UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

VINDOLOR, LLC, Plaintiff v. **HAT WORLD, INC. D/B/A LIDS,** Defendant	**Case No. 2:18-cv-00187-JRG-RSP** **JURY TRIAL DEMANDED**

AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Vindolor, LLC ("Vindolor") hereby asserts the following claims for patent infringement against Defendant Hat World, Inc. d/b/a Lids ("Defendant" or "Lids"), and alleges as follows:

THE PARTIES

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

2.   Defendant is a corporation organized and existing under the laws of Minnesota with its principal place of business at PO Box 17, Nashville, Tennessee 37202.

JURISDICTION AND VENUE

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

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

5.   Defendant has a regular established place of business in this judicial district at 4601 S Broadway Ave, Tyler, Texas 75703.

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

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

<div align="center"><u>**OVERVIEW OF THE '391 PATENT**</u></div>

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

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

10.   As described in the following passages from the specification of the '391 Patent, there were problems and shortcomings in the then-existing field of ***portable electronic personal identification systems***:

> As the computer age has progressed in recent years, there has been a vast increase in the use of private electronic transactions. Banks, credit card companies and other financial institutions offer a wide variety of options and services that may now be conducted online. The ever expanding Internet has brought computerized home shopping to the forefront of cyber-technology. Consumers may now conduct a majority of their financial business in numerous ways that either did not exist, or were not available for use by the general public as little as five years ago. Some examples of such transactions include computerized home banking, the use of automatic teller machines, computerized stock transactions, credit or debit based product dispensers, security entrances, telephone access and transactions, long distance calling cards, identification cards (including any such card used for services like health care, insurance, automobile service accounts, etc.), and even secure transactions over the Internet.

The essence of any secret transaction, whether financial or not, is the ability to keep it private and secure from potential theft. Although computerization of transactions and improvements in technology have increased the ease with which consumers may conduct these private transactions, the nature of the technology is such that the information, when transmitted electronically, can be intercepted and used for criminal purposes.   Consequently, as the usage of these kinds of electronic transactions has increased, a need for improved systems and methods to ensure their security has increased as well. Completion of most electronic financial transactions requires the use of a password or personal identification number (PIN) that identifies a person as one authorized to conduct a specific transaction. For example, most automatic teller machine (ATM) cards have a magnetic strip that, when read by the ATM computer, identifies the bank and the account to be accessed. The machine then asks for entry of the PIN which has been assigned to that account. If the correct PIN code is entered, the user may access the bank account to conduct a variety of transactions, including, withdrawals, deposits or requesting account statements.

There are several drawbacks to this approach. First, the PIN must be chosen when the account is opened, and may only be changed by bank personnel upon request by the user. Therefore, a person who hasn't realized that her ATM card was stolen may go days without requesting a new PIN number to be assigned to her account. During that time, the thief who stole her card may have discovered the PIN number, and made unauthorized withdrawals from her account. Second, the "choose-your-own" PIN code system is not sufficiently unique to provide adequately reliable identification. A person not the owner of an account who obtains knowledge of a PIN code may easily gain unauthorized access to that account because, all she or he needs to do is discover the four digit PIN code number associated with that account. While there are thousands of possible permutations or combinations of digits that could make up any one PIN code, the actual code is not specifically unique to that person. For example, two or more bank accounts at the same bank could theoretically have the same PIN code. As long as the correct PIN code is entered for the account sought to be accessed, the system does not care if the entered PIN code could also access other accounts as well, because it only focuses on the specific account number received from the ATM card's magnetic strip. The major fault with this system is that it does not truly identify the account holder, but allows access to anyone holding the card who also enters the correct identification number. In other words, the current system merely assumes that if the individual who attempts to use the card knows the correct PIN number, then that person is authorized to access the account. Therefore, the PIN code system does not offer the flexibility, security, and uniqueness that other forms of identification may offer. Specifically, the PIN code system cannot distinguish between users actually

authorized to access the account, and unauthorized users that have discovered the correct PIN code.

In typical applications which require the use of a pass key to facilitate access, users are issued a key that contains a specific, pre-determined access code stored on a magnetic strip or other such storage device, and which de-activates a locking mechanism, alarm system, or other such device and allows the key holder to access whatever secure objective was being protected. Again, this method of restricting access provides flawed security because it fails to provide a means for positively identifying the user as an authorized user as a condition precedent to granting access to the secure objective.

Others have attempted to solve the security problem by creating means for identification based on a biometric character trait unique to specific users. Such character traits may include voice identification, fingerprint analysis, retina scan, DNA analysis, or other biometric characteristic. By utilizing technology which analyzes these types of character traits, systems have been developed which can more accurately identify specific persons. For example, the invention disclosed in Parra, teaches a method and apparatus for identifying a particular individual based on the uniqueness of the acoustic characteristics of his/her voice. According to Parra, the voice characteristics of the user are stored on a magnetic strip on the back of a card. When the card is inserted into the interface, the user is prompted to speak a word. The spoken word is then digitized and its acoustic characteristics compared to a stored digital version of the word. If the characteristics of the stored word match those of the spoken word, the user may be granted access.

There are several drawbacks to this approach. First, while the Parra invention attempts to address the security issue regarding uniqueness of identification characteristics, it does not address flexibility of use. The Parra system, like the PIN code system requires the use of a pre-programmed word or phrase that is compared to the spoken word or phrase. Parra offers no built-in ability to change the access word or phrase without going through bank personnel. Further, the Parra invention does not address tying the voice-identification to the generation of voice pattern-based numeric, alphanumeric or telephone tone codes for use in applications like telephone long distance credit cards, or Internet passwords, which would allow more widespread use of the identification technology. Finally, the Parra invention is specifically limited to a voice identification technology system, rather than relating to a non-platform specific system.

Online systems, such as those disclosed in the June, 1997 issue of *Byte* magazine (volume 22, number 6, pp. 70-80) rely on digital signatures, digital certificates and

server-based verification of smart card electronic signatures in creating a high level of security for financial transactions and other secured access applications. These systems involve high-end algorithmic encoding of identification numbers which may then be sent to and from clients and servers during the authorization process. These systems, while providing high levels of security are not fool proof.

For "hash" signatures, both the client and server must have the access key to complete the encoding and decoding of the hashed data. This means that a security breach at either end (client or server) may result in a hacker's ability to obtain a forgery of the access key, and thereby, access to the client's restricted data or accounts.

Public-key algorithms, provide better security in that the server does not need to have a copy of the access key to verify a digital signature. The private key algorithms used to encode the data are known only to the client encryptor. However, the system of encoding and decoding is set up such that the server side can use a different decoder algorithm to verify the encoded signature. Therefore, the access key remains significantly more secure than a hash based signature, because it is only known to the client side, while the server can still authenticate it. Public-key algorithms, however, do not assure that the person using the key is the actual owner, rather than a forgery. The key is actually just a number; it bears no resemblance to the particular user, and carries no personal or unique data about the user. Further, the public key system requires a great deal of support and infrastructure, particularly in maintaining databases of all active and revoked certificates or keys.

'391 Patent at col. 1, l. 16 – col. 3, l. 33.

11.   As described in the following passages from the specification of the '391 Patent, the

claimed invention of the '391 Patent is directed to specific improvements and solutions to the

problems and shortcomings in the then-existing field of ***portable electronic personal***

identification:

A preferred embodiment of the invention is a card or other small portable device that contains a device which positively identifies the cardholder as an authorized or unauthorized user, and thereby provides or prevents access to a specific secure objective (e.g. an ATM machine, security gate or door, computer scanning device, and other such accounts, areas or the like which require restricted access). The invention obtains the potential user's unique personal identification profile, preferably a digital representation of some uniquely identifying trait of the user,

AMENDED COMPLAINT   5

such as, but not limited to any biometric analysis system (e.g. fingerprint, DNA, palm print, retina scan, etc.), or other identification system which produces a digital profile that is sufficiently unique as to provide a reasonable degree of certainty as to identification. In a preferred embodiment of the invention, the device, circuitry or apparatus by which the system obtains the user's ID profile is contained on board the invention. However, the disclosed invention may receive and utilize an ID profile calculated by an outside system as well.

The identification profile created (or received) by the invention may be a numeric, alphanumeric, or other digital representation of the user's unique biometric or digital signature profile. The spontaneously created identification profile is then compared to any predetermined authorized profiles associated with the invention to determine if the user is authorized as one of the users assigned to that account. The invention anticipates that more than one "account" may be assigned to any particular embodiment of the invention (e.g. an ID card, bank account card, etc.), so that families, businesses, or other groups may share identification devices. In other words, members of a particular household may use each other's identification cards in order to promote flexibility of use.

Once authorization has been established, the digital representation of the identification value may be converted into one or more access codes which may be used to provide access to a particular one of any number of secure accounts or databases, restricted areas, or other secure objectives. This feature allows for the existence of individually secure "accounts" on multiple-user cards. Since several individual and group "accounts" may be stored on a single card or other small portable identification device, the creation of ID profile-based personal identification numbers (PINs) provides a means by which cards utilized for group accounts may also be utilized for individual accounts without risk of security breach.

For example, considering an embodiment of the invention as an ID card containing two different accounts, a group account may provide access to a residence or other shared secure objective, while on the same ID card, an individual account may provide individual access to a bank account. Any member of the group may use the ID card to access the residence. The card will be able to verify all of the group members' profiles as authorized to use the card to access the residence. However, if the bank account can only be accessed by a specific PIN code, which is based on the authorized user's ID profile, then any PIN code calculated using any other group members' ID code will not produce the PIN required to access the account, and other group members will be denied access to the bank account.

One preferred embodiment of the invention is a bank account or credit account "smart card" utilizing voice identification technology (similar to that disclosed in Parra), however, it may be noted that other biometric identification analyses may be used (such as fingerprint scan, iris scan, DNA, etc.). In the voice identification based system, the smart card converts the user's spoken words into a numerical value based on the user's unique digital acoustic characteristics. At the time a bank (or other financial institution) account is opened, the account holder speaks a predetermined phrase and/or several predetermined "code words" that are analyzed and converted into a base digital voice signature value. The account holder's account information (which may include the original voice profile) may then be stored on the card. The predetermined voice profile represents the unique ID profile associated with that account holder, and may be stored on the institution's main computer database, on the smart card, or both.

When the account holder wishes to access his account, he activates the on-board voice identification device, which analyzes his voice patterns to determine if he is authorized to use the card. Next, the user inserts the card into an ATM (or other device employed for accessing an account). The invention converts the user's spontaneous word or phrase into a voice print value. The voice print value is then compared with the predetermined ID profile stored on the ATM card, the online computer database, or both, for match or discrepancy range. If the user's voice pattern matches, or is within the acceptable discrepancy range assigned to the account, then the smart card may authorize the user to access the account. Otherwise, access to the account may be denied. The system may require the user to speak one of any specific code words previously recorded by the user, or may simply analyze any random words or phrases spoken by the account holder, depending on what kind of voice identification technology is employed by the financial institution, or stored on the card or other portable device.

Other uses for the disclosed invention may include such uses in conjunction with a healthcare services card, driver's license, or passport. As a healthcare services card the present invention may provide a quick and efficient means for positive identification and access to medical history. In emergency situations such information must be quickly obtained in order to provide safe and adequate diagnosis and treatment. Because many emergency patients arrive at the emergency room unconscious, the disclosed invention is particularly suited to allow ER physicians and nurses rapid access to important medical information that they would not otherwise be able obtain from the patient herself.

As used in conjunction a driver's license or passport, the disclosed invention has particularly important applications, not only for positively identifying a person, but

also for allowing a police officer or other official access to information about a cardholder's criminal record, driving record, or other such information that may be useful for law enforcement or regulation of international travel.

The disclosed invention differs from the prior art in two important ways. First, the biometric identification device is preferably on board the card, rather than contained in the ATM machine. This allows the user to verify his identity before physically interacting with the account interface (e.g. ATM machine). Further, it facilitates the use of other features of the invention, such as remote control operation, as well as eliminating the need for expensive, onsite identification devices or systems. The card automatically identifies the user, verifies his status as authorized or unauthorized, and grants or denies access accordingly.

Second, the invention includes a feature which allows the creation of unique, secure PIN codes for use as preliminary or secondary verification of identification, and which allows multiple group and individual accounts to exist on a single card. For example, the card or system may include a device for creating a distinctive, and user-specific alphanumeric code based on the potential user's unique identification profile value. When the potential user activates the verification process, the spontaneously created identification value calculated from his profile is transformed by the invention into a specific code which can be used by the device protecting the secure objective as a secondary or supplemental means for positive identification.

A specifically useful application of this feature for financial transactions is the creation of secure PIN codes for ATM cards. This feature adds flexibility to such cards in that in the event of a malfunction of or mis-recognition by the primary identification method, the uniquely generated PIN code may still authorize access. This secondary ID method is equally secure, since it is generated according to the originally stored voice print or other ID characteristic. Also, as explained above, this feature allows for the existence and efficient management of multiple accounts on a single card.

Another difference from the prior art, is that the system of the present invention, as disclosed herein, may include a means for generating unique access codes for use in identifying a user via telephone or computer modem. Like the secondary PIN codes, the transmitted tone codes are generated according to the unique ID number assigned to the user's voice print, or other distinctive identification characteristic. Therefore, since the tone codes are unique to the user, they are more secure, and unusable by anyone other than the authorized user. Further, the ability to generate these tone codes provides a more flexible use of the disclosed invention, because

compatible on-site equipment at an account location is not required. The card automatically generates the correct telephone tones corresponding to the account's access code, and thus providing access as if the code had been entered manually. This tone code is more secure, however, because it is only generated once identification has been established.

The disclosed invention may be integrated into existing portable electronic devices, like cellular phones, laptop computers, portable digital assistants (PDAs), calculators, electronic address books, etc., to increase the flexibility and portability for the user. For example, integration of the invention into a telephone particularly a cellular telephone) may be significantly useful. As described above, the invention may create specific tone codes for identification purposes, and may have a voice identification based ID system. By integrating the invention into a cellular (or other) telephone, the device can take advantage of components already present in the "host" device. In the telephone example, the device may use the phone's built in microphone and/or speaker system as the voice ID input. Additionally, any tone codes the device may create and transmit may be so created and transmitted by the phone's built in tone generator.

A preferred embodiment of the invention also includes the ability to update information (such as the algorithm used to create the specific identification number-based numeric, alphanumeric, or tone code associated with a particular account) each time the account is accessed. An account utilizing this feature is not issued a specific PIN code, but instead uses dynamic codes. Once the account has been accessed, the card stores a new algorithm to use the next time the account will be accessed. Upon subsequent use, the new algorithm converts the user's unique identification value into a completely new PIN code which the account database has already associated with the account at the prior transaction. This feature provides better security because any person not authorized to access the account, who may happen to obtain the PIN code on one occasion, will not be able to access the account, because the PIN code changes each time the account is accessed.

Alternatively, the account may be assigned a plurality of PIN codes, any of which may authorize access. The smart card may store the algorithms which produce these PIN codes from an authorized user's unique identification value. Each time the account is accessed, the access code generator uses a different, randomly chosen stored algorithm, to produce one of the acceptable account access codes. In this manner, the account may be further protected because a chance interception of one access code will not automatically grant authorization, since the same access code is never allowed twice in a row.

The invention as disclosed herein may also be easily integrated into existing renewal systems. The identification system may include the ability to store and/or calculate renewal dates, or the number of times a particular secure objective has been accessed in order to determine when the account must be renewed. For example, when an account card, pass key, etc. is issued, it may grant only limited access in that it remains active only for a specific period of time or for a particular number of accesses, until reactivated or reprogrammed. Each time the card or key is used, it may determine whether the access period has lapsed by determining whether the renewal date has passed, or whether the maximum number of accesses has been exceeded. The card or other device may be renewed via bio-metric identification, or may be reprogrammed, either directly or on line. In this manner, the system provides for increased security in that a card or other device will automatically cease to provide access upon expiration, so that anyone who manages to obtain unauthorized access using that card will be unable to renew it and continue gaining unauthorized access.

Id. at col. 3, l. 47 – col. 7, l. 13.

12.   Claim 1 of the '391 Patent recites:

1.   A portable identification system comprising

[a]   a storage medium for storing electronic data;

[b]   one or more inputs; one or more outputs;

[c]   a verifying means for determining user authorization or non-authorization, said verifying means receiving data from at least one of said one or more inputs, which data is derived from biometric or other distinctive characteristics of the user, said verifying means generating an identification profile for each user, wherein said identification profile is determined from said data, and

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

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

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

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

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

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

17.   As appreciated from the substance and disclosure of the '391 Patent application, the record

disclosed from the examination of the '391 Patent, including the statements in the notice of

allowance, the record of the prior art identified and considered by the examiner, and the patents

and patent applications citing to and discusses the '391 Patent, the claimed inventions of the '391

Patent:

- increase the accuracy of portable electronic personal identification systems, which had been an issue with prior systems;

- improve the security and portability of portable electronic personal identification systems, which had been an issue with prior systems;

- improve personal identification security of portable electronic personal identification systems, which had been an issue with prior systems;

- improve the ease and flexibility of use of portable electronic personal identification systems, which had been an issue with prior systems;

- decrease fraudulent transactions associated with the use portable electronic personal identification systems, which had been an issue with prior systems;

- improve the uniqueness of access codes generated by portable electronic personal identification systems, which had been an issue with prior systems;

- improve the complexity of access codes generated by portable electronic personal identification systems while improving its ease of using the portable electronic personal identification systems, which had been an issue with prior systems;

- improve the security and uniqueness of access codes generated by portable electronic personal identification systems by generating an access code that is an identification specific digital signature, which had been an issue with prior systems;

- improve the security and uniqueness of access codes generated by portable electronic personal identification systems by generating an access code that is identification specific, which had been an issue with prior systems;

- improve portable electronic personal identification systems by requiring positive identification prior to granting access to a secure objective, which had been an issue with prior systems;

- reduce risks associated with security and data breaches of portable electronic personal identification systems, which had been an issue with prior systems;

- reduce infrastructure, support, and maintenance of portable electronic personal identification systems, which had been an issue with prior systems;

- increase the efficiencies of portable electronic personal identification systems, which had been an issue with prior systems;

- reduce infrastructure, support, and maintenance of portable electronic personal identification systems, which had been an issue with prior systems; and

- are directed to improvements in the electronic personal identification technology itself and not directed to generic components performing conventional activities.

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

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

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

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

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

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

23.   As demonstrated above by its frequent citation (over 265) by the United Stated Patent Office in other later-issued patents, reexaminations, and patent applications, the '391 Patent represents a fundamental technical improvement in the area of electronic identification systems. "USPTO Patent Full-Text and Image Database – ref/6213391" ("**USPTO Patent Search**"), available at http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL &p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=6213391.PN.&OS=P N/6213391&RS=PN/6213391 (last accessed April 9, 2018), "USPTO Patent Application Full Text and Image Database" ("**USPTO Patent Application Search**"), http://appft.uspto.gov/ netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=0&f=S&l=50&TERM1=6213391&FIELD1=&co1=AND&TERM2=&FIELD2=& d=PG01 (last accessed April 9, 2018).

24.   These patents were issued to such companies as:

- Amazon Technologies, Inc.,

- American Express Travel Related Services Company, Inc.,

- Apple, Inc.,

- AT&T Corp.,

- Bell South Intellectual Property Corporation,

- Citicorp Development Center, Inc.,

- Exxonmobile Research & Engineering Company,

- First Data Corporation,

- First USA Bank, N.A.,

- Fujitsu Limited,

- International Business Machines Corporation,

- JP Morgan Chase Bank,

- Mastercard International, Inc.,

- Motorola, Inc.,

- Palm, Inc.,

- Securecard Technologies, Inc.,

- Sprint Communications Company, L.P.,

- The Western Union Company, and

- Visa U.S.A., Inc.

USPTO Patent Search.

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

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

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

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

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

purpose computer, nor does it rely on a purely conventional computer implementation of an abstract mathematical formula, nor is it based on generalized steps to be performed on a computer using conventional activity.

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

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

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

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

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

35.   On November 27, 2000, Examiner Diane I. Lee issued a notice of allowance for the '391

Patent, which is noted with her signature on the notice of allowance.

36.   Supervisory Examiner Michael G. Lee approved the issuance of the notice of allowance

for the '391 Patent, which is noted by his signature on the notice of allowance.

37.   As stated in the notice of allowance:

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

Lane discloses an identification card having an input device having fingerprint sensor for capturing the fingerprints of the user, a storage medium for storing the user's fingerprint information, a display and a speaker as output devices, a controller/authenticator for verifying an authorized user by a comparison with the stored fingerprints and the captured fingerprint, and upon a successful match, the output device provide a vidual [sic] indication with LED light and audibly indicating (i.e., with tone) that the obtained user information is authenticated. Land does not teaches [sic] the authenticated signal is an identification specific digital signature profile. In view of Muller and Lane, one of ordinary skill in the art would

not have been motivated to modify the teachings of Muller and Lane in order to obtain a portable identification system having a generator employing the code generating algorithm to transform the access code into an identification specific digital signature profile when the determination of user is made, as set forth in the claims.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

60.   After conducting the searches for prior patents and publications, the USPTO examiners identified references considered relevant to the examination of the '391 Patent, which are identified on the '391 Patent.

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

- U.S. Patent No. 4,148,012 to Baump et al;

- U.S. Patent No. 4,218,738 to Matyas et al;

- U.S. Patent No. 4,264,782 to Konheim;

- U.S. Patent No. 4,315,101 to Atella;

- U.S. Patent No. 4,438,824 to Mueller-Schloer;

- U.S. Patent No. 4,630,201 to White;

- U.S. Patent No. 4,804,825 to Bitoh;

- U.S. Patent No. 4,825,050 to Griffith et al;

- U.S. Patent No. 4,827,518 to Feustal et al;

- U.S. Patent No. 4,961,229 to Takahashi;

- U.S. Patent No. 4,993,068 to Piosenka et al;

- U.S. Patent No. 4,998,279 to Weiss;

- U.S. Patent No. 5,151,684 to Johnsen;

- U.S. Patent No. 5,276,444 to McNair;

- U.S. Patent No. 5,313,556 to Parra;

- U.S. Patent No. 5,386,103 to DeBan et al;

- U.S. Patent No. 5,513,272 to Bogosian, Jr;

- U.S. Patent No. 5,552,777 to Gokcebat et al;

- U.S. Patent No. 5,581,630 to Bonneau, Jr;

- U.S. Patent No. 5,594,493 to Nemirofsky;

- U.S. Patent No. 5,623,552 to Lane;

- U.S. Patent No. 5,793,027 to Baik;

- U.S. Patent No. 5,815,658 to Kuriyama;

- U.S. Patent No. 5,825,871 to Mark;

- U.S. Patent No. 5,825,882 to Kowalski et al;

- U.S. Patent No. 5,870,724 to Lowlor et al;

- German Patent Document No. 3731773 (DE);

- Japanese Patent Document No. 4-135293 (JP);

- "High-Tech Building Security", Siuru, Bill, *Popular Electronics*, Dec. 1996, pp. 39–42, 46;

- "Who Goes There?", Wyner, Peter, *Byte*, vol. 22, No. 6, Jun. 1997, pp. 70–80;

- "No Place to Hide", Marsh, Ann, *Porhes*, Sep. 22, 1997, pp. 226–234;

- "The Generation Gap", Vesley, Rebecca, *Wired*, Oct. 1997, pp. 53–56, 207; and

- "Look. Forward", *Internet User Magazine*, Summer 1997, pp. 11, 12, 14, 21.

62.   As noted by the United States Patents, foreign patent documents, and other publications

cited by the '391 Patent, the claimed inventions of the '391 Patent do not preempt the field of its

invention or preclude the user of other electronic personal identification systems. Instead, the

claims of the '391 Patent cover very specific technologies used on specialized devices (*e.g.,* the

use of a code generator after verifying and determining a user's authorization based on data derived

from biometric or other distinctive characteristics of the user, as claimed, employing the code

generating algorithm to generate one or more access codes based upon an identification profile

wherein at least one of the generated access codes is an identification specific digital signature)

while leaving open other known or unknown technology for identifying a user.

63.   Many means and methods exist for portable electronic personal identification not covered

by the claims of the '391 Patent. The art cited by the Examiners in the examination of the '391

Patent all represent patentably distinct and in some instances prior art means and methods for

electronic personal identification from those of the '391 Patent.

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

64.   Vindolor incorporates by reference and alleges all of the foregoing paragraphs of this

Complaint as if fully set forth herein.

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

customers.

66.   Within its retail establishments, Defendant has operated contactless point of sale terminals

("POS terminals") and has accepted payments using at least one of Microsoft Wallet, Wells Fargo

Wallet, Masterpass, Samsung Pay, Android Pay, Google Pay, Google Wallet, Apple Pay, and

PayPal mobile.
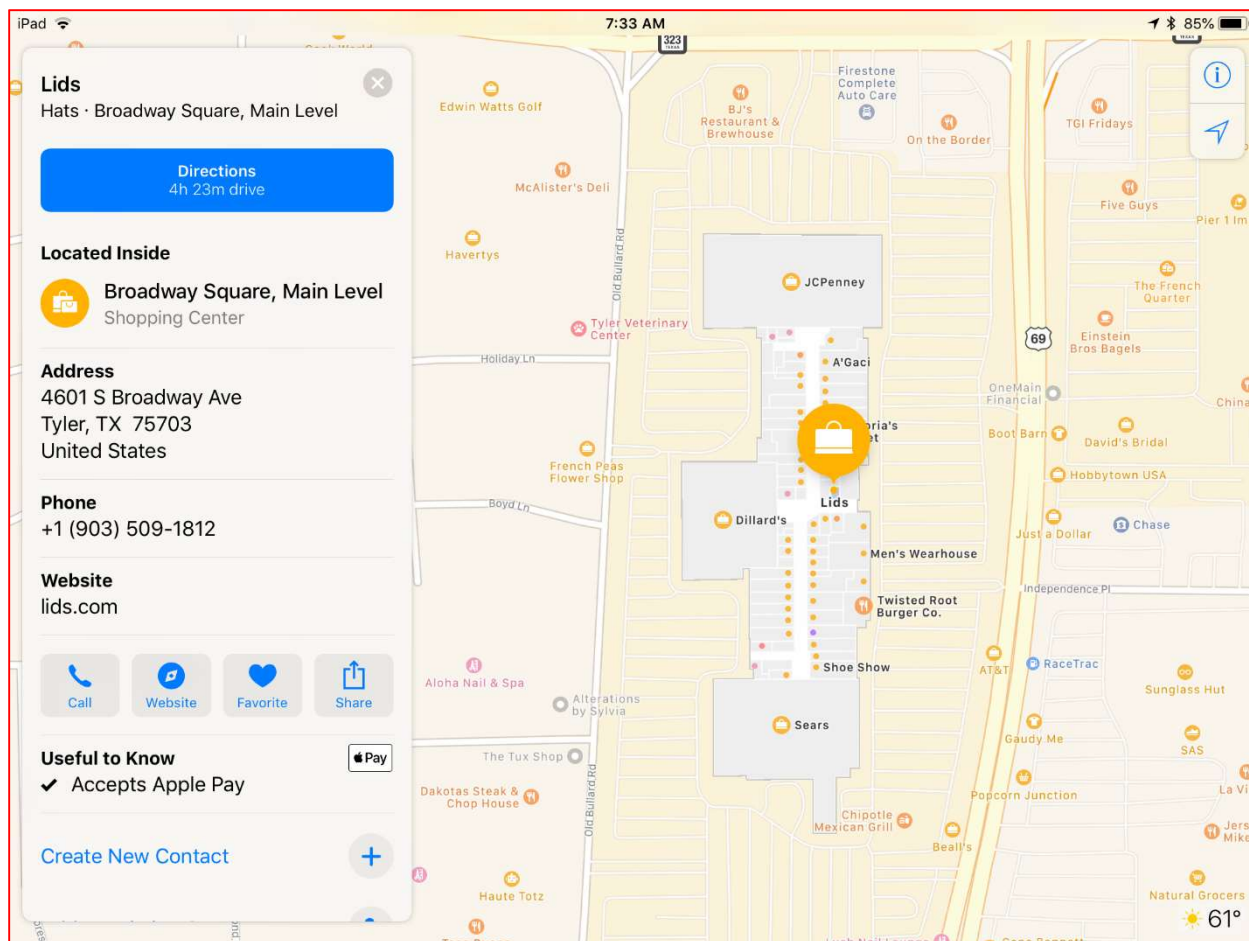
67.   Prior to September 10, 2017, Defendant tested and used portable identification systems in the United States. Such devices include:

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

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

(c)   Apple based phones and mobile devices (*e.g.* the Apple iPhone 6, and iPhone 6+)

installed with the PayPal Mobile App, the Apple Wallet, or the Apple Pay App.

(collectively "Accused Infringing Devices").

68.   The Accused Infringing Devices are non-limiting examples that were identified based on publicly available information, and Vindolor reserves the right to identify additional infringing activities, products and services, including, for example, on the basis of information obtained during discovery. For example, there are additional manufacturers and/or models of Windows based mobile devices that were installed with the Microsoft Wallet App, also there are additional manufacturers and/or models of Android based mobile devices that were installed with the PayPal Mobile App, the Wells Fargo Wallet App, the Masterpass App, the Google Wallet App, the Android Pay App, the Google Pay App, or the Samsung Pay App, and there are additional models of Apple based mobile devices that were installed with the PayPal Mobile App, the Apple Wallet, and the Apple Pay App.

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

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

71.   Defendant used POS terminals within retail establishments to process credit transactions with the Accused Infringing Devices using contactless technology. The contactless technology includes Near Field Communication technology. The contactless technology also includes Magnetic Secure Transmission (MST) technology, which allows the terminals to operate and accept payments using Accused Infringing Devices, including Samsung Pay devices, such as the accused Samsung Galaxy S6, even if the NFC functionality of the POS terminal is not enabled.

72.   Defendant used POS terminals within retail establishments to process credit transactions with the Accused Infringing Devices using both MST and NFC technology.

73.   As described in more detail below, Defendant used the Accused Devices by controlling the operation of the Accused Devices either directly or indirectly (including the operation of each claimed element of the Accused Device), and benefited from each and every element of the Accused Devices.

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

75.   The Accused Infringing Devices are portable devices that implement a portable identification system wherein the system comprises a storage medium for storing electronic data; one or more inputs; one or more outputs; a verifying means for determining user authorization or non-authorization, said verifying means receiving data from at least one of said one or more inputs, which data is derived from biometric or other distinctive characteristics of the user, said verifying means generating an identification profile for each user, wherein said identification profile is determined from said data, and a code generator employing at least one code generating algorithm for generating one or more access codes based upon said identification profile wherein at least one of the said one or more access codes is an identification specific digital signature.

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

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

1(a) A portable identification system comprising: –

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

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

the Apple Pay service.

80.   With the iPhone 6 configured with a customer's credit card account, Defendant has

initiated a credit card transaction with use of a NFC-enabled credit card payment terminal ("POS

terminal") and a connection to a credit card processing server.

81.   The iPhone 6 includes Touch ID, which provides biometric fingerprint identification,

authorization, and verification for Apple Pay.

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

83.   As supported by the disclosures of Apple, the iPhone 6 is a portable identification system.
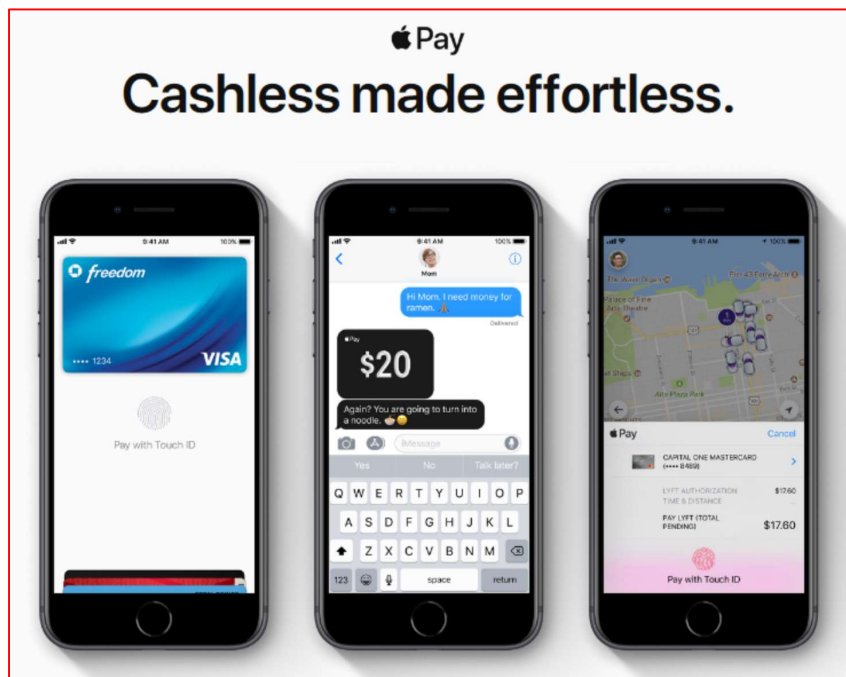
"Cashless   made   effortless"   ("**Cashless   Made   Effortless**"),   *available   at*

https://www.apple.com/apple-pay/ (last accessed April 9, 2018).
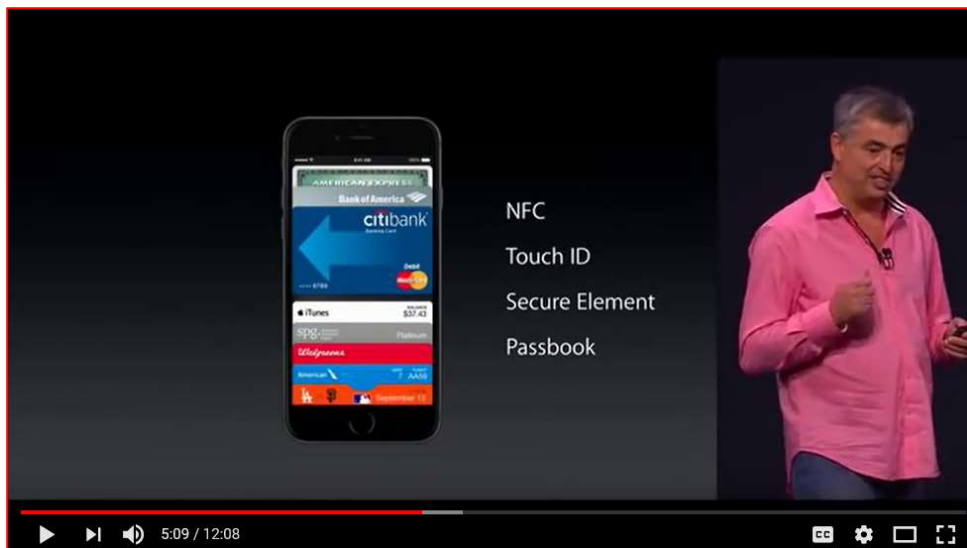
"Apple Pay Presentation (Sept 2014)" ("**Apple Pay Presentation**"), *available at*

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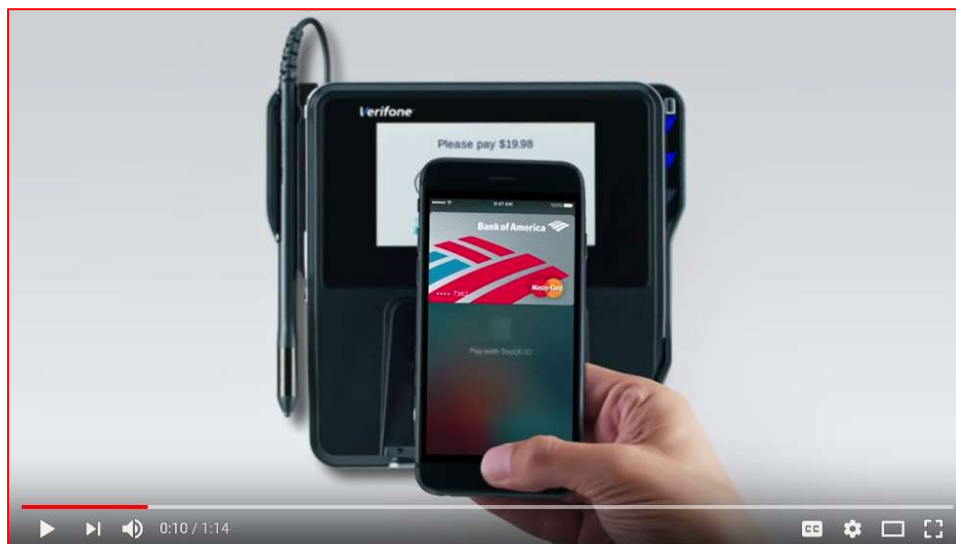
"iPhone – Guided Tour: Apple Pay" ("**iPhone – Guided Tour: Apple Pay**"), *available at*

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

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

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

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

Id.

iOS Security at 7.
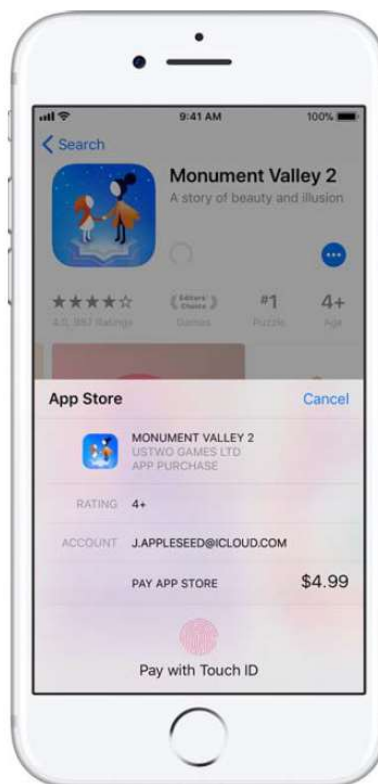
Use Touch ID.

Weight and Dimensions[2]

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

Technical Specifications.

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

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

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

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

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

Capacity[1]

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

Technical Specifications.

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

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

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

iOS Security at p. 7.

> ## Secure Enclave
>
> The chip in your device includes an advanced security architecture called the Secure Enclave, which was developed to protect your passcode and fingerprint data. Touch ID doesn't store any images of your fingerprint, and instead relies only on a mathematical representation. It isn't possible for someone to reverse engineer your actual fingerprint image from this stored data.
>
> Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave. Your fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data. It can't be accessed by the OS on your device or by any applications running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases.

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

> *1(c) one or more inputs; –*

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

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

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

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

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

External Buttons and Connectors

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

Technical Specifications.

Sensors

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

Id.

Cellular and Wireless

- **Model A1549 (GSM)*/ Model A1522 (GSM)***

  - UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - GSM/EDGE (850, 900, 1800, 1900 MHz)
  - LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29)

- **Model A1549 (CDMA)*/ Model A1522 (CDMA)***

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

  Model A1586*/ Model A1524*

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

- **All models**

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

Id.

About Touch ID advanced security technology

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

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

About Touch ID.

Advanced technologies

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

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

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

Id.

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

Apple Pay Security.

When you pay using Apple Pay in stores

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

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

Id.

    1(d) one or more outputs; –

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

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

Display

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

Technical Specifications.

Cellular and Wireless

- **Model A1549 (GSM)*/ Model A1522 (GSM)***

  - UMTS/HSPA+/DC–HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  - GSM/EDGE (850, 900, 1800, 1900 MHz)
  - LTE (Bands 1, 2, 3, 4, 5, 7, 8, 13, 17, 18, 19, 20, 25, 26, 28, 29)

- **Model A1549 (CDMA)*/ Model A1522 (CDMA)***

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

Model A1586*/ Model A1524*

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

- **All models**

  - 802.11a/b/g/n/ac Wi–Fi
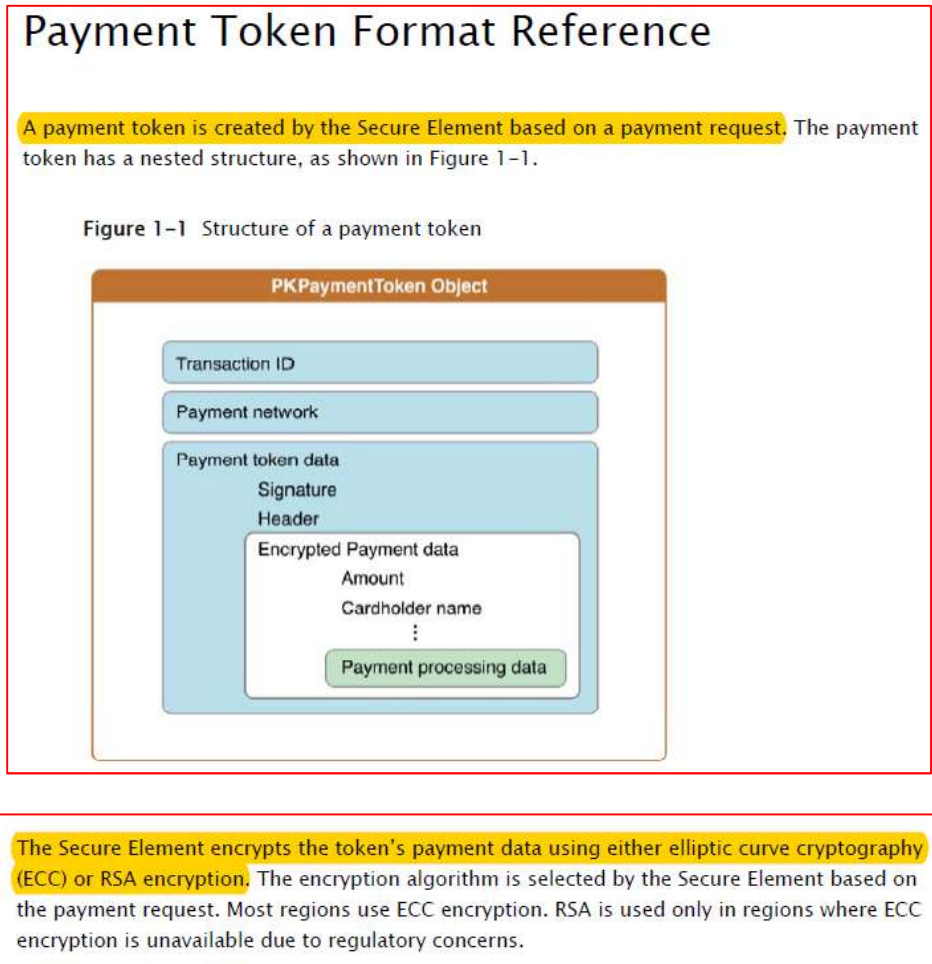 - Bluetooth 4.2 wireless technology
  - NFC

Id.

Transaction-specific dynamic security code

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

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

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

iOS Security at p. 38.

Payment Token Format Reference

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

Figure 1–1 Structure of a payment token

PKPaymentToken Object

Transaction ID

Payment network

Payment token data
  Signature
  Header
  Encrypted Payment data
    Amount
    Cardholder name
    ⋮
    Payment processing data

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

"Payment Token Format Reference" ("**Payment Token Format Reference**"), *available at*

https://developer.apple.com/library/content/documentation/PassKit/Reference/PaymentTokenJS

ON/PaymentTokenJSON.html (last accessed April 9, 2018).

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

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

96.   When a user makes a purchase with Apple Pay using the iPhone 6, the user can use Touch

ID to authorize the purchase.

AMENDED COMPLAINT   39

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

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

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

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

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

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

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

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

About Apple Pay

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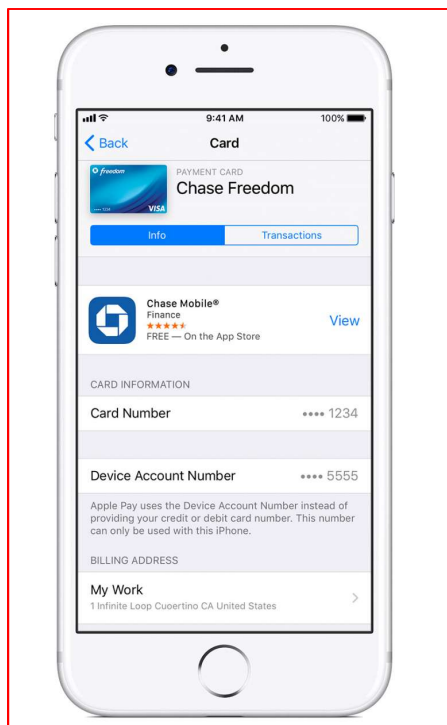
How secure is Apple Pay?

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

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

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

iOS Security at p. 7.

About Touch ID advanced security technology

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

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

About Touch ID.

Advanced technologies

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

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

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

Id.

Secure Enclave

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

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

Id.

Apple Pay components

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

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

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

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

iOS Security at p. 34.

How Apple Pay uses the Secure Element

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

Id.

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

Apple Pay Security.

When you pay using Apple Pay in stores

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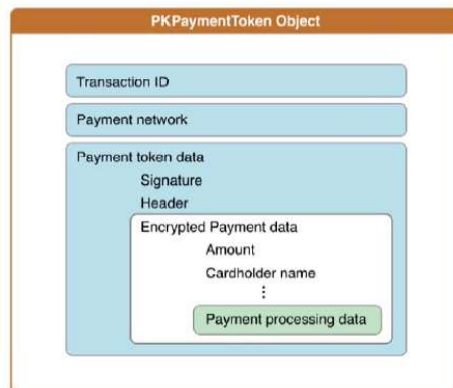
After you use Touch ID or enter your passcode on iPhone, or double-click the side button on Apple Watch at a payment terminal, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code. This information is sent along with additional information needed to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

Id.

Payment Token Format Reference

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

Figure 1-1   Structure of a payment token

PKPaymentToken Object

Transaction ID

Payment network

Payment token data
Signature
Header
Encrypted Payment data
Amount
Cardholder name
⋮
Payment processing data

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

Payment Token Format Reference.

Credit, debit, and prepaid card provisioning

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

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

Full card numbers aren't stored on the device or on Apple servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS and watchOS, is never stored on Apple servers, and is never backed up to iCloud.

iOS Security at p. 35.

> **Transaction-specific dynamic security code**
>
> All payment transactions originating from the payment applets include a transaction-specific dynamic security code along with a Device Account Number. This one-time code is computed using a counter that is incremented for each new transaction, and a key that's provisioned in the payment applet during personalization and is known by the payment network and/or the card issuer. Depending on the payment scheme, other data may also be used in the calculation of these codes, including the following:
>
> - A random number generated by the payment applet
> - Another random number generated by the terminal—in the case of an NFC transaction or
> - Another random number generated by the server—in the case of transactions within apps
>
> These security codes are provided to the payment network and the card issuer, which allows them to verify each transaction. The length of these security codes may vary based on the type of transaction being done.

Id. at p. 38.

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

Id. at p. 37.

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

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

106.   The AR is generated in the Secure Enclave when the user first provisions a credit card and

is persisted while Apply Pay is enabled.

107.   All payment transactions originated from the iPhone 6 using Apple Pay include a

transaction specific dynamic security code with a Device Account Number ("DAN").

108.   This dynamic security code is a one-time code and is computed using a counter that is

incremented for each new transaction and a key that is provisioned in the payment applet during

personalization and is known by the payment network and/or card issuer.

109.   The AR generated by the Secure Enclave is used in the generation of these dynamic

security codes.

110.   A random number generated by the NFC POS terminal is also used in the generation of

these dynamic security codes.

111.   These dynamic security codes are provided to the payment network and the card issuer,

which allows the payment network and card issuer to verify each transaction.

112.   As supported by the disclosures of Apple, Secure Element is a code generator that employs

a code generating algorithm for generating an access code based upon the user's identification

profile, which includes the provisioned key.   The dynamic security code is an identification

specific digital signature.

When you pay using Apple Pay in stores

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

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

Apple Pay Security.

Payment Token Format Reference

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

Figure 1–1 Structure of a payment token

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

Payment Token Format Reference.

Credit, debit, and prepaid card provisioning

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

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

Full card numbers aren't stored on the device or on Apple servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS and watchOS, is never stored on Apple servers, and is never backed up to iCloud.

iOS Security at p. 35.

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

Id. at p. 37.

AMENDED COMPLAINT   49

Transaction-specific dynamic security code

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

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

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

Id. at p. 38.

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

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

Elyse Betters | 4 October 2017

POCKET-LINT
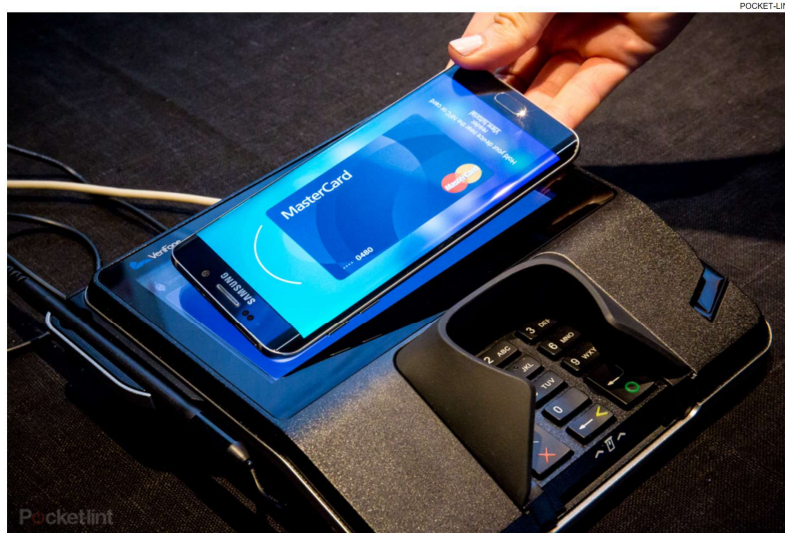
Samsung Pay: More than NFC

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

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

"What is Samsung Pay, how does it work, and which banks support it?" ("**What is Samsung Pay**")

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

How does Google Wallet/Android Pay work?

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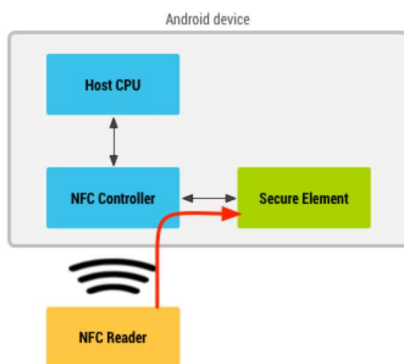
Card Emulation with a Secure Element (Source: *developer.android.com*)

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

"Microsoft Wallet: FAQ" ("**Microsoft Wallet**"), at p. 3, *available at* https://www.co-opfs.org/media/microsoft_wallet_b2b_faq.pdf (last access April 4, 2018).

"Wells Fargo Wallet" ("**Wells Fargo Wallet**"), *available at* https://www.wellsfargo.com/mobile-payments/wells-fargo-wallet/ (last accessed April 9, 2018).

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

Samsung Pay

Credit: Samsung

What it is: Samsung Pay is Samsung's answer to Apple Pay, and unlike its competitors, it works with just about any POS system. Samsung Pay works not only with NFC, but also with standard magnetic-stripe retail terminals featuring MST (Magnetic Secure Transmission) and EMV (Europay MasterCard Visa) readers, currently used for traditional and chip-based credit card transactions.

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

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

2018).

AMENDED COMPLAINT   53
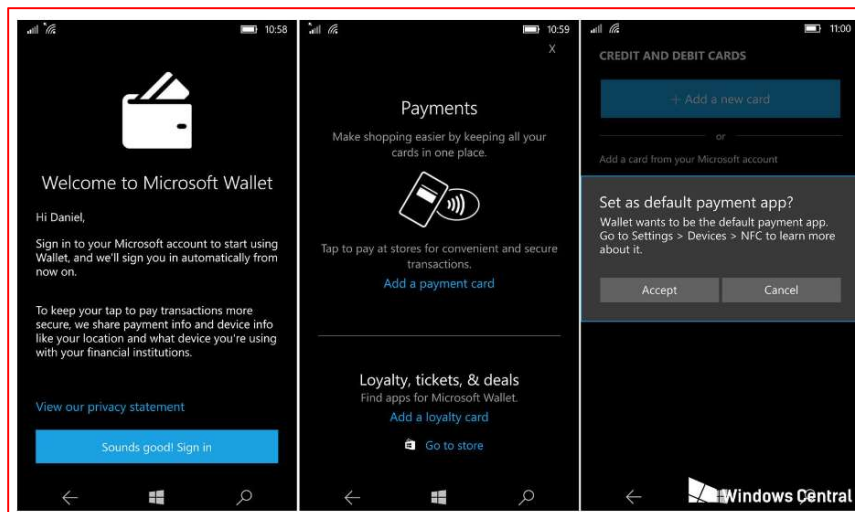
"NFC Tap to Pay is coming to Windows 10 Mobile with Microsoft Wallet 2.0" ("**NFC Tap to Pay**"), *available at* https://www.windowscentral.com/nfc-tap-pay-coming-windows-10-mobile (last accessed April 9, 2018).
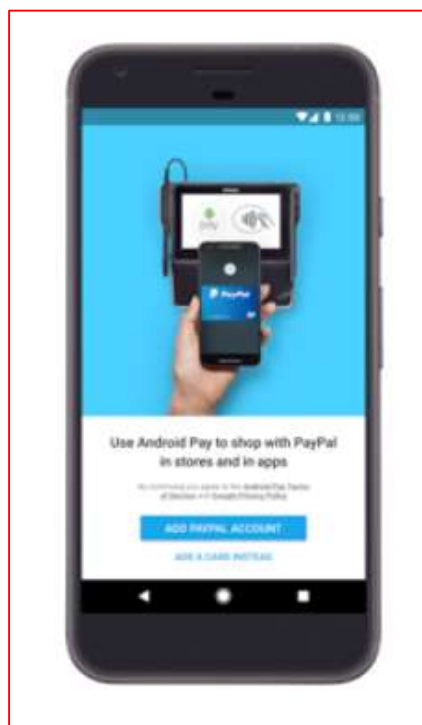
"PayPal teams up with Android Pay for mobile payment" ("**PayPal teams up with Android**"), *available at* https://techcrunch.com/2017/04/18/paypal-teams-up-with-android-pay-for-mobile-payments/ (last accessed April 9, 2018).

AMENDED COMPLAINT   54

Direct Infringement by Testing

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

115.   On information and belief, Defendant has tested the operation of its point of sales systems with an Accused Infringing Device prior to the expiration of the '391 Patent. Based on this actual use of at least one Accused Infringing Devices, Defendant infringed the '391 Patent.[1]

Direct Infringement by Putting Accused Devices Into Service

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

117.   In the operation and control of the POS terminal, Defendant exercised control of the Accused Infringing Devices by issuing commands from the POS terminal to the Accused Infringing Devices to initiate and control the generation of a response from the Accused Infringing Devices, which included an authorization code necessary to complete a credit transaction. But for the issuance of these commands from the POS terminal, the Accused Infringing Devices could not have been used to purchase goods from Defendant using the Accused Infringing Devices. The Defendant's actions are "use" of the Accused Infringing Devices because, but for Defendant's actions, the Accused Infringing Device would not have been put into service.[2] *Centillion Data Systems, LLC v. Qwest Communications International, Inc.*, 631 F.3d 1279, 1285 (Fed. Cir. 2011).

118.   In the operation and control of the POS terminal in conjunction with the Accused Infringing Devices, Defendant put the Accused Infringing Devices, as claimed in the '391 Patent, as a whole into service for its benefit. For example, sending commands from the POS terminal to initiate the

---

[1] *See also Supra.*
[2] *See also Supra.*

payment process and to cause the claimed elements to operate in order to complete the transaction. But for sending these commands to the Accused Infringing Devices, the Accused Infringing Devices would not generate the appropriate access code needed in order to conduct the credit or debit transaction. As a result of sending these commands to the Accused Infringing Devices, the elements of the Accused Infringing Devices were put into action and as a result generated an appropriate access code needed to complete the sales transaction.

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

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

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

Over Breach" ("**Target Paying \$19 Million to MasterCard**"), *available at*
http://fortune.com/2015/04/16/target-mastercard/ (last accessed April 9, 2018); "Target Offers \$10
Million Settlement In Data Breach Lawsuit" ("**Target Offers \$10 Million Settlement**"), *available
at* https://www.npr.org/sections/thetwo-way/2015/03/19/394039055/target-offers-10-million-
settlement-in-data-breach-lawsuit (last accessed April 9, 2018); "Panerabread.com Leaks Millions
of Customer Records" ("**Panerabread.com Leaks Millions of Customer Records**"), *available
at* https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/
(last accessed April 9, 2018); "Neiman Marcus Reports New Breach" ("Neiman Marcus Reports
New Breach"), *available at* https://www.bankinfosecurity.com/new-neiman-marcus-breach-
authentication-must-change-a-8843 (last accessed April 9, 2018); "5 million credit cards exposed
in Saks and Lord & Taylor data breach" ("5 Million credit cards exposed"), *available at*
https://nakedsecurity.sophos.com/2018/04/03/5-million-credit-cards-exposed-in-saks-and-lord-
taylor-data-breach/ (last accessed April 9, 2018); "This Week In Credit Card News: A Record
Number of Data Breaches; Starbucks Enters Credit Card Market" ("**A Record Number of Data
Breaches**") ("The Identify Theft Resource Center reports the number of U.S. data breaches
reached an all-time high in 2017. Data breaches totaled 1,579, up 45% from 2016. 55% hit the
business sector…"), *available at* https://www.forbes.com/sites/billhardekopf/2018/02/02/this-
week-in-credit-card-news-a-record-number-of-data-breaches-starbucks-enters-credit-card-
market/#1c5af1a07346 (last accessed April 9, 2018); and "Equifax breach exposes data of 147.9
million U.S. consumers") ("**Equifax breach exposes data of 147.9 million**"), *available at*
https://www.creditcards.com/credit-card-news/equifax-data-breach-143-million-id-theft.php (last
accessed April 9, 2018);

122.   When retailers, including Defendant, processed payments using the Accused Infringing Devices, the retailer was able to avoid the data breach problem and liabilities suffered by Home Depot, Target, Neiman Marcus, Saks, Lord & Taylor, and others for transactions using the Accused Infringing Devices because, during such transactions, the retailer never obtained the customers' credit card number. See, *e.g.,* "Unable to target Apple Pay, criminals unsurprisingly stick to bank fraud, identity theft" ("**Unable to Target Apple Pay**"), *available at* https://www.imore.com/unable-target-apple-pay-criminals-unsurprisingly-stick-fraud-identity-theft (last accessed April 9, 2018).

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

https://www.trc-solutions.com/apple-pay-means-retail/ (last accessed April 9, 2018); and "About

Apple   Pay   for   Merchants"   ("**About   Apple   Pay   for   Merchants**"),   *available   at*

https://support.apple.com/en-us/HT204274 (last accessed April 9, 2018).
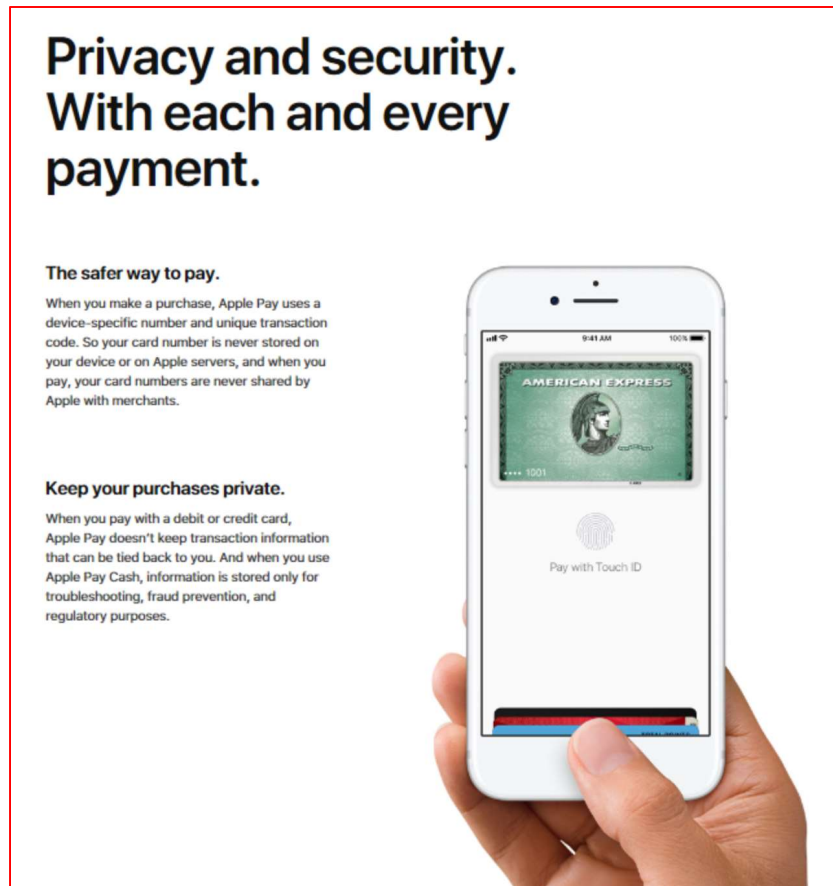
Cashless Made Effortless.

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

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

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

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

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

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

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

completed the transaction approval process by sending the authorization code to a servicing bank. "An Introduction to NFC Standards" ("**Introduction to NFC Standards**"), *available at* http://www.icma.com/ArticleArchives/StandardsOct12.pdf (last accessed April 9, 2018); "NFC Standards" ("**NFC Standards**"), *available at* http://www.themobileknowledge.com/wp-content/uploads/2017/05/NFC-Standards.pdf (last accessed April 9, 2018); "NFC Essentials" ("**NFC Essestials**"), *available at* http://www.themobileknowledge.com/wp-content/uploads/2017/05/NFC-Essentials-v2.0.1.pdf (last accessed April 9, 2018); "Smart Card Technology FAQ" ("**Smart Card Technology**"), *available at* http://www.smartcardalliance.org/smart-cards-faq/ (last accessed April 9, 2018).

125.   The interchange of commands issued from the POS terminal to the Accused Infringing Devices and responses to the commands received from the Accused Infringing Devices to the POS terminal is specified, in part, according to the ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 18092, and ISO/IEC 21481 standards. *Id.*
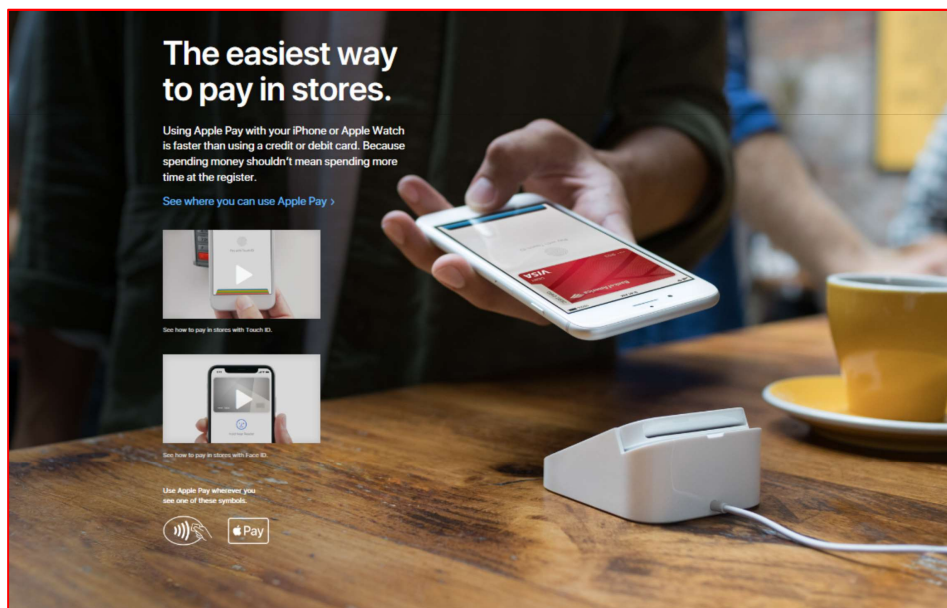
Cashless Made Effortless.
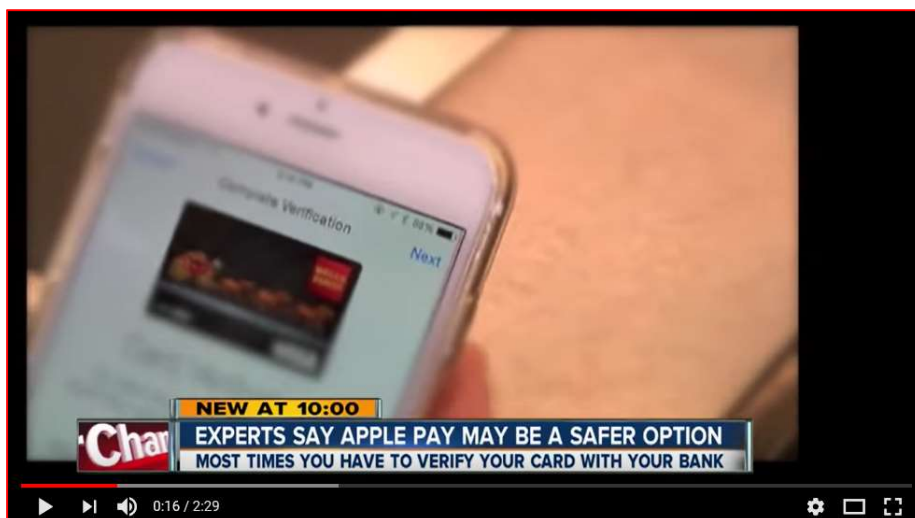
"Which is safer: Apple Pay or credit cards?" ("**Which is safer**"), *available at* https://www.youtube.com/watch?v=06ZWlNuaeMM&t=16s (last accessed April 9, 2018).
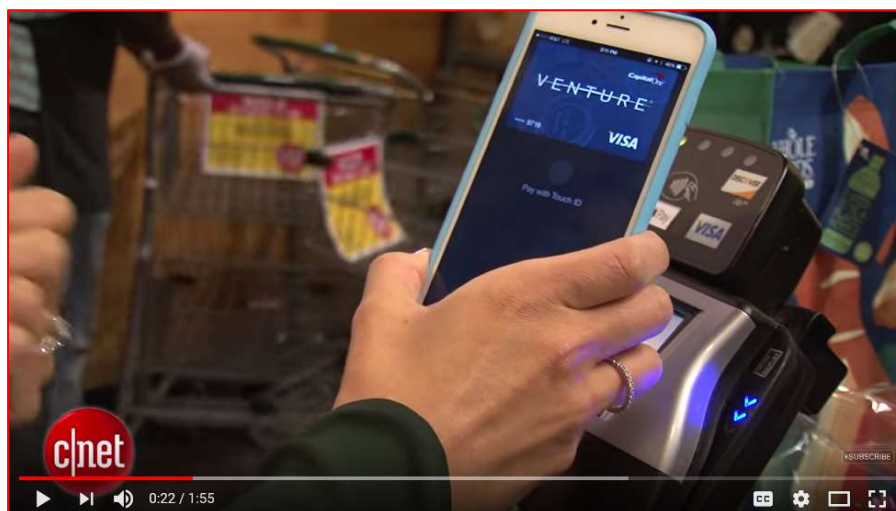
"Apple Pay is the most secure way to pay, with a catch" ("**Apple Pay is the most secure way to pay**"), *available at* https://www.youtube.com/watch?v=9-f4rdSq2QY (last accessed April 9, 2018)

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

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

- authenticating the identity of the user, which reduced fraudulent charges and charge backs and allowed the customer to complete the transaction;

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

- more secure transactions, which reduced fraud and lowered transaction costs with credit servicing companies and prevented fraudulent transactions on customers' accounts;

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

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

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

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

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

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

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

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

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

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

1(a) A portable identification system comprising: –

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

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

132.   The Defendant benefitted through the use of the Accused Infringing Devices because the Defendant did not receive the customers' credit card number, thereby alleviating the Defendant

from liability associated with data breaches, identity theft, fraud, and possible charge backs from the bank servicing the credit card transactions.

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

134.   The Defendant controlled the use of Accused Infringing Devices by issuing commands from the POS terminal to the Accused Infringing Devices, which caused the Accused Infringing Devices to respond to the commands ultimately resulting in the generation of an authorization code that allowed the Defendant to complete a credit or debit card transaction.

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

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

136.   By storing the instructions for how to respond to commands issued from the POS terminal, the Accused Infringing Devices were able to process the commands and cause additional elements, such as the code generator, to be put into service and generate an access code that was used to complete the sales transactions. As such, the storage medium directly benefited Defendant because but for the storage medium storing these instructions, the Accused Infringing Devices would not be able to process and respond to the commands issued by the POS terminal.

137.   Without the use of a storage medium in the Accused Infringing Devices, the Defendant would have been prohibited from processing a credit transaction needed to process and profit from the sales transaction and to receive the Asserted Benefits.

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

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

140.   The Defendant controlled the use of the storage medium by issuing commands from the POS terminal to the Accused Infringing Devices, which caused the Accused Infringing devices to store received commands in the storage medium, to read instructions from the storage medium for how to respond to incoming commands from the POS terminal, to read profile information that is stored in the storage medium in order to generate an identification specific digital signature, and to store the generated identification specific digital signature so that it could be then transmitted back to the POS terminal.

        1(c) one or more inputs; –

141.   The Defendant benefited from the use of one or more inputs in the Accused Infringing Devices.   The one or more inputs (e.g. NFC radio receiver) allowed the Accused Infringing Devices to receive commands from the POS terminal to initiate and process credit transactions for the sale of goods from Defendant.   The use of the one or more inputs in the Accused Infringing Devices directly benefitted Defendant by allowing the Accused Infringing Devices to receive the initiating commands from the POS terminal in order to start the identification and authorization process, which is needed to complete a sale.   But for the one or more input devices, the Accused

Infringing Device would not be able to receive the initiating commands from the Defendant's POS terminal. As a result of the one or more inputs receiving commands from Defendant's POS terminal, the commands are received by the Accused Infringing Devices to put into service the other elements of the claim. As a result, Defendant benefited from the use of the one or more inputs because of the one or more inputs produced the result of causing other elements of the Accused Infringing Devices to operate and be put into service. As a result of Defendant's use of the one or more inputs, Defendant was able to control the operation of the Accused Infringing Devices including the additional claimed elements, thus benefiting Defendant. As a result of Defendant's use of the one or more inputs, Defendant was able to receive an authorization code from the Accused Infringing Device, which was necessary in order to complete the customer's purchase.

142.   The one or more inputs (e.g. NFC radio receiver) allowed the Accused Infringing Devices to receive and process commands from the Defendant's POS terminal in order to generate the required access coded required in order for Defendant to process and profit from the credit/debit transaction for the sale of goods from the Defendant, thereby benefiting the Defendant.

143.   Additional inputs (e.g. biometric fingerprint reader) allowed the Accused Infringing Devices to verify the identity of the authorized account holder to approve the transaction from the sale of goods from the Defendant.

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

145.   With the use of the one or more inputs (e.g. touch screen and fingerprint reader) in the Accused Infringing Devices, the verification means element in the Accused Infringing Devices

was able to operate to authorize the credit transaction for the sale goods from the Defendant, thereby benefiting the Defendant.

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

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

148.   The Defendant controlled the inputs in the Accused Infringing Devices by transmitting commands from the POS terminal to the Accused Infringing Devices, causing the NFC radio receiver to receive RF signals and decode the RF signals into a digital representation and causing the NFC radio to send the digital signals to the processing circuitry within the Accused Infringing Devices.

149.   The defendant also controlled the inputs in the Accused Infringing Devices by transmitting commands from the POS terminal to the Accused Infringing Devices, causing the touch screen input and fingerprint reader to operate to receive data in order to receive data necessary for the verification means authorize the identity of the person wishing to purchase items from the Defendant.

1(d) one or more outputs; –

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

151.   The use of the one or more outputs in the Accused Infringing Devices directly benefitted Defendant by allowing the Accused Infringing Devices to communicate with the Defendant's POS

terminal, which is needed to complete a sale. But for the one or more output devices, the Accused

Infringing Device would not be send the generated access code to the Defendant's POS terminal.

152.   The one or more outputs allowed the Accused Infringing Devices to transmit to the

Defendant the generated access code need to approve and authorize the credit transaction for the

sale of goods from the Defendant, thereby benefiting the Defendant.

153.   Without the use of the one or more outputs in the Accused Infringing Devices, the

Defendant would have been prohibited from processing a credit transaction to receive profit from

the sales transaction and the Asserted Benefits.

154.   Without the use of the one or more outputs in the Accused Infringing Devices, the

Defendant would not have been able to receive the appropriate authorization code to authorize and

complete the credit transaction for the sale goods from the Defendant.

155.   With the use of the one or more outputs in the Accused Infringing Devices, the Defendant

was able to prevent a fraudulent sales transaction, thereby benefiting the Defendant.

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

Benefits.

157.   The Defendant controlled the use of the one or more outputs in the Accused Infringing

Devices. The one or more outputs (e.g. NFC radio transmitter)

158.   The Defendant controlled an output (e.g. display) in the Accused Infringing Devices by

transmitting commands from the POS terminal to the Accused Infringing Devices, causing the

display in the Accused Infringing Device to display instructions and information to the user in

response to the transmitted commands from the POS terminal.

159.   The Defendant also control an output (e.g. NFC radio transmitter) in the Accused

Infringing Devices by transmitting commands from the POS terminal to the Accused Infringing

Devices, causing the NFC radio transmitter to transmit a response back to the POS terminal, including a response with an authorization code used to complete the credit or debit transaction.

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

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

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

162.   Without the use of the verifying means element in the Accused Infringing Devices, the Accused Infringing Devices would not have generated the access code required by Defendant for processing the sales transaction with customer. As a result, Defendant would have been prohibited from processing a credit transaction to receive the Asserted Benefits.

163.   Without the use of the verifying means element in the Accused Infringing Devices, the Accused Infringing Devices would not be able to respond to the commands received from the Defendant's POS terminal in order to generate the appropriate access code needed to complete the transaction and profit from the transaction.

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

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

166. With the use of the verifying means element, the Defendant was able to realize profits from the sales transaction and the Asserted Benefits.

167. With the use of the verifying means element in the Accused Infringing Devices, the Defendant was able to cause the code generator in the Accused Infringing Devices to generate an access code based on an identification profile that was generated by the verifying means. By generating the access code, the Defendant was able to realize the Asserted Benefits.

168. The Defendant controlled the use of the verifying means by issuing commands from the POS terminal to the Accused Infringing Devices, which caused elements of the verifying means (e.g. Touch ID, Secure Element, and Secure Enclave) to process data to verify the user authorization or non-authorization. The commands issued from the POS terminal also control and cause components of the verifying means (e.g. Secure Element and Secure Enclave) to generate an identification profile, which is determined from data received from the input sources.

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

169. The Defendant benefited from the use of the code generator in the Accused Infringing Devices. The code generator allowed the Accused Infringing Devices to generate an access code that was transmitted to the POS terminal that was required in order for Defendant to process the credit transaction for the sale of goods from the Defendant identify the authorized account holder for the credit transaction for the sale of good from the Defendant.

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

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

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

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

174.   The Defendant controlled the use of the code generator by issuing commands from the POS terminal to the Accused Infringing Devices, which cause the code generator in the Accused Infringing Devices to generate an access code that was transmitted back to the POS terminal via the NFC radio transmitter.

**Direct Infringement by Conditioning the Participation in
Use of The Accused Infringing Devices**

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

176.   The Defendant and its customers share a retailor-customer relationship.   In this relationship, the Defendant sells goods to its customers for a monetary benefit. When completing a sales transaction with use of the Accused Infringing Devices, Defendant and its customers are able to generate an authorization access code that is sent to a banking processing center. When an authorized access code is approved by the banking processing center, the sales transaction between the Defendant and the customer is completed, wherein the customer receives the goods and Defendant receives a financial benefit, including profit from the sale.

177.   When Defendant's customers purchased goods, Defendant directed and controlled the manner and timing of the use of the Accused Infringing Devices in the process of completing credit

transactions.[3] Defendant profited from the direct infringement of the use of the Accused Infringing

Devices and had a right and ability to stop or limit that infringement. As a result, Defendant is

liable as a direct infringer. *Akamai Technologies, Inc. v. Limelight Networks, Inc. (Akamai V),* 797

F.3d 1020, 1023 (Fed. Cir. 2015) (en banc).

178.   The Defendant, with the use of the POS terminal, initiated communications from the POS

terminal to the Accused Infringing Devices with commands to initiate functions and operations

within the device.

179.   The timing of sending the commands from the Defendant's equipment to the Accused

Infringing Devices was timed to occur only after determining the amount of sale for goods the

customer wanted to purchase and when Defendant issued instructions to the point of sale

equipment to communicate with the Accused Infringing Devices. Upon receiving commands from

the POS terminal, the Accused Infringing Devices verified the identity of the customer as an

authorized person to approve the credit transaction, generated an authorization code and

transmitted the authorization code back to the POS terminal as requested from the POS terminal.

180.   The Defendant then transmitted the authorization code to a bank servicing partner for

final approval of the sale. Upon receiving approval from the bank servicing partner, the Defendant

completed the sale with the customer.

181.   But for Defendant sending these commands to the Accused Infringing Devices, the

Accused Infringing Devices would not operate to generate the required access code needed by

Defendant in order to process the sale of goods, and without the issuance of these commands,

Defendant's customers could not complete a sales transaction using the Accused Infringing

Devices. Without the Defendant's actions, directions, and control, the Defendants' customers

---

[3] *See also Supra.*

would not have been able to use the Accused Infringing Devices to purchase goods from the Defendant.

182.   In this process, the Defendant conditioned the sale to the customer based on the customer using the Accused Infringing Device as directed by Defendant's actions of having the point of sale terminal issue commands to the Accused Infringing Devices in order to verify the customer's identity. If the customer failed to verify their identity with the Accused Infringing Devices, the Defendant did not process the credit transaction using the Accused Infringing Device.

183.   As a result of conditioning the use of the Accused Infringing Devices in order to complete a sales transaction, as noted above, Defendant benefited and profited from the sales transactions with its customers and the use of the Accused Infringing Devices.

184.   During the process of conducting the sales transaction, Defendant is aware of the use of the Accused Infringing Devices to generate a requested authorization code in order to approve the credit transaction.

185.   On information and belief, Defendant advertised, promoted, and fostered the use of the Accused Infringing Devices to generate a requested authorization code in order to approve credit transactions for the sale of goods to customers.

186.   Defendant the right and ability to stop, limit, and refuse to allow the use of the Accused Infringing Devices to complete a sales transaction in its stores. Defendant benefited from the use of the Accused Infringing Devices and did not exercise the right to stop, limit, or refuse to allow the use of the Accused Infringing Devices to complete sales transactions using the Accused Infringing Devices.

187.   By controlling whether the Accused Infringing Devices may be used or not used in a sales transaction, by controlling the timing of any use of the Accused Infringing Devices to complete a

sales transaction, by controlling the timing and initiation of commands sent to the Accused Infringing Devices to generate the access code needed to complete the sales transaction, the Defendant is responsible for all actions of the customers to complete the sales transaction using the Accused Infringing Devices. Accordingly, any and all actions taken by a customer in the sales transaction with the Accused Infringing Devices in order to complete the sales transaction, are attributable to the Defendant.

Direct Infringement by Actions of a Joint Enterprise

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

189.   Defendant has acted alone and in concert with others, including its customers, and is otherwise liable jointly, severally or otherwise for a right to relief related to or arising out of the same transaction, occurrence or series of transactions or occurrences related to using at least one of the Accused Infringing Devices. *Akamai*, 797 F.3d 1023. In so doing, Defendant has formed a joint enterprise with its customers when it participated in the payment for goods using the Accused Infringing Devices as described in detail above.[4] For doing so, Defendant is liable as a direct infringer out of the actions of the joint enterprise.

190.   Defendant and its customers (1) have an agreement, express or implied, between the Defendants and its customers; (2) have a common purpose to be carried out by the Defendant and the Defendant's customers; (3) have a community of pecuniary interest in that purpose; and (4) have an equal right to a voice in the direction of the enterprise, which gives an equal right of control.

---

[4] *See also Supra*.

1.   Agreement with Customers

191.   Defendant and its customers formed an agreement, express or implied, to conduct a sales transaction for the customers' purchase of goods from the Defendant and Defendant's receipt for payment for the goods from the customers. Defendant and its customers also formed an agreement, express or implied, for the use of the Accused Infringing Devices to generate an authorization code that would be used by Defendant to submit the transaction for approval by an appropriate merchant banking service. The Defendant and its customers formed an agreement, express or implied, to charge the customers' credit or debit banking account by using an authorization code generated by the Accused Infringing Devices instead of the credit card or debit card number assigned to the customers' accounts.

2.   Common Purpose

192.   The purpose of the agreements between Defendant and its customers was to complete a sales transaction, wherein the customer would receive goods from the Defendant and Defendant would receive financial payment from its customers. Additionally, the purpose of the agreements to use the Accused Infringing Devices was to do so in a manner that would protect the disclosure of the customers' financial credentials that could be later used for fraudulent purposes. Additionally, the purpose was to perform the sales transaction quickly and efficiently with use of the Accused Infringing Devices.

3.   Community of Pecuniary Interest

193.   Defendant and its customers had a community of pecuniary interest in the purpose of the joint enterprise. The sales transaction between the Defendant and its customers is a financial transaction in which personal identifying information of the customer is shared with Defendant. The Defendant and its customers also had a pecuniary interest in protecting the details of the

financial transaction from disclosure to other parties that could use the information to conduct fraudulent transactions. Such a disclosure would have harmed both Defendant and its customers. The Defendant would have been harmed as a result of incurred liability to banks and its customers for the fraudulent use of the customers' information. The customers would have been harmed as a result of fraudulent charges to its credit or debit accounts. By using the Accused Infringing Devices, Defendant and its customers benefited in the shared pecuniary interest of completing a sales transaction in a manner that protected both from financial losses.

194.   To further this community of pecuniary interest, the Defendant and its customers shared resources. The Defendant provided its POS terminal and infrastructure and the customers provided the Accused Infringing Devices. As a result of pooling these resources, Defendant and its customers achieved and enjoyed joint benefits.[5]

4.   Equal Rights

195.   Defendant and its customers each had a right to voice a direction of the joint enterprise. The choice to conduct a transaction using the Accused Infringing Devices is equally controlled by Defendant and its customers. The Defendant can prevent the use of the Accused Infringing Devices from being used to conduct a sales transaction in its stores by disabling all functionality of its POS terminals. Defendant's customers can prevent the use of the Accused Infringing Devices by not presenting it to the POS terminal to receive the initiating commands from the POS terminal. But for the use of a POS terminal, a sales transaction cannot be completed with the use of an Accused Infringing Device. Additionally, but for the use of the Accused Infringing Devices, a sales transaction cannot be completed with the use of an Accused Infringing Device.

---

[5] *See also Supra.*

196.   By setting the timing conditions and initiating the commands from the POS terminal to the Accused Infringing Devices, Defendant willingly controlled and directed the use of the Accused Infringing Devices. At all times, Defendant had full right and ability to not allow the use of the Accused Infringing Devices to complete a sales transaction.

197.   By providing, configuring, and presenting the Accused Infringing Devices, Defendant's customers willingly voiced a direction in the joint enterprise to use the Accused Infringing Devices to complete a sales transaction. At all times, Defendant's customers had full right and ability to not allow the use of the Accused Infringing Devices to complete a sales transaction.

198.   As a result, both Defendant and its customers had an equal right to voice a direction of the joint enterprise of using the Accused Infringing Devices to conduct a sales transaction.

Damages

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

PRAYER FOR RELIEF

Vindolor respectfully requests the Court enter judgment against Defendant:

1.   declaring that Defendant has infringed the '391 Patent;

2.   awarding Vindolor its damages suffered as a result of Defendant's infringement of the '391 Patent;

3.   awarding Vindolor its costs, attorneys' fees, expenses, and interest; and

4.   granting Vindolor such further relief as the Court finds appropriate.

JURY DEMAND

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

Dated: July 12, 2018   Respectfully Submitted

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

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

                                                         ATTORNEYS FOR PLAINTIFF