(e), *supra*. As another example, token information (and their domain restrictions) are retrieved from a "secure digital vault" within Visa's Token Vault (a part of Visa Token Services). *See* "Visa Token Service," *available at* https://usa.visa.com/partner-with-us/payment-technology/visa-token-service.html. *See also* Apple Pay for Visa Cardholders ("**How to Make a Payment with Apple Pay** - Visa cardholders can make in store purchases . . . by holding the phone in front of a contactless reader and placing their fingertip on the Touch ID to authorize the payment. More than 220,000 merchant locations in the U.S. have installed contactless readers."); Visa and Apple Opening a New Era ("Thanks to a new capability called Visa Token Service, participating financial institutions in the U.S. . . . will be able to add Visa debit and credit cards to Apple Pay, Apple's new payment service, and enable their customers to make easy and secure purchases at select U.S. merchants both in stores and in apps.").

The second authentication information may alternatively or additionally take the form of domain restrictions associated with the token provisioned by Visa's Token Services. For example, a domain restriction used with Apple Pay transaction includes a domain restrictions "limit[ing] a token to be used with a specific device." The second authentication information could therefore also constitute a device identifier used to enforce a token's domain restrictions. *See* "Getting Started With Visa Token Services," *available at* https://developer.visa.com/products/vts/guides ("Token provisioning is the process of requesting that Visa issue a token for a specific PAN and for a specific purpose, domain, or device. The same PAN may have multiple tokens provisioned to it from the same or different token requestors. To obtain a token, the token requestor submits a token provisioning request to the Visa Token Service, which then performs an eligibility check using decision rules defined by the card issuer when provisioning tokens on their behalf. If the PAN is eligible, the Visa Token Service generates a new payment token and provisions it to the token requestor. Visa may optionally send a notification to the issuer to advise them that the token provisioning was successful. A key characteristic of tokens is that they are always accompanied by domain restrictions, a set of rules that define how and when a token can be used for a payment. The domain restrictions vary depending upon the purpose for which the token is being requested. Domain restrictions could limit a token to be used with a specific device, a specific channel (contactless v. e-commerce), or a specific merchant or token requestor. Tokens may be limited to a specific number of transactions, a specific duration (time to live), or a specific transaction amount. A token may need to be accompanied by a cryptogram that must travel to the network with it. These domain restrictions are set as part of the provisioning process and are stored with the token in the Visa Token Vault.").

10(g) *authenticating the identity of the first entity based upon the first authentication information and the second authentication information* – One or more Visa and/or Apple backend servers or systems associated with the Visa payment processing network authenticate the identity of the first entity based upon the first authentication information and the second authentication information. As one example, Visa's Token Services validates at least the received Device Account Number and/or a transaction-specific dynamic security code in order to authenticate the identity of the Apple Pay user. Domain restrictions (for example limiting use of the token to a specific mobile device) are also validated. *See* "Getting Started With Visa Token Services," *available at* https://developer.visa.com/products/vts/guides ("Transaction processing is the process of using a token to complete a purchase. The consumer initiates a purchase on a web site, with a mobile phone at a retail store, or within a merchant application. The merchant submits a token and use case-specific dynamic security information (such as a cryptogram) in place of the PAN to its acquirer. The acquirer passes the token and its security information to the payment network as if it were a PAN. Visa detects the token and validates that the circumstances of the transaction are consistent with the domain restrictions defined for the token. If the token is authentic, Visa exchanges it for the corresponding PAN that is securely stored in Visa's Token Vault, and passes both the PAN and the token to the issuer for an authorization decision. The issuer (or its processor) approves or declines the transaction and returns the response to Visa. Visa exchanges the PAN for its token and sends the response with the token back to the acquirer and on to the merchant."); *See also* iOS Security Guide, at 34-35 ("Payment transactions are between the user, the merchant, and the card issuer. . . . **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. . . . During a transaction, the terminal communicates directly with the Secure Element through the Near Field Communication (NFC) controller over a dedicated hardware bus. . . . As the gateway to the Secure Element, the NFC controller ensures that all contactless payment transactions are conducted using a point-of-sale terminal that is in close proximity with the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. . . . Once payment is authorized by the card holder using Touch ID or passcode, . . . contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field."), 38 ("**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. . . . These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction.. . . . Once the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment."); Apple Pay Security ("Payment transactions are between you, the merchant, . . . and your bank. . . . **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. . . . After you use Touch ID or enter your passcode on iPhone, . . . 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. . . . Before they approve the payment, your bank 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 for Visa Cardholders ("**How to Make a Payment with Apple Pay** - Visa cardholders can make in store purchases . . . by holding the phone in front of a contactless reader and placing their fingertip on the Touch ID to authorize the payment. More than 220,000 merchant locations in the U.S. have installed contactless readers."); Visa and Apple Opening a New Era ("Thanks to a new capability called Visa Token Service, participating financial institutions in the U.S. . . . will be able to add Visa debit and credit cards to Apple Pay, Apple's new payment service, and enable their customers to make easy and secure purchases at select U.S. merchants both in stores and in apps."). *See also* 10(a)-10(f), *supra*.

After authentication, Visa's Token Services also "[l]ink[s] tokens to a cardholder's PAN for payment processing" and completes the transaction. *See* "Visa Token Service," *available at* https://usa.visa.com/partner-with-us/payment-technology/visa-token-service.html. *See also* "Getting Started With Visa Token Services," *available at* https://developer.visa.com/products/vts/guides ("Transaction processing is the process of using a token to complete a purchase. The consumer initiates a purchase on a web site, with a mobile phone at a retail store, or within a merchant application. The merchant submits a token and use case-specific dynamic security information (such as a cryptogram) in place of the PAN to its acquirer. The acquirer passes the token and its security information to the payment network as if it were a PAN. Visa detects the token and validates that the circumstances of the transaction are consistent with the domain restrictions defined for the token. If the token is authentic, Visa exchanges it for the corresponding PAN that is securely stored in Visa's Token Vault, and passes both the PAN and the token to the issuer for an authorization decision. The issuer (or its processor) approves or declines the transaction and returns the response to Visa. Visa exchanges

the PAN for its token and sends the response with the token back to the acquirer and on to the merchant.").

85. To the extent necessary to direct infringement of any claim of the '826 patent by Apple and/or Visa, Apple and Visa are engaged in a joint enterprise with respect to the Apple Pay service such that the acts of one are attributable to the other. On information and belief, Apple and Visa worked together to develop and implement the Apple Pay service, and they offer Apple Pay to users pursuant to contractual agreement, with a common purpose to "accelerate adoption of mobile payments" using Visa cards together with the Apple Pay service, a shared pecuniary interest in that purpose, and shared control over the direction of the enterprise. *See* "Visa and Apple Opening a New Era of Payments on Mobile Devices," *available at* http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1965351&highlight. According to Visa executive Jim McCarthy, "It was obvious that the Apple environment was going to be the launch partner" for using electronic devices to make touchless mobile payments without transmitting customer account information to and from merchants. *See* "American Express and Visa Love Apple Pay. Will Consumers?" *available at* https://www.bloomberg.com/news/articles/2014-10-23/apple-pay-partners-with-american-express-visa-card-networks. On information and belief, Visa dedicated 1,000 personnel to developing the Apple Pay service. *See* "Banks Did it Apple's Way in Payments by Mobile," *available at* https://dealbook.nytimes.com/2014/09/11/banks-did-it-apples-way-in-payments-by-mobile/?_r=0.

86. To the extent necessary to direct infringement of any claim of the '826 patent by Apple, Apple is also engaged in a joint enterprise tied to the Apple Pay service with other payment networks, whose acts are attributable to Apple. On information and belief, Apple and

other payment networks worked together to develop and implement the Apple Pay service, and they offer Apple Pay to users pursuant to contractual agreement, with a common purpose that their cards be used with the Apple Pay service, a shared pecuniary interest in that purpose, and shared control over the direction of the enterprise. *See* "American Express and Visa Love Apple Pay. Will Consumers?" *available at* https://www.bloomberg.com/news/articles/2014-10-23/apple-pay-partners-with-american-express-visa-card-networks; "Banks Did it Apple's Way in Payments by Mobile," *available at* https://dealbook.nytimes.com/2014/09/11/banks-did-it-apples-way-in-payments-by-mobile/?_r=0.

87. To the extent necessary to direct infringement of any claim of the '826 patent by Apple and/or Visa, the acts of card issuers tied to the Apple Pay service are attributable to Apple and, for transactions involving Visa cards, to Visa. On information and belief, Apple and Visa condition participation in the Apple Pay service (and receipt of revenue resulting therefrom) upon performance of claimed steps of '826 patent claims associated with processing Apple Pay transaction requests, and they establish the manner and timing of that performance. *See, e.g.*, "Apple Pay participating banks in Canada and the United States," *available at* https://support.apple.com/en-us/HT204916; "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides.

88. To the extent necessary to direct infringement of any claim of the '826 patent by Apple and/or Visa, the acts of end-users of Apple devices tied to the Apple Pay service are attributable to Apple and, for transactions involving Visa cards, to Visa. On information and belief, Apple and Visa condition participation in the Apple Pay service (and receipt of benefits therefrom) upon performance of claimed steps of '826 patent claims associated with processing Apple Pay transaction requests, and they establish the manner and timing of that performance.

See, e.g., "Apple Pay," *available at* http://www.apple.com/apple-pay/; "Using Apple Pay in stores, and within apps and websites," *available at* https://support.apple.com/en-us/HT201239; "Apple Pay," *available at* https://usa.visa.com/pay-with-visa/featured-technologies/apple-pay.html.

89. At least as early as the filing and service of this Complaint, Apple is also indirectly infringing the '826 patent.

90. Apple has actual knowledge of USR's rights in the '826 patent and details of Apple's infringement of the '826 patent based on at least the filing and service of this Complaint.

91. Apple manufactures, uses, imports, offers for sale, and/or sells the '826 Accused Products with knowledge of or willful blindness to the fact that its actions will induce Apple's partners and end users to infringe the '826 patent. When used to conduct and/or process an Apple Pay transaction, the '826 Accused Products perform all of the steps of one or more claims of the '826 patent. Apple induces others to infringe the '826 patent in violation of 35 U.S.C. § 271 by encouraging and facilitating others to practice the '826 patent's inventions for performing secure financial transactions. Apple enables others to infringe the '826 patent by incorporating both software and hardware into the '826 Accused Products enabling others to conduct and/or process transactions with Apple Pay, and by publishing information about infringing aspects of its Apple Pay service.

92. Apple actively and knowingly induces end users to infringe the '826 patent by teaching and encouraging end users to use Apple Pay in an infringing manner, with the specific intent to cause the infringing acts. For example, Apple induces end users to authenticate their identities in connection with Apple Pay transactions in ways that infringe claims of the '826 patent. Apple's website advertises the Apple Pay service to end users as follows: "Make secure

purchases in stores, in apps, and now on the web." *See, e.g.*, "Apple Pay," *available at* http://www.apple.com/apple-pay/. The same site includes an instructional video showing users how to use Apple Pay at a point of sale. *Id.* Another page on Apple's website further explains to users how to use Apple Pay. *See, e.g.*, "Using Apple Pay in stores, and within apps and websites," *available at* https://support.apple.com/en-us/HT201239. When end users used the Apple Pay service to conduct transactions in the manner Apple instructs, they infringe one or more claims of the '826 patent.

93. Apple actively and knowingly induces Visa and other partners to infringe the '826 patent by adding payments cards to Apple devices and sending Apple Pay transaction requests to Visa and other partners' servers for processing, thereby inducing Visa and other partners to process Apple Pay transactions in an infringing manner, with the specific intent to cause the infringing acts. Apple induces Visa and other partners to authenticate the identities of users in connection with Apple Pay transactions in ways that infringe claims of the '826 patent. *See, e.g.*, "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides; "Apple Pay," *available at* https://usa.visa.com/pay-with-visa/featured-technologies/apple-pay.html; "American Express and Visa Love Apple Pay. Will Consumers?" *available at* https://www.bloomberg.com/news/articles/2014-10-23/apple-pay-partners-with-american-express-visa-card-networks; "Banks Did it Apple's Way in Payments by Mobile," *available at* https://dealbook.nytimes.com/2014/09/11/banks-did-it-apples-way-in-payments-by-mobile/?_r=0.

94. Apple contributes to the infringement of the '826 patent in violation of 35 U.S.C. § 271. Apple knows that infringing components of the '826 Accused Products are especially

made or especially adapted for use in the infringement of the '826 patent. The infringing components of these products are not staple articles or commodities of commerce suitable for substantial non-infringing use, and the infringing components of these products are a material part of the invention of the '826 patent. The '826 Accused Products contain infringing components, such as software enabling the use of the Apple Pay service and one or more processors specially configured to generate authentication information and supporting Apple Pay transactions. These hardware and/or software components that Apple provides are separable from Apple's products, a material part of the patented invention, and have no substantial non-infringing use. Accordingly, Apple is also contributing to the direct infringement of the '826 patent by the end users and by Visa.

95. At least as early as the filing and service of this Complaint, Visa is also indirectly infringing the '826 patent.

96. Visa has actual knowledge of USR's rights in the '826 patent and details of Apple's infringement of the '826 patent based on at least the filing and service of this Complaint.

97. Visa manufactures, uses, imports, offers for sale, and/or sells the '826 Accused Products with knowledge of or willful blindness to the fact that its actions will induce Visa's partners and end users to infringe the '826 patent. When used to conduct and/or process an Apple Pay transaction, the '826 Accused Products perform all of the steps of one or more claims of the '826 patent. Visa induces others to infringe the '826 patent in violation of 35 U.S.C. § 271 by encouraging and facilitating others to practice the '826 patent's inventions for performing secure financial transactions. Visa enables others to infringe the '826 patent by enrolling Visa cards in the Apple Pay service, providing the Visa Token service, providing instructions for how to use Apple Pay, and processing Apple Pay transactions.

98. Visa actively and knowingly induces end users to infringe the '826 patent by teaching and encouraging end users to use Apple Pay in an infringing manner, with the specific intent to cause the infringing acts. For example, Visa induces end users to authenticate their identities in connection with Apple Pay transactions in ways that infringe claims of the '826 patent. Visa's website advertises the Apple Pay service to end users as follows: "Visa with Apple Pay: a simple, secure way to pay. Learn how to start using your Visa card on Apple Pay today." *See, e.g.*, "Apple Pay," *available at* https://usa.visa.com/pay-with-visa/featured-technologies/apple-pay.html. The same site includes written information and an instructional video showing users how to use Apple Pay at a point of sale. *Id.* When end users used the Apple Pay service to conduct transactions in the manner Visa instructs, they infringe one or more claims of the '826 patent.

99. Visa actively and knowingly induces Apple and other partners to infringe the '826 patent by enrolling Visa cards in the Apple Pay service and processing Apple Pay transaction requests from Apple devices, thereby enabling Apple's devices and servers and other partners' servers to carry out Apple Pay transactions in an infringing manner, with the specific intent to cause the infringing acts. Visa induces Apple and other partners to authenticate the identities of users in connection with Apple Pay transactions in ways that infringe claims of the '826 patent. *See, e.g.*, "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides.

100. Visa also contributes to the infringement of the '826 patent in violation of 35 U.S.C. § 271. Visa knows that infringing components of the '826 Accused Products are especially made or especially adapted for use in the infringement of the '826 patent. The infringing components of these products are not staple articles or commodities of commerce

suitable for substantial non-infringing use, and the infringing components of these products are a material part of the invention of the '826 patent. Visa provides "a unique digital identifier called a token," which is a 16-digit sequence of numbers formatted just like a payment-card number. *See* "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides. This "token" is used by Apple Pay; Visa also provides components used to generate a transaction-specific dynamic security code used by Apple Pay, and provides programmed servers that process Apple Pay transactions. The components Visa provides are separable from the '826 Accused Products, a material part of the patented invention, and have no substantial non-infringing use. Accordingly, Visa is also contributing to the direct infringement of the '826 patent by the end users and by Apple.

101. Defendants' infringement has caused, and is continuing to cause, damage and irreparable injury to USR, and USR will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

102. USR is entitled to injunctive relief and damages in accordance with 35 U.S.C. §§ 271, 281, 283, and 284.

103. This is an exceptional case. USR is entitled to attorneys' fees and costs under 35 U.S.C. § 285 as a result of the infringement of the '826 patent by Defendants.

COUNT IV: INFRINGEMENT OF U.S. PATENT NO. 9,530,137

104. USR incorporates by reference and realleges foregoing paragraphs 1-40 of this Complaint as if fully set forth herein.

105. Defendants have directly infringed and are currently directly infringing the '137 patent by making, using, selling, offering for sale, and/or importing into the United States, without authority, products, methods, equipment, and/or services that practice one or more claims of the '137 patent in connection with the Apple Pay service, including but not limited to

the iPhone 7, iPhone 7 Plus, iPhone 6s, iPhone 6s Plus, iPhone 6, iPhone 6 Plus, iPhone SE, iPhone 5, 5s and 5c (paired with Apple Watch), iPad (5th generation), iPad Pro (12.9-inch), iPad pro (9.7-inch), iPad Air 2, iPad mini 4, iPad mini 3, Apple Watch Series 2, Apple Watch Series 1, Apple Watch (1st generation), MacBook Pro with Touch ID, all other Mac models introduced in 2012 or later (with an Apple Pay-enabled iPhone or Apple Watch), and all other Apple products that support the Apple Pay service; the Visa payment processing network, Visa Token Service, and other Visa servers and/or systems that process Apple Pay transactions and/or otherwise support the Apple Pay service; and other Apple and Visa activities, products and/or systems that process Apple Pay transactions and/or otherwise support the Apple Pay service (collectively, "the '137 Accused Products"). The '137 Accused Products are non-limiting examples that were identified based on publicly available information, and USR reserves the right to identify additional infringing activities, products and services, including, for example, on the basis of information obtained during discovery.

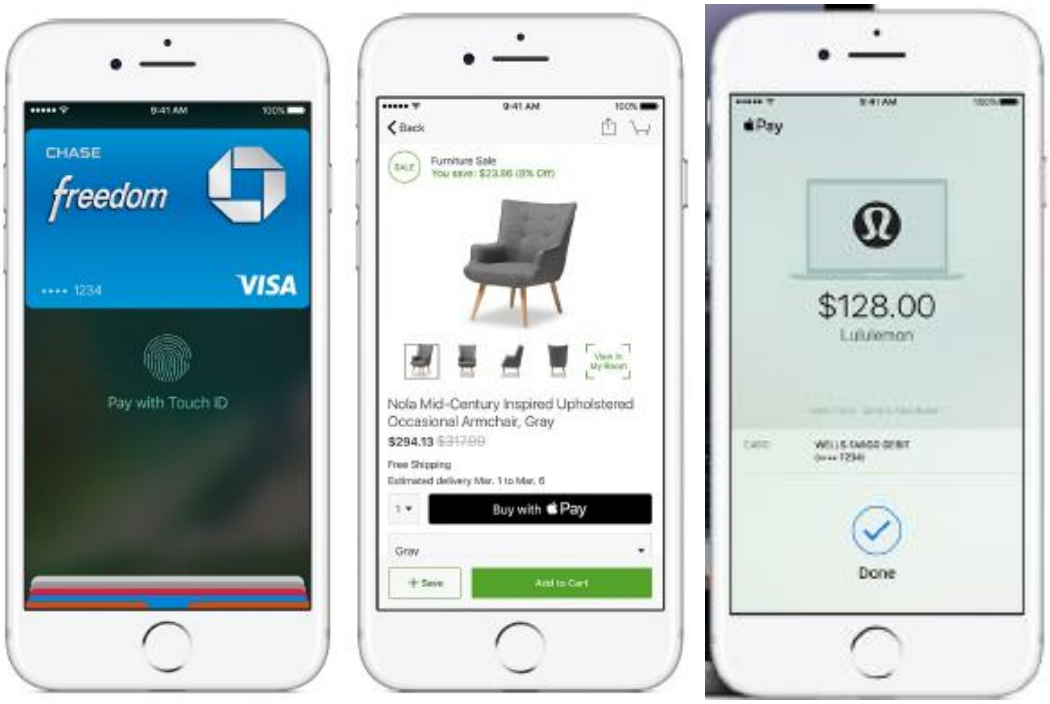
106. As just one non-limiting example, set forth below (with claim language in italics) is a description of infringement of exemplary claim 12 of the '137 patent in connection with an Apple iPhone 7, the Visa payment network, and the Visa token service. This description is based on publicly available information. USR reserves the right to modify this description, including, for example, on the basis of information about the '137 Accused Products that it obtains during discovery.

12(a) *A system for authenticating a user for enabling a transaction, the system comprising:* – Apple and Visa make, use, sell, offer for sale, and/or import products, servers, and systems that support the Apple Pay service. As an example, Apple sells the iPhone 7, and Visa processes Apple Pay transactions using Visa cards and the iPhone 7. The iPhone 7 comprises a

system for authenticating a user (e.g., via Touch ID) for enabling a transaction (e.g., to allow a user to use Apple Pay to make a payment in a store, within an App, or on a website). *See, e.g.*, "iPhone 7 Tech Specs" ("iPhone 7 Tech Specs"), *available at* http://www.apple.com/iphone-7/specs/ ("Apple Pay - Pay with your iPhone using Touch ID in stores, within apps, and on the web"); *See, e.g.*, "Using Apple Pay in stores, and within apps and websites" ("Using Apple Pay"), *available at* https://support.apple.com/en-us/HT201239 ("**Pay in stores** - With your iPhone or Apple Watch, you can pay in stores that accept contactless payments.. . . . To use your default card, rest your finger on Touch ID and hold your iPhone within an inch of the contactless reader until you see Done and a checkmark on the display. . . . **Pay within apps** - With your iPhone, iPad, and Apple Watch you can use Apple Pay to pay within apps when you see Apple Pay as a payment option. . . . On your iPhone or iPad, place your finger on Touch ID. . . . When your payment is successful, you'll see Done and a checkmark on the screen. . . . **Pay on websites in Safari -** With your iPhone, iPad, and Mac you can use Apple Pay to pay on websites in Safari. . . . When you're ready, make your purchase and place your finger on Touch ID. When your payment is successful, you'll see Done and a checkmark on the screen."); "iOS Security Guide" ("iOS Security"), *available at* https://www.apple.com/business/docs/iOS_Security_Guide.pdf, at 37 ("**Payment authorization** - On devices that have a Secure Enclave, the Secure Element will only allow a payment to be made after it receives authorization from the Secure Enclave. On iPhone or iPad, this involves confirming the user has authenticated with Touch ID or the device passcode."); "Apple Pay security and privacy overview" ("Apple Pay Security"), *available at* https://support.apple.com/en-us/HT203027 ("To send your payment information, you must authenticate using Touch ID or your passcode. No payment information is sent without your authentication."); "Getting Started with Apple Pay" ("Getting Started"), *available at*

https://developer.apple.com/apple-pay/get-started/ ("Apple Pay provides an easy and secure way for users to buy goods and services in your iOS app, watchOS app, or on your website. . . . Within your app or website, users can authorize payments using Touch ID . . . ."); "Apple Pay Available to Millions of Visa Cardholders" ("Apple Pay for Visa Cardholders"), *available at* http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1978656 ("**How to Make a Payment with Apple Pay** - Visa cardholders can make in store purchases . . . by holding the phone in front of a contactless reader and placing their fingertip on the Touch ID to authorize the payment. . . . Visa account holders can also make purchases within apps . . . ."); "Visa and Apple Opening a New Era of Payments on Mobile Devices" ("Visa and Apple Opening a New Era"), *available at* http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1965351 ("Thanks to a new capability called Visa Token Service, participating financial institutions in the U.S. . . . will be able to add Visa debit and credit cards to Apple Pay, Apple's new payment service, and enable their customers to make easy and secure purchases at select U.S. merchants both in stores and in apps.").

Pictures showing an iPhone authenticating a user for enabling an Apple Pay transaction are shown below.



12(b) *a first device including: a biometric sensor configured to capture a first biometric information of the user;* – The iPhone 7 comprises a first device including a biometric sensor (e.g., a Touch ID fingerprint sensor) configured to capture a first biometric information of the user (e.g., fingerprint data) in connection with authorizing an Apple Pay transaction using Touch ID. *See* 12(a), *supra*; *see also, e.g.*, iPhone 7 Tech Specs ("Touch ID - Fingerprint sensor built into the new Home button"); iOS Security Guide, at 7-8 ("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. . . . 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 . . . . The fingerprint sensor is active only when the capacitive steel ring that surrounds the Home button detects the touch of a finger, which triggers the advanced imaging array to scan the finger and send the scan to the Secure Enclave.").

A picture identifying the Touch ID sensor on an iPhone 7 is shown below.

12(c) *a first processor programmed to: 1) authenticate a user of the first device based on secret information,* – The iPhone 7 includes a first processor (e.g., one or more processors within the iPhone 7) programmed to authenticate a user of the first device based on secret information (e.g., passcode) in connection with unlocking the iPhone 7. *See, e.g.*, iPhone 7 Tech Specs ("**Chip** . . . A10 Fusion chip with 64-bit architecture"); iOS Security Guide, at 7 ("**Secure Enclave -** The Secure Enclave is a coprocessor fabricated in the Apple S2, Apple A7, and later A-series processors. . . . 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. . . . To use Touch ID, users must set up their device so that a passcode is required to unlock it. When Touch ID scans and recognizes an enrolled fingerprint, the device unlocks without asking for the device passcode. The passcode can always be used instead of Touch ID, and it's still required under the following circumstances: [t]he device has just been turned on or restarted; [t]he device has not been unlocked for more than 48 hours; [t]he passcode has not been used to unlock the device in the last 156 hours (six and a half days) and Touch ID has not unlocked the device in the last 4 hours; [t]he device has received a remote lock command; [a]fter five unsuccessful attempts to match a fingerprint;

[w]hen setting up or enrolling new fingers with Touch ID."), 12 ("**Passcodes** . . . iOS supports six-digit, four-digit, and arbitrary-length alphanumeric passcodes. In addition to unlocking the device, a passcode provides entropy for certain encryption keys."), 34 ("**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. . . . **Secure Enclave**: . . . the Secure Enclave manages the authentication process and enables a payment transaction to proceed. . . . The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes payment applets certified by the payment networks."), 37 ("Communication between the Secure Enclave and the Secure Element takes place over a serial interface, with the Secure Element connected to the NFC controller, which in turn is connected to the application processor."); Apple Pay Security ("To help ensure the security of Apple Pay, you must have a passcode set on your device . . . .").

12(d) *2) retrieve or receive first biometric information of the user of the first device, –* The processor of the iPhone 7 is programmed to retrieve or receive first biometric information (e.g., fingerprint data) of the user of the first device in connection with authorizing an Apple Pay transaction. *See* 12(a)-12(c), *supra*; *see also, e.g.*, iOS Security Guide, at 7-8 ("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. . . . 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 . . . . The fingerprint sensor is active only when the capacitive steel ring that surrounds the Home button detects the touch of a finger, which triggers the advanced imaging array to scan the finger and send the scan to the Secure Enclave."), 34 ("**Secure**

Enclave: . . . the Secure Enclave manages the authentication process and enables a payment transaction to proceed. It stores fingerprint data for Touch ID.").

A picture showing a processor on the iPhone receiving a biometric input in connection with an Apple Pay transaction is shown below.

12(e) *3) authenticate the user of the first device based on the first biometric,* – The processor of the iPhone 7 is programmed to authenticate the user of the first device based on the first biometric information (e.g., the fingerprint data) in connection with authorizing an Apple Pay transaction. *See* 12(a), 12(c), 12(d), *supra*; *see also, e.g.*, iOS Security Guide, at 7 ("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."), 34 ("**Secure Enclave**: . . . the Secure Enclave manages the authentication process and enables a payment transaction to proceed. It stores fingerprint data for Touch ID."), 37 ("**Payment authorization** - On devices that have a Secure Enclave, the Secure Element will only allow a payment to be made after it receives authorization from the Secure

Enclave. On iPhone or iPad, this involves confirming the user has authenticated with Touch ID or the device passcode."); Apple Pay Security ("To send your payment information, you must authenticate using Touch ID or your passcode. No payment information is sent without your authentication."); Getting Started ("Apple Pay provides an easy and secure way for users to buy goods and services in your iOS app, watchOS app, or on your website. . . . Within your app or website, users can authorize payments using Touch ID . . . .").

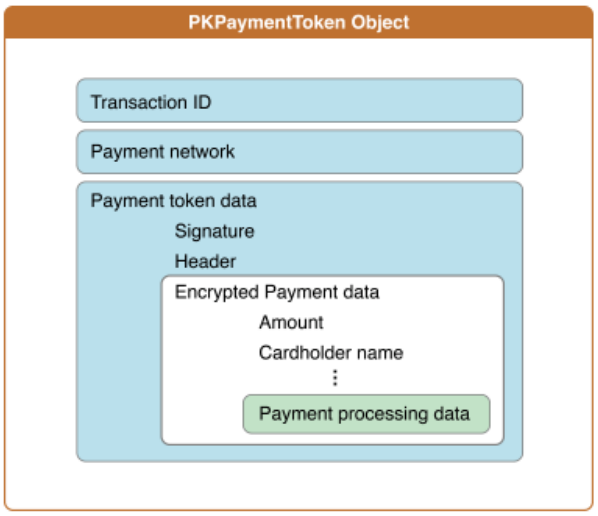
12(f) *4) generate one or more signals including first authentication information, an indicator of biometric authentication of the user of the first device, and a time varying value; and* – The processor of the iPhone 7 is programmed to generate one or more signals including first authentication information (e.g., a Device Account Number and/or other payment data), an indicator of biometric authentication of the user of the first device (e.g., a transaction-specific dynamic security code and/or other payment data), and a time varying value (e.g., a random number and/or counter) in connection with an Apple Pay transaction. *See* 12(a), 12(c), 12(e), *supra*; *see also, e.g.*, iOS Security Guide, at 34 ("**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. . . . **Secure Enclave**: . . . the Secure Enclave manages the authentication process and enables a payment transaction to proceed. . . . The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes payment applets certified by the payment networks."), 35 ("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."), 37 ("**Payment authorization** - On devices that have a Secure Enclave, the Secure Element will only allow a payment to be made after it receives authorization from the Secure Enclave. On iPhone or iPad, this involves confirming the user has

authenticated with Touch ID or the device passcode. . . . 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. . . . Using the pairing key and its copy of the current AR value, the Secure Element verifies the authorization received from the Secure Enclave before enabling the payment applet for a contactless payment. This process also applies when retrieving encrypted payment data from a payment applet for transactions within apps."), 38 ("**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 . . . . Next, the user must authenticate using Touch ID or their passcode before payment information is transmitted. . . . Once the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment."); Apple Pay Security ("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. . . . To send your payment information, you must authenticate using Touch ID or your passcode. . . . After you use Touch ID or enter your passcode on iPhone, . . . the Secure Element

provides your Device Account Number and a transaction-specific dynamic security code."); Getting Started ("Within your app or website, users can authorize payments using Touch ID . . . . Once authorized by the user, your app or website receives a payment object, which contains an encrypted payment token from PassKit. The payment token encapsulates the information needed to complete a payment transaction, including the device-specific account number, the amount, and a unique, one-time-use cryptogram."); "Visa Token Service Guide" ("Visa Token Service"), *available at* https://developer.visa.com/products/vts/guides ("**Transaction Processing** - Transaction processing is the process of using a token to complete a purchase. The consumer initiates a purchase on a web site, with a mobile phone at a retail store, or within a merchant application. The merchant submits a token and use case-specific dynamic security information (such as a cryptogram) in place of the PAN to its acquirer."); "Payment Token Format Reference" ("Payment Token"), *available at* https://developer.apple.com/library/content/documentation/PassKit/Reference/PaymentTokenJSON/PaymentTokenJSON.html#//apple_ref/doc/uid/TP40014929 ("A payment token is created by the Secure Element based on a payment request.").

Diagrams and tables describing the contents of the payment token sent in an App or web-based Apple Pay transaction are shown below.

Figure 1-1 Structure of a payment token



After being decrypted, the encrypted payment data contains the following keys and values:

Key	Value	Description
`applicationPrimaryAccountNumber`	string	Device-specific account number of the card that funds this transaction.
`applicationExpirationDate`	date as a string	Card expiration date in the format *YYMMDD*.
`currencyCode`	string	ISO 4217 numeric currency code, as a string to preserve leading zeros.
`transactionAmount`	number	Transaction amount.
`cardholderName`	string	*Optional.* Cardholder name.
`deviceManufacturerIdentifier`	string	Hex-encoded device manufacturer identifier.
`paymentDataType`	string	Either `3DSecure` or, if using Apple Pay in China, `EMV`.
`paymentData`	payment data dictionary	Detailed payment data.

Detailed Payment Data Keys (3-D Secure)

Key	Value	Description
`onlinePaymentCryptogram`	A Base64 encoded string	Online payment cryptogram, as defined by 3-D Secure.
`eciIndicator`	string	*Optional.* ECI indicator, as defined by 3-D Secure. The card network may add an ECI indicator to the card data. This indicator is then included in the payment token. If you receive an ECI indicator, you must pass it on to your payment processor; otherwise, the transaction fails.

12(g) *a first wireless transceiver coupled to the first processor and programmed to wirelessly transmit the one or more signals to a second device for processing;* – The iPhone 7 includes a first wireless transceiver (e.g., a Near Field Communication (NFC), Wi-Fi, Bluetooth, and/or Cellular Network transceiver) coupled to the processor and programmed to wirelessly transmit the one or more signals to a second device (e.g., a server or servers in the Visa payment

processing network, the Visa Token Service, and/or a payment processing system operated by another payment network and/or card issuer) for processing in connection with an Apple Pay transaction. *See* 12(a) and 12(f), *supra*; *see also, e.g.*, iPhone 7 Tech Specs ("**Cellular and Wireless** . . . LTE . . . WiFi . . . Bluetooth . . . NFC"); iOS Security Guide, at 34 ("**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."), 35 ("**How Apple Pay uses the NFC controller** - As the gateway to the Secure Element, the NFC controller ensures that all contactless payment transactions are conducted using a point-of-sale terminal that is in close proximity with the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. Once payment is authorized by the card holder using Touch ID or passcode, . . . contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field."), 38 ("**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. . . . These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction."); Apple Pay Security ("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. . . . After you use Touch ID or enter your passcode on iPhone, . . . 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. . . . Before they approve the payment, your bank 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 for Visa Cardholders ("**How to Make a Payment with Apple Pay** - Visa cardholders can make in store purchases . . . by holding the phone in front of a contactless reader and placing their fingertip on the Touch ID to authorize the payment. . . . Visa account holders can also make purchases within apps."); "Visa and Apple Opening a New Era ("Thanks to a new capability called Visa Token Service, participating financial institutions in the U.S. . . . will be able to add Visa debit and credit cards to Apple Pay, Apple's new payment service, and enable their customers to make easy and secure purchases at select U.S. merchants both in stores and in apps."); Visa Token Service ("**Transaction Processing** - Transaction processing is the process of using a token to complete a purchase. The consumer initiates a purchase on a web site, with a mobile phone at a retail store, or within a merchant application. The merchant submits a token and use case-specific dynamic security information (such as a cryptogram) in place of the PAN to its acquirer. The acquirer passes the token and its security information to the payment network as if it were a PAN. Visa detects the token and validates that the circumstances of the transaction are consistent with the domain restrictions defined for the token. If the token is authentic, Visa exchanges it for the corresponding PAN that is securely stored in Visa's Token Vault, and passes both the PAN and the token to the issuer for an authorization decision."); Getting Started ("Once authorized by the user, your app or website receives a payment object, which contains an encrypted payment token from PassKit. The payment token encapsulates the information needed to complete a payment transaction, including the device-specific account number, the amount,

and a unique, one-time-use cryptogram. . . . the app calls appropriate APIs in the payment processor SDK to pass the payment information to the payment processor for processing.").

A flow chart showing the steps in a typical Apple Pay transaction flow, including transmitting the signal(s) to a second device, is shown below.

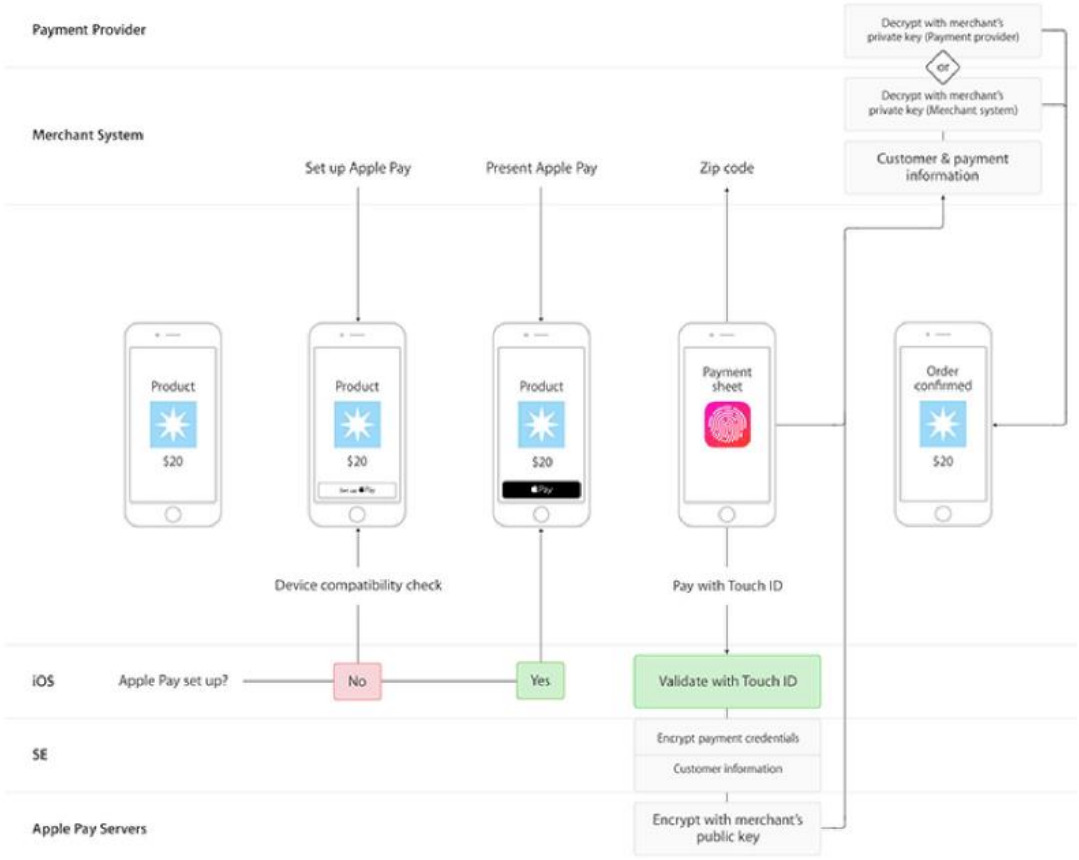


Figure 2: Payment Flow

12(h) *wherein generating the one or more signals occurs responsive to valid authentication of the first biometric information; and* – The processor of the iPhone 7 generates the one or more signals responsive to valid authentication of the first biometric information (e.g., fingerprint data) in connection with an Apple Pay transaction. *See* 12(a), 12(c), 12(e), 12(f), *supra*; *see also, e.g.*, iOS Security Guide, at 7 ("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."), 34 ("**Secure Enclave**: . . . the Secure Enclave manages the authentication process and enables a payment transaction to proceed. It stores fingerprint data for Touch ID."), 37 ("**Payment authorization** - On devices that have a Secure Enclave, the Secure Element will only allow a payment to be made after it receives authorization from the Secure Enclave. On iPhone or iPad, this involves confirming the user has authenticated with Touch ID or the device passcode. . . . 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. . . . Using the pairing key and its copy of the current AR value, the Secure Element verifies the authorization received from the Secure Enclave before enabling the payment applet for a contactless payment. This process also applies when retrieving encrypted payment data from a payment applet for transactions within apps."), 38 ("[T]he user must authenticate using Touch ID or their passcode before payment information is transmitted. . . . Once the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment."); Apple Pay Security ("To send your payment information, you must authenticate using Touch ID or your passcode. No payment information is sent without your authentication. . . . After you use Touch ID or enter your passcode on iPhone, . . . the Secure Element provides your Device Account Number and a transaction-specific dynamic security code."); Getting Started ("Within your app or website, users can authorize payments using Touch ID . . . . Once authorized by the user, your app or website receives a payment object, which contains an encrypted payment token from PassKit. The payment token encapsulates the information needed to complete a payment transaction,

including the device-specific account number, the amount, and a unique, one-time-use cryptogram.").

A flow chart showing the steps in a typical Apple Pay transaction flow, including generating the signal(s) responsive to Touch ID validation, is shown below.

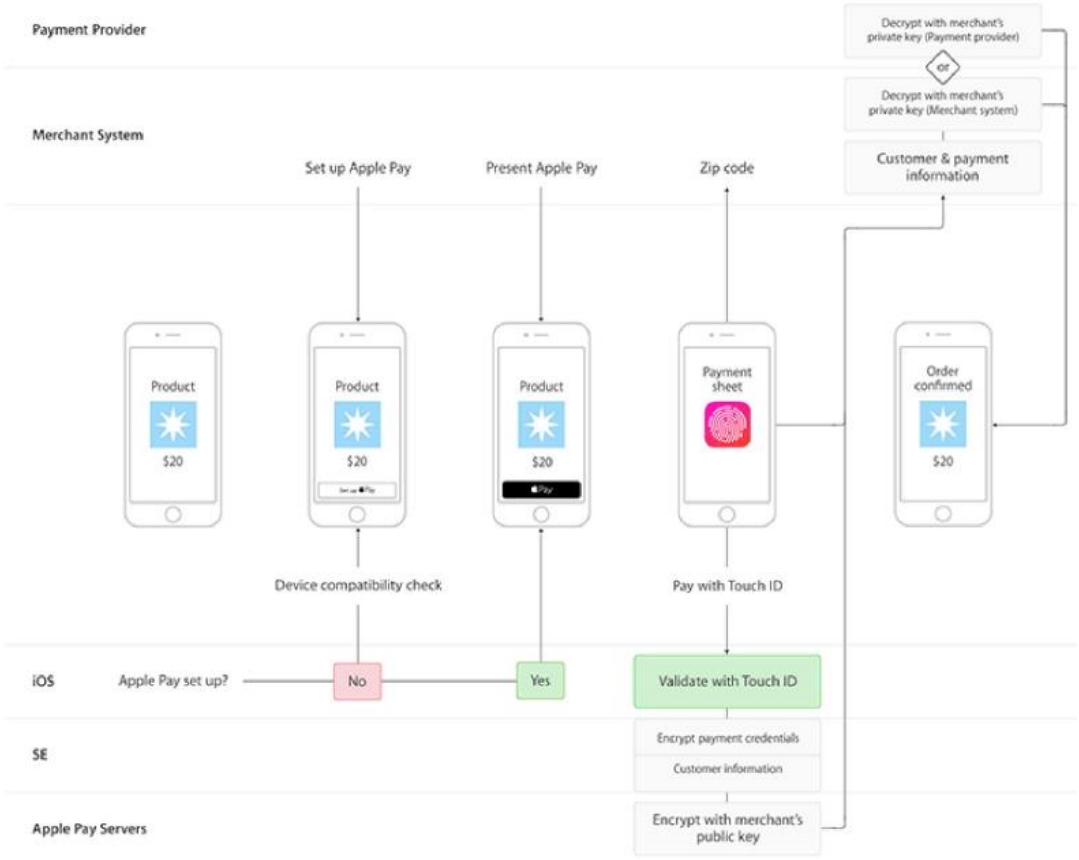


Figure 2: Payment Flow

12(i) *wherein the first processor is further programmed to receive an enablement signal indicating an approved transaction from the second device, wherein the enablement signal is provided from the second device based on acceptance of the indicator of biometric authentication and use of the first authentication information and use of second authentication information to enable the transaction.* – The processor of the iPhone 7 is further programmed to receive an enablement signal indicating an approved transaction (e.g., successful payment via

Apple Pay) from the second device (e.g., the server or servers in the Visa payment processing network, the Visa Token Service, and/or a payment processing system operated by another payment network and/or card issuer), wherein the enablement signal is provided from the second device based on acceptance of the indicator of biometric authentication (e.g., the transaction-specific dynamic security code and/or other payment data) and use of the first authentication information (e.g., the Device Account Number and/or other payment data) and use of second authentication information (e.g., a stored Device Account Number and/or other payment account data) to enable the Apple Pay transaction. *See* 12(a), 12(c), 12(e)-12(g), *supra*; *see also, e.g.*, Using Apple Pay ("**Pay in stores** . . . rest your finger on Touch ID and hold your iPhone within an inch of the contactless reader until you see Done and a checkmark on the display. . . . **Pay within apps** . . . place your finger on Touch ID. . . . When your payment is successful, you'll see Done and a checkmark on the screen. . . . **Pay on websites in Safari** . . . place your finger on Touch ID. When your payment is successful, you'll see Done and a checkmark on the screen."); iOS Security Guide, at 34 ("**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. . . . The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes payment applets certified by the payment networks."), 35 ("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."), 38 ("**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. . . . These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction. . . . the Device Account Number and a

transaction-specific dynamic security code are used when processing the payment."); Apple Pay Security ("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 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. . . . Before they approve the payment, your bank 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 for Visa Cardholders ("When paying with Visa through Apple Pay, the account holder's personal account information, including the 16-digit credit or debit card number, is never stored on the phone or by the merchant. Instead, Visa's new technology generates a unique digital account number that is a proxy for the primary card number, and is used to facilitate the payment. Digital account numbers are device-specific, meaning they are designed to only be used to make purchases with a specific mobile device or phone. . . . Visa cardholders can make in store purchases . . . by holding the phone in front of a contactless reader and placing their fingertip on the Touch ID to authorize the payment. . . . Visa account holders can also make purchases within apps."); "Visa and Apple Opening a New Era ("Visa Token Service technology works by replacing sensitive payment account information found on plastic cards with a digital account number or "token" that can be safely stored on mobile devices and used for in store and in app purchases. . . . Apple Pay lets you make purchases in some of the most highly visited stores and

within apps on the App Store with just the touch of a finger"); Visa Token Service ("**Transaction Processing -** Transaction processing is the process of using a token to complete a purchase. The consumer initiates a purchase on a web site, with a mobile phone at a retail store, or within a merchant application. The merchant submits a token and use case-specific dynamic security information (such as a cryptogram) in place of the PAN to its acquirer. The acquirer passes the token and its security information to the payment network as if it were a PAN. Visa detects the token and validates that the circumstances of the transaction are consistent with the domain restrictions defined for the token. If the token is authentic, Visa exchanges it for the corresponding PAN that is securely stored in Visa's Token Vault, and passes both the PAN and the token to the issuer for an authorization decision. The issuer (or its processor) approves or declines the transaction and returns the response to Visa. Visa exchanges the PAN for its token and sends the response with the token back to the acquirer and on to the merchant."); Getting Started ("Once authorized by the user, your app or website receives a payment object, which contains an encrypted payment token from PassKit. The payment token encapsulates the information needed to complete a payment transaction, including the device-specific account number, the amount, and a unique, one-time-use cryptogram. . . . the app calls appropriate APIs in the payment processor SDK to pass the payment information to the payment processor for processing.").

A flow chart showing the steps in a typical Apple Pay transaction flow, including receiving an enablement signal, is shown below.

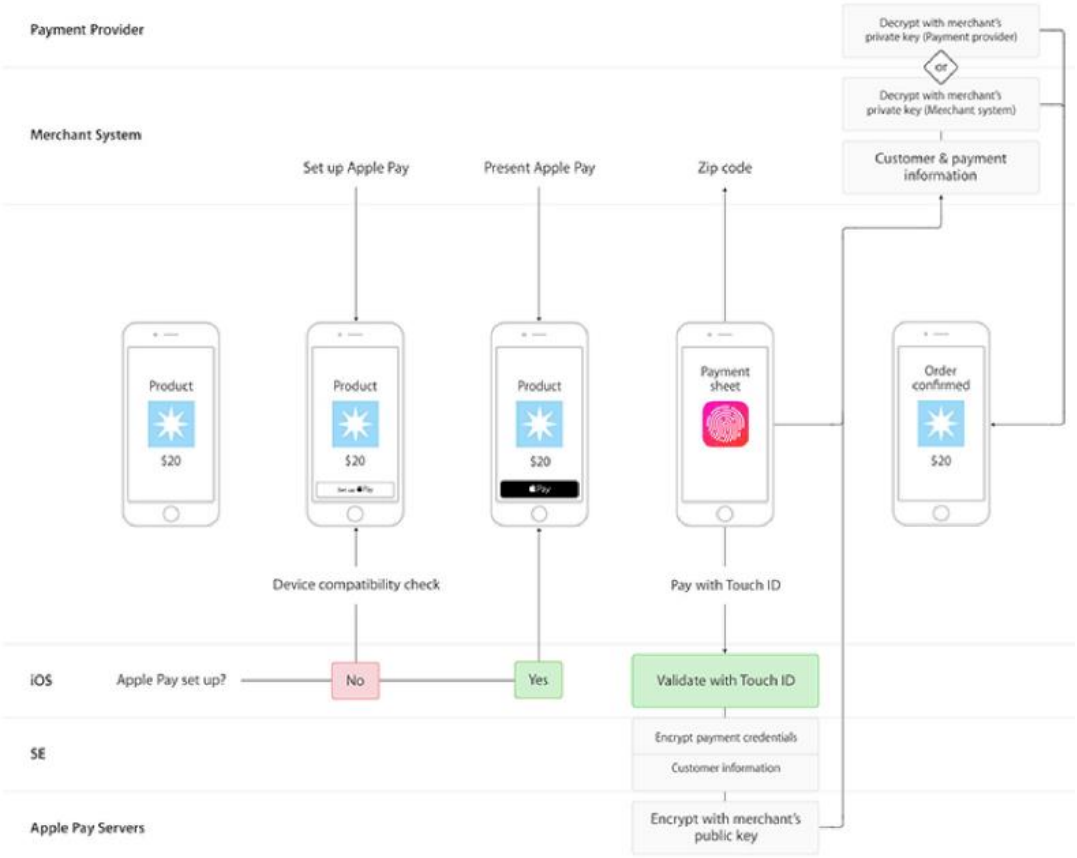


Figure 2: Payment Flow

107. To the extent necessary to direct infringement of any claim of the '137 patent by Apple and/or Visa, Apple and Visa are engaged in a joint enterprise with respect to the Apple Pay service such that the acts of one are attributable to the other. On information and belief, Apple and Visa worked together to develop and implement the Apple Pay service, and they offer Apple Pay to users pursuant to contractual agreement, with a common purpose to "accelerate adoption of mobile payments" using Visa cards together with the Apple Pay service, a shared pecuniary interest in that purpose, and shared control over the direction of the enterprise. *See* "Visa and Apple Opening a New Era of Payments on Mobile Devices," *available at* http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1965351&highlight. According to Visa executive Jim McCarthy, "It was

obvious that the Apple environment was going to be the launch partner" for using electronic devices to make touchless mobile payments without transmitting customer account information to and from merchants. *See* "American Express and Visa Love Apple Pay. Will Consumers?" *available at* https://www.bloomberg.com/news/articles/2014-10-23/apple-pay-partners-with-american-express-visa-card-networks. On information and belief, Visa dedicated 1,000 personnel to developing the Apple Pay service. *See* "Banks Did it Apple's Way in Payments by Mobile," *available at* https://dealbook.nytimes.com/2014/09/11/banks-did-it-apples-way-in-payments-by-mobile/?_r=0.

108. To the extent necessary to direct infringement of any claim of the '137 patent by Apple, Apple is also engaged in a joint enterprise tied to the Apple Pay service with other payment networks, whose acts are attributable to Apple. On information and belief, Apple and other payment networks worked together to develop and implement the Apple Pay service, and they offer Apple Pay to users pursuant to contractual agreement, with a common purpose that their cards be used with the Apple Pay service, a shared pecuniary interest in that purpose, and shared control over the direction of the enterprise. *See* "American Express and Visa Love Apple Pay. Will Consumers?" *available at* https://www.bloomberg.com/news/articles/2014-10-23/apple-pay-partners-with-american-express-visa-card-networks; "Banks Did it Apple's Way in Payments by Mobile," *available at* https://dealbook.nytimes.com/2014/09/11/banks-did-it-apples-way-in-payments-by-mobile/?_r=0.

109. To the extent necessary to direct infringement of any claim of the '137 patent by Apple and/or Visa, the acts of card issuers tied to the Apple Pay service are attributable to Apple and, for transactions involving Visa cards, to Visa. On information and belief, Apple and Visa condition participation in the Apple Pay service (and receipt of revenue resulting therefrom)

upon performance of claimed steps of '137 patent claims associated with processing Apple Pay transaction requests, and they establish the manner and timing of that performance. *See, e.g.*, "Apple Pay participating banks in Canada and the United States," *available at* https://support.apple.com/en-us/HT204916; "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides.

110. To the extent necessary to direct infringement of any claim of the '137 patent by Apple and/or Visa, the acts of end-users of Apple devices tied to the Apple Pay service are attributable to Apple and, for transactions involving Visa cards, to Visa. On information and belief, Apple and Visa condition participation in the Apple Pay service (and receipt of benefits therefrom) upon performance of claimed steps of '137 patent claims associated with processing Apple Pay transaction requests, and they establish the manner and timing of that performance. *See, e.g.*, "Apple Pay," *available at* http://www.apple.com/apple-pay/; "Using Apple Pay in stores, and within apps and websites," *available at* https://support.apple.com/en-us/HT201239; "Apple Pay," *available at* https://usa.visa.com/pay-with-visa/featured-technologies/apple-pay.html.

111. At least as early as the filing and service of this Complaint, Apple is also indirectly infringing the '137 patent.

112. Apple has actual knowledge of USR's rights in the '137 patent and details of Apple's infringement of the '137 patent based on at least the filing and service of this Complaint.

113. Apple manufactures, uses, imports, offers for sale, and/or sells the '137 Accused Products with knowledge of or willful blindness to the fact that its actions will induce Apple's partners and end users to infringe the '137 patent. When used to conduct and/or process an Apple Pay transaction, the '137 Accused Products practice one or more claims of the '137 patent.

Apple induces others to infringe the '137 patent in violation of 35 U.S.C. § 271 by encouraging and facilitating others to practice the '137 patent's inventions for performing secure financial transactions. Apple enables others to infringe the '137 patent by incorporating both software and hardware into the '137 Accused Products enabling others to conduct and/or process transactions with Apple Pay, and by publishing information about infringing aspects of its Apple Pay service.

114. Apple actively and knowingly induces end users to infringe the '137 patent by teaching and encouraging end users to use Apple Pay in an infringing manner, with the specific intent to cause the infringing acts. For example, Apple induces end users to authenticate their identity in connection with Apple Pay transactions in ways that infringe claims of the '137 patent. Apple's website advertises the Apple Pay service to end users as follows: "Make secure purchases in stores, in apps, and now on the web." *See, e.g.*, "Apple Pay," *available at* http://www.apple.com/apple-pay/. The same site includes an instructional video showing users how to use Apple Pay at a point of sale. *Id.* Another page on Apple's website further explains to users how to use Apple Pay. *See, e.g.*, "Using Apple Pay in stores, and within apps and websites," *available at* https://support.apple.com/en-us/HT201239. When end users used the Apple Pay service to conduct transactions in the manner Apple instructs, they infringe one or more claims of the '137 patent.

115. Apple actively and knowingly induces Visa and other partners to infringe the '137 patent by adding payments cards to Apple devices and sending Apple Pay transaction requests to Visa and other partners' servers for processing, thereby inducing Visa and other partners to process Apple Pay transactions in an infringing manner, with the specific intent to cause the infringing acts. Apple induces Visa and other partners to authenticate users in connection with Apple Pay transactions in ways that infringe claims of the '137 patent. *See, e.g.*, "Getting Started

with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides; "Apple Pay," *available at* https://usa.visa.com/pay-with-visa/featured-technologies/apple-pay.html; "American Express and Visa Love Apple Pay. Will Consumers?" *available at* https://www.bloomberg.com/news/articles/2014-10-23/apple-pay-partners-with-american-express-visa-card-networks; "Banks Did it Apple's Way in Payments by Mobile," *available at* https://dealbook.nytimes.com/2014/09/11/banks-did-it-apples-way-in-payments-by-mobile/?_r=0.

116. Apple contributes to the infringement of the '137 patent in violation of 35 U.S.C. § 271. Apple knows that infringing components of the '137 Accused Products are especially made or especially adapted for use in the infringement of the '137 patent. The infringing components of these products are not staple articles or commodities of commerce suitable for substantial non-infringing use, and the infringing components of these products are a material part of the invention of the '137 patent. The '137 Accused Products contain infringing components, such as software enabling the use of the Apple Pay service and one or more processors specially configured to generate authentication information and supporting Apple Pay transactions. These hardware and/or software components that Apple provides are separable from Apple's products, a material part of the patented invention, and have no substantial non-infringing use. Accordingly, Apple is also contributing to the direct infringement of the '137 patent by the end users and by Visa.

117. At least as early as the filing and service of this Complaint, Visa is also indirectly infringing the '137 patent.

118. Visa has actual knowledge of USR's rights in the '137 patent and details of Visa's infringement of the '137 patent based on at least the filing and service of this Complaint.

119. Visa manufactures, uses, imports, offers for sale, and/or sells the '137 Accused Products with knowledge of or willful blindness to the fact that its actions will induce Visa's partners and end users to infringe the '137 patent. When used to conduct and/or process an Apple Pay transaction, the '137 Accused Products perform all of the steps of one or more claims of the '137 patent. Visa induces others to infringe the '137 patent in violation of 35 U.S.C. § 271 by encouraging and facilitating others to practice the '137 patent's inventions for performing secure financial transactions. Visa enables others to infringe the '137 patent by enrolling Visa cards in the Apple Pay service, providing the Visa Token service, providing instructions for how to use Apple Pay, and processing Apple Pay transactions.

120. Visa actively and knowingly induces end users to infringe the '137 patent by teaching and encouraging end users to use Apple Pay in an infringing manner, with the specific intent to cause the infringing acts. For example, Visa induces end users to authenticate their identity in connection with Apple Pay transactions in ways that infringe claims of the '137 patent. Visa's website advertises the Apple Pay service to end users as follows: "Visa with Apple Pay: a simple, secure way to pay. Learn how to start using your Visa card on Apple Pay today." *See, e.g.*, "Apple Pay," *available at* https://usa.visa.com/pay-with-visa/featured-technologies/apple-pay.html. The same site includes written information and an instructional video showing users how to use Apple Pay at a point of sale. *Id.* When end users used the Apple Pay service to conduct transactions in the manner Visa instructs, they infringe one or more claims of the '137 patent.

121. Visa actively and knowingly induces Apple and other partners to infringe the '137 patent by enrolling Visa cards in the Apple Pay service and processing Apple Pay transaction requests from Apple devices, thereby enabling Apple's devices and servers and other partners'

servers to carry out Apple Pay transactions in an infringing manner, with the specific intent to cause the infringing acts. Visa induces Apple and other partners to authenticate users in connection with Apple Pay transactions in ways that infringe claims of the '137 patent. *See, e.g.*, "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides.

122. Visa contributes to the infringement of the '137 patent in violation of 35 U.S.C. § 271. Visa knows that infringing components of the '137 Accused Products are especially made or especially adapted for use in the infringement of the '137 patent. The infringing components of these products are not staple articles or commodities of commerce suitable for substantial non-infringing use, and the infringing components of these products are a material part of the invention of the '137 patent. Visa provides "a unique digital identifier called a token," which is a 16-digit sequence of numbers formatted just like a payment-card number. *See* "Getting Started with Visa Token Services," *available at* https://developer.visa.com/products/vts/guides. This "token" is used by Apple Pay; Visa also provides components used to generate a transaction-specific dynamic security code used by Apple Pay, and provides programmed servers that process Apple Pay transactions. The components Visa provides are separable from the '137 Accused Products, a material part of the patented invention, and have no substantial non-infringing use. Accordingly, Visa is also contributing to the direct infringement of the '137 patent by the end users and by Apple.

123. Defendants' infringement has caused, and is continuing to cause, damage and irreparable injury to USR, and USR will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

124. USR is entitled to injunctive relief and damages in accordance with 35 U.S.C. §§ 271, 281, 283, and 284.

125. This is an exceptional case. USR is entitled to attorneys' fees and costs under 35 U.S.C. § 285 as a result of the infringement of the '137 patent by Defendants

PRAYER FOR RELIEF

WHEREFORE, USR respectfully requests:

1. That Judgment be entered that Defendants have infringed one or more of the Asserted Patents, directly and indirectly, by way of inducement or contributory infringement, literally or under the doctrine of equivalents;

2. That, in accordance with 35 U.S.C. § 283, Defendants and all affiliates, employees, agents, officers, directors, attorneys, successors, and assigns and all those acting on behalf of or in active concert or participation with any of them, be preliminarily and permanently enjoined from (1) infringing the Asserted Patents and (2) making, using, selling, and offering for sale the Accused Products;

3. An award of damages sufficient to compensate USR for Defendants' infringement under 35 U.S.C. ¶ 284;

4. That the case be found exceptional under 35 U.S.C. § 285 and that USR be awarded its attorneys' fees;

5. Costs and expenses in this action;

6. An award of prejudgment and post-judgment interest; and

7. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, USR respectfully demands a trial by jury on all issues raised by the Complaint.

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Jack B. Blumenfeld

Jack B. Blumenfeld (#1014)
Jeremy A. Tigan (#5239)
1201 N. Market Street
P.O. Box 1347
Wilmington, DE 19899-1347
(302) 658-9200
jblumenfeld@mnat.com
jtigan@mnat.com
Attorneys for Universal Secure Registry LLC

OF COUNSEL:

Harold Barza
Tigran Guledjian
Valerie Roddy
Jordan Kaericher
QUINN EMANUEL
URQUHART & SULLIVAN, LLP
865 S Figueroa Street, 10th Floor
Los Angeles, CA 90017
(213) 443-3000

Sean Pak
Brian E. Mack
QUINN EMANUEL
URQUHART & SULLIVAN, LLP
50 California Street, 22nd Floor
San Francisco, CA 94111
(415) 875-6600

May 21, 2017
11055218