

Exhibit A to CardWare’s Preliminary Infringement Contentions
Infringement of U.S. Patent No. 10,339,520

This claim chart is based on publicly available literature. Plaintiff CardWare Inc. (“CardWare”) reserves the right to supplement and/or amend its positions based on discovery from Apple Inc. (“Apple” or “Defendant”), including technical documentation such as schematics and datasheets, and source code.

Apple infringed and continues to infringe U.S. Patent No. 10,339,520 (the “’520 patent”) by making, using, selling or offering for sale, and/or importing into the United States devices implementing a method of storing and generating payment information, covered by one or more claims of the ’520 patent. CardWare’s allegations include all such devices, unless otherwise noted or prohibited by license (“Accused Products”). *See infra* Appendix. Apple has also infringed by performing such methods of storing and generating payment information and/or contributing to and/or inducing infringement by others, for the reasons set forth herein.

To the extent certain acts or steps constituting part of the infringement are performed by another entity besides Apple (*e.g.*, a third party payment processor or token service provider), those acts may be attributed to Apple because Apple and the other entity, or entities, are acting in a joint enterprise with respect to the infringement, or, in the alternative, Apple directs or controls the other entity or entities’ performance, such as by conditioning their participation in the accused system or method on their performance of certain steps and establishing the manner and/or timing of that performance.

Theories exemplifying how the Accused Products infringed and continue to infringe the asserted claims of the ’520 patent are detailed herein. The products included are representative; on information and belief, all Accused Products function in substantially the same manner as one or more of the examples provided, and include generally the same components. CardWare reserves its right to amend these contentions under the procedures set forth in the Standing Order Governing Proceedings (OGP) 4.4 – Patent Cases.

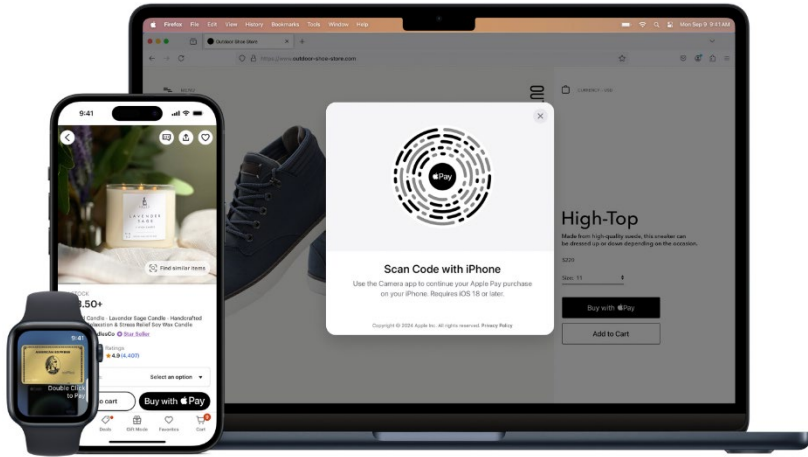
Claim No.	Accused Products
1 [Pre]: An electronic device comprising	To the extent the preamble is limiting, an Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, is an electronic device.  Personal data. Protected. When you make a purchase, Apple Pay uses a device-specific number and unique transaction code. So your card number is never stored on your device or on Apple servers. And when you pay, your card numbers are never shared by Apple with merchants. If you prefer not to share your email address with merchants when paying online, you can use Hide My Email to generate unique, random email addresses that automatically forward to your personal inbox.  In apps and online. Use Apple Pay to seamlessly make purchases in Safari and other browsers — on iPhone, iPad, Mac, and other computers — without the lengthy checkout forms. On an Apple device, click or tap the Apple Pay button and pay with a touch or glance. On a non-Apple device, scan the Apple Pay code with your iPhone camera and use your iPhone to complete your purchase.⁵ You can even use Apple Pay to subscribe to services like Apple Music, Apple News+, and Apple TV+, buy apps and games on the App Store, and upgrade your iCloud storage. At stores and more. Apple Pay is accepted at over 85 percent of retailers in the U.S., so you can likely use it wherever and however you want. If you’re not sure, just ask. Apple Pay works anywhere that takes contactless payments — from vending machines and grocery stores to taxis and subway stations. See, e.g., <i>Apple Pay</i>, Apple, https://www.apple.com/apple-pay/ last visited Dec. 27, 2024; <i>Devices compatible with Apple Pay</i>, Apple (Nov. 22, 2024), https://support.apple.com/en-us/102896; Abby Ferguson, <i>How to set up Apple Pay</i>, Popular Sci. (May 12, 2024 3:04 PM EDT), https://www.popsci.com/diy/how-to-set-up-apple-pay/ (“[The Wallet app] is pre-installed on Apple devices, so you won’t need to install it first.”).

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
1[a] a near-field communication (NFC) unit;	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, includes an NFC unit. 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. [. . .] Paying with cards in stores If iPhone or Apple Watch is on and detects an NFC field and if Apple Wallet is set as the default Payments and Contactless app, the device presents the user with the requested card (if automatic selection is turned on for that card) or the default card from Apple Wallet (which is managed in Settings). The user can also go to Apple Wallet and choose a card or, when the device is locked, can: • Double-click the side button on devices with Face ID (if Apple Wallet is the default app) • Double-click the Home button on devices with Touch ID (if Apple Wallet is the default app) • Using Accessibility features that allow Apple Pay from the Lock Screen [. . .] NFC controller The NFC controller handles NFC protocols and routes communication between the Application Processor and the Secure Element, and between the Secure Element and the point-of-sale terminal. The NFC controller helps ensure that contactless transactions are conducted using a terminal that’s in close proximity to the device. Only requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions. <i>See, e.g., Apple Platform Security</i>, at 177, 184 196, 260 (Dec. 2024) available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; <i>Apple Platform Security, Paying with cards using Apple Pay</i>, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/paying-with-cards-using-apple-pay-secfbd5c0e54/web; <i>Apple Pay component security</i>, Apple (May 13, 2022), https://support.apple.com/guide/security/apple-pay-component-security-sec2561eb018/web; <i>Apple Platform Security, NFC & SE Platform Security</i>, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/nfc-se-platform-security-secda20f3f41/web; <i>see also, e.g., iPhone 16 – Tech Specs</i>, Apple, https://support.apple.com/en-us/121029 (last visited Dec. 29, 2024) (noting that all models have “NFC with reader mode”); <i>Make purchases using Apple Pay</i>, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102626; <i>Apple Watch User Guide – watchOS 11, Make purchases with Apple Pay on Apple Watch</i>, Apple, https://support.apple.com/guide/watch/make-purchases-apdbe9c11bba/watchos (last visited Dec. 29, 2024).

Claim No.	Accused Products
	When you use Apple Pay in stores When you use Apple Pay in stores that accept contactless payments, Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard, contactless technology that’s designed to work only across short distances. If your iPhone is on and detects an NFC field, it will present you with your default card. To send your payment information, you must authenticate using Face ID, Touch ID, or your passcode (except when you use Express Mode with a payment or transit card). With Face ID or with Apple Watch, you must double-click the side button when the device is unlocked to activate your default card for payment. <i>See, e.g., Apple Pay security and privacy overview, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554.</i>
1[b] a touch sensor array;	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, includes a touch sensor array (<i>e.g.</i>, in a touch screen panel). Use Touch Accommodations 1. Go to the Settings app  on your Apple Watch. 2. Go to Accessibility > Touch Accommodations to do any of the following: • <i>Respond to touches of a certain duration:</i> Turn on Hold Duration, then tap the plus or minus buttons to adjust the duration. To perform swipe gestures without waiting for the specified hold duration, tap Swipe Gestures, then turn on Swipe Gestures. You can choose the amount of required movement before a swipe gesture begins. <i>See, e.g., Apple Watch User Guide – watchOS11, Adjust motor skills settings on Apple Watch, Apple, https://support.apple.com/guide/watch/adjust-motor-skills-settings-apdfbb1b0550/watchos (last visited Dec. 29, 2024).</i> If your screen is too sensitive or responds intermittently to touch 1. Restart your iPhone or iPad. 2. Make sure that your screen is clean and free of any debris or water. 3. Disconnect any Lightning or USB-C accessories. If your screen works after removing an accessory, try using a different outlet, cable, or charger. 4. Remove any cases or screen protectors. <i>See, e.g., If the screen isn’t working on your iPhone or iPad, Apple (Oct. 15, 2024), https://support.apple.com/en-us/102567.</i>

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
1[c] a display;	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, includes a display. <i>See supra</i> limitation 1[b]. iPhone 16 Pro Max  6.9" Super Retina XDR display¹ iPhone 16 Pro  6.3" Super Retina XDR display¹ iPhone 16  6.1" Super Retina XDR display¹ <i>See, e.g., Compare iPhone Models</i>, Apple, https://www.apple.com/iphone/compare/ (last visited Dec. 29, 2024).  Apple Watch SE  Retina display Up to 1000 nits  Apple Watch Series 10  Always-On Retina display Up to 2000 nits  Apple Watch Ultra 2  Always-On Retina display Up to 3000 nits [. . .] <i>See, e.g., Watch</i>, Apple, https://www.apple.com/watch/ (last visited Dec. 29, 2024).

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products												
1[d] a motion rate detection array;	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, includes a motion rate detection array (e.g., high dynamic range gyroscope, high-g accelerometer, proximity sensor). iPhone 16 Pro Max  iPhone 16 Pro  iPhone 16  [. . .] [. . .] Sensors <table><tr><td>High dynamic range gyro</td><td>High dynamic range gyro</td><td>High dynamic range gyro</td></tr><tr><td>High-g accelerometer</td><td>High-g accelerometer</td><td>High-g accelerometer</td></tr><tr><td>Proximity sensor</td><td>Proximity sensor</td><td>Proximity sensor</td></tr></table> See, e.g., <i>Compare iPhone Models</i>, Apple, https://www.apple.com/iphone/compare/ (last visited Dec. 29, 2024); see also, e.g., <i>Core Motion</i>, Apple Developer, https://developer.apple.com/documentation/CoreMotion. Apple Watch SE (2nd generation)  Apple Watch Series 10  Apple Watch Ultra 2  [. . .] [. . .] Sensors <table><tr><td>High dynamic range gyroscope</td><td>High dynamic range gyroscope</td><td>High dynamic range gyroscope</td></tr></table> See, e.g., <i>Compare Apple Watch models</i>, Apple, https://www.apple.com/watch/compare/ (last visited Dec. 29, 2024); <i>Apple Watch Series 9 – Technical Specifications</i>, Apple Support, https://support.apple.com/en-us/111833 (last visited Feb. 6, 2025) (listing “High-g accelerometer,” “High dynamic range gyroscope,” “Ambient light sensor”).	High dynamic range gyro	High dynamic range gyro	High dynamic range gyro	High-g accelerometer	High-g accelerometer	High-g accelerometer	Proximity sensor	Proximity sensor	Proximity sensor	High dynamic range gyroscope	High dynamic range gyroscope	High dynamic range gyroscope
High dynamic range gyro	High dynamic range gyro	High dynamic range gyro											
High-g accelerometer	High-g accelerometer	High-g accelerometer											
Proximity sensor	Proximity sensor	Proximity sensor											
High dynamic range gyroscope	High dynamic range gyroscope	High dynamic range gyroscope											

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
1[e] a memory for storing a user data and a currency amount;	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, includes a memory (<i>e.g.</i>, system memory, memory of secure element, memory of secure enclave, memory of eSIM/SIM, or combination of the same) for storing a user data (<i>e.g.</i>, name, account information, birthdate, phone number, passwords, and payment card information) and a currency amount (<i>e.g.</i>, balances on stored payment cards Apple Card, and Apple Cash, transaction history, and scheduled payments). iPhone 16 Pro Max  Capacity⁹ 256GB From \$1199 512GB From \$1399 1TB From \$1599 iPhone 16 Pro  128GB From \$999 256GB From \$1099 512GB From \$1299 1TB From \$1499 iPhone 16  128GB From \$799 256GB From \$899 512GB From \$1099 See, <i>e.g.</i>, <i>Compare iPhone Models</i>, Apple, https://www.apple.com/iphone/compare/ (last visited Dec. 29, 2024); <i>About eSIM on iPhone</i>, Apple Support (Oct. 21, 2024), https://support.apple.com/en-us/118669.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“’520 Patent”)

Claim No.	Accused Products
	Apple Watch SE (2nd generati⌵ Apple Watch Series 10⌵ Apple Watch Ultra 2⌵ An Apple Watch SE (2nd generation) with a black case and a black sport band. The screen shows a blue background with a person's face and the time 10:09. An Apple Watch Series 10 with a black case and a black sport band. The screen shows a black background with the time 10:09 in white. An Apple Watch Ultra 2 with a black case and a black mesh band. The screen shows a colorful watch face with the time 10:09, a date, and various weather and activity widgets.

Chip

32GB capacity64GB capacity64GB capacity

See, e.g., Compare Apple Watch models, Apple <https://www.apple.com/watch/compare/> (last visited Dec. 29, 2024); If your Apple Watch storage is full, Apple (Sept. 16, 2024), <https://support.apple.com/en-us/102407>; Use Dual SIM with Apple Watch GPS + Cellular models, Apple Support (Apr. 24, 2024),<https://support.apple.com/en-us/102359>.

Secure Element

The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets’ security domain. This data is stored within these 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.

[. . .]

Contactless payment component security

- Secure Element: The Secure Element hosts the payment kernels which read and secure the contactless payment card data.

[. . .]

Claim No.	Accused Products
	NFC & SE Platform component security The NFC & SE Platform provides access to hardware and software features that enable developers to provide secure transactions for iPhone users. Secure Element The Secure Element is an industry-standard integrated circuit that runs the Java Card platform. Certified by both EMVCo and Common Criteria, it supports standard Java Card applets, including those approved for the NFC & SE Platform. It also has a special applet for managing NFC & SE Platform applets’ authorization and activation. Credential data can be encrypted and sent to these applets using unique keys. This data is stored in the applets and secured by the Secure Element’s security features. During transactions, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller. [. . .] Secure Enclave The Secure Enclave manages the user authentication and secure intent processes on the device, allowing authorized transactions to proceed. Communication between the Secure Enclave and the Secure Element takes place over a serial interface, with the Secure Element connected to the NFC controller, which in turn is connected to the Application Processor. Though not directly connected, the Secure Enclave and Secure Element can communicate securely using a shared secret generated at runtime, which can be used to provide confidentiality and integrity over the communication link as needed. <i>See, e.g., Apple Platform Security</i>, at 178, 196, 260-261 (Dec. 2024), available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; <i>see also, e.g., Apple Platform Security, How Apple Pay keeps users’ purchases protected</i>, (Dec. 19, 2024), https://support.apple.com/guide/security/how-apple-pay-keeps-users-purchases-protected-secb53a35f0/web; <i>Apple Platform Security, Tap to Pay on iPhone security</i> (Dec. 19, 2024), https://support.apple.com/guide/security/tap-to-pay-on-iphone-sec72cb155f4/web; <i>Apple Platform Security, NFC & SE Platform Security</i> (Dec. 19, 2024), https://support.apple.com/en-mn/guide/security/secda20f3f41/web. When you add credit, debit, prepaid, or transit cards Apple doesn’t store or have access to the original card numbers of credit, debit, or prepaid cards that you add to Apple Pay. Apple Pay stores only a portion of your actual card numbers and a portion of your Device Account Numbers, along with a card description. Your cards are associated with your Apple Account to help you add and manage your cards across your devices. <i>See, e.g., Apple Pay security and privacy overview</i>, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554.

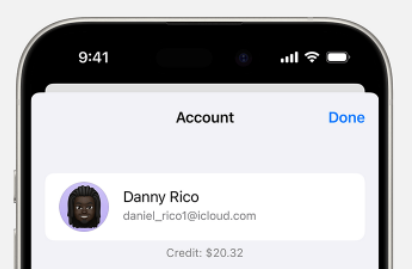
Claim No.	Accused Products
	Manage your Apple Account Because your Apple Account is used across all your devices and services, it’s important to keep your account information up to date. Simply sign in on account.apple.com² at any time to manage your account: • Update trusted phone numbers and devices that you’re currently signed in to with your Apple Account. • Change your password to help maintain the security of your account. • Update your Apple Account primary email address³ to make sure it’s an address that you use frequently. • Add additional email addresses and phone numbers to help people find and communicate with you on Apple services like FaceTime¹, iMessage, and Find My. You can also use these email addresses to sign in to your Apple Account. • Update the birth date associated with your Apple Account. • Change your Apple Account country or region. • Manage the payment methods associated with your Apple Account. • Manage subscriptions from the App Store and other Apple media services. You can also learn how to change or update your payment information or cancel subscriptions on your iPhone, iPad, or Mac. <i>See, e.g., Manage and use your Apple Account</i>, Apple (Nov. 15, 2024), https://support.apple.com/en-us/105023; <i>iPhone User Guide – iOS 18, Sign in and manage your Apple Account on iPhone</i>, Apple, https://support.apple.com/guide/iphone/sign-in-and-manage-your-apple-account-iph76e54c61e/ios (last visited Dec. 29, 2024); <i>Apple Watch User Guide – watchOS 11, Manage your Apple Account Settings on Apple Watch</i>, Apple, https://support.apple.com/guide/watch/manage-your-apple-account-apda9ebaa6d3/watchos (last visited Dec. 29, 2024); Laura McCamy, <i>How to find the phone number associated with an iPhone in 3 different ways</i>, Business Insider (Sept. 8, 2022, 3:59 PM PDT), https://www.businessinsider.com/guides/tech/how-to-find-phone-number-on-iphone.. Check your balance in Wallet on your iPhone or Apple Watch You might also be able to check your account balance in the Wallet app in some countries or regions. 1. Open the Wallet app. 2. Tap your Apple Account card. 3. If you have a balance, the amount appears below your Apple Account card. <i>See, e.g., Check your Apple Account balance</i>, Apple (Dec. 9, 2024), https://support.apple.com/en-us/119902; <i>iPhone User Guide – iOS 18, Use Apple Cash in Wallet on iPhone</i>, https://support.apple.com/guide/iphone/apple-cash-iph385cf0980/ios (last visited Dec. 29, 2024); <i>see also, e.g., Apple introduces Apple Pay Later to allow consumers to pay for purchases over time</i>, Apple Newsroom (Mar. 28, 2023), https://www.apple.com/newsroom/2023/03/apple-introduces-apple-pay-later/; Rhett Intriago, <i>How to See Apple Pay History on iPhone</i>, iPhone Life (May 20, 2024), https://www.iphonelife.com/content/how-to-see-apple-pay-history. 

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

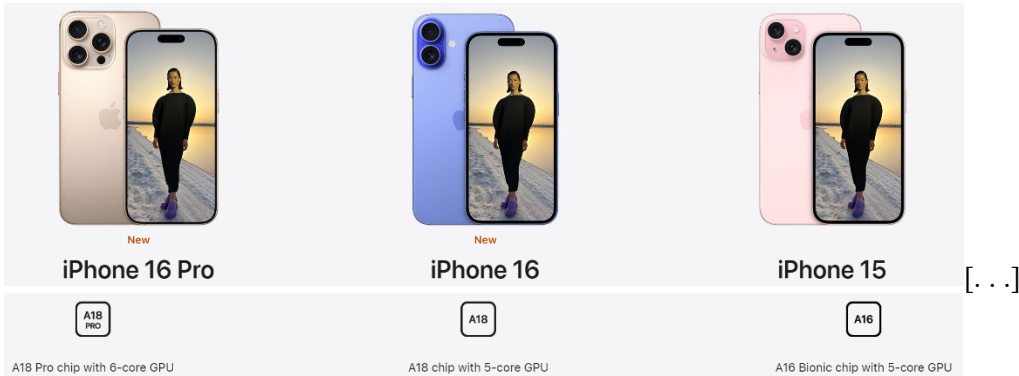
Claim No.	Accused Products
	Open the Apple Watch app on your iPhone, tap My Watch, then tap Wallet & Apple Pay. There you can do the following: • Tap the Apple Cash card to set up Apple Cash.  Tip: If you already have Apple Cash set up on another device, it will be ready to use on your Apple Watch Ultra without further setup. • Add funds from a debit card in Wallet. You can also set up Auto Reload. • Transfer money to a bank account. See the Apple Support article Transfer money in Apple Cash to your bank account or debit card. • View your Apple Cash balance.  Tip: To view your Apple Cash balance on your Apple Watch Ultra, open the Wallet app , then tap the Apple Cash card. Or double-click the side button, then scroll to the Apple Cash card. See, e.g., Apple Watch Ultra User Guide – WatchOS 10, <i>Manage Apple Cash with Apple Watch Ultra (U.S. only)</i>, Apple https://support.apple.com/en-bw/guide/watch-ultra/apd83f8ed083/watchos (last visited Dec. 29, 2024); Apple Watch User Guide – WatchOS 11, <i>Use Apple Cash on Apple Watch</i>, Apple, https://support.apple.com/guide/watch/use-apple-cash-apda7cde6cd7/watchos (last visited Dec. 29, 2024). To the extent that storing user data and a currency amount for an Apple Watch at a paired iPhone does not meet this limitation literally, CardWare contends that it is met under the doctrine of equivalents because it performs the same function in the same way to achieve the same result (<i>i.e.</i>, storing a user data and a currency amount on a memory (<i>i.e.</i>, the memory of an paired iPhone) associated with a device (<i>i.e.</i>, an Apple Watch)).
1[f] a processor operatively coupled to the NFC unit, the touch sensor array, the display, the motion rate detection array, and the memory;	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, includes a processor (<i>e.g.</i>, system processor, processor of the secure element, processor of the secure enclave, or any combination of the same) operatively coupled to the NFC unit, the touch sensor array, the display, the motion rate detection array, and the memory. See <i>supra</i> limitations 1[a], 1[b], 1[c], 1[d], and 1[e].  iPhone 16 Pro iPhone 16 iPhone 15 [...] A18 Pro chip with 6-core GPU A18 chip with 5-core GPU A16 Bionic chip with 5-core GPU See, e.g., <i>iPhone</i>, Apple, https://www.apple.com/iphone/ (last visited Dec. 27, 2024).

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“’520 Patent”)

Claim No.	Accused Products
	 Apple Watch SE S8 S8 SIP  Apple Watch Series 10 S10 S10 SIP  Apple Watch Ultra 2 S9 S9 SIP [. . .] See, e.g., <i>Watch</i>, Apple, https://www.apple.com/watch/ (last visited Dec. 27, 2024). Secure Element The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets’ security domain. This data is stored within these 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. [. . .] Contactless payment component security • <i>Secure Element</i>: The Secure Element hosts the payment kernels which read and secure the contactless payment card data. [. . .]

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	NFC & SE Platform component security The NFC & SE Platform provides access to hardware and software features that enable developers to provide secure transactions for iPhone users. Secure Element The Secure Element is an industry-standard integrated circuit that runs the Java Card platform. Certified by both EMVCo and Common Criteria, it supports standard Java Card applets, including those approved for the NFC & SE Platform. It also has a special applet for managing NFC & SE Platform applets’ authorization and activation. Credential data can be encrypted and sent to these applets using unique keys. This data is stored in the applets and secured by the Secure Element’s security features. During transactions, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller. [. . .] Secure Enclave The Secure Enclave manages the user authentication and secure intent processes on the device, allowing authorized transactions to proceed. Communication between the Secure Enclave and the Secure Element takes place over a serial interface, with the Secure Element connected to the NFC controller, which in turn is connected to the Application Processor. Though not directly connected, the Secure Enclave and Secure Element can communicate securely using a shared secret generated at runtime, which can be used to provide confidentiality and integrity over the communication link as needed. <i>See, e.g., Apple Platform Security</i>, at 178, 196, 260-261 (Dec. 2024), available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; <i>see also, e.g., Apple Platform Security, How Apple Pay keeps users’ purchases protected</i>, (Dec. 19, 2024), https://support.apple.com/guide/security/how-apple-pay-keeps-users-purchases-protected-secb53a35f0/web; <i>Apple Platform Security, Tap to Pay on iPhone security</i> (Dec. 19, 2024), https://support.apple.com/guide/security/tap-to-pay-on-iphone-sec72cb155f4/web; <i>Apple Platform Security, NFC & SE Platform Security</i> (Dec. 19, 2024), https://support.apple.com/en-mn/guide/security/secda20f3f41/web. ◦ NFC Transaction and Presentment: ▪ An NFC transaction can be made only after authorization from the Secure Enclave. On iPhone, this involves confirming that the user has authenticated with Face ID, Touch ID, or the device passcode. While the default method is Face ID or Touch ID, if available, the passcode can be used at any time. ▪ A user can initiate an NFC transaction by launching an eligible iOS app and selecting the credential to present to the NFC terminal which invokes a transaction authorization API. <i>See, e.g., NFC & SE Platform for secure contactless transactions</i>, Apple Developer Support, https://developer.apple.com/support/nfc-se-platform/ (last visited Jan. 21, 2025).

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

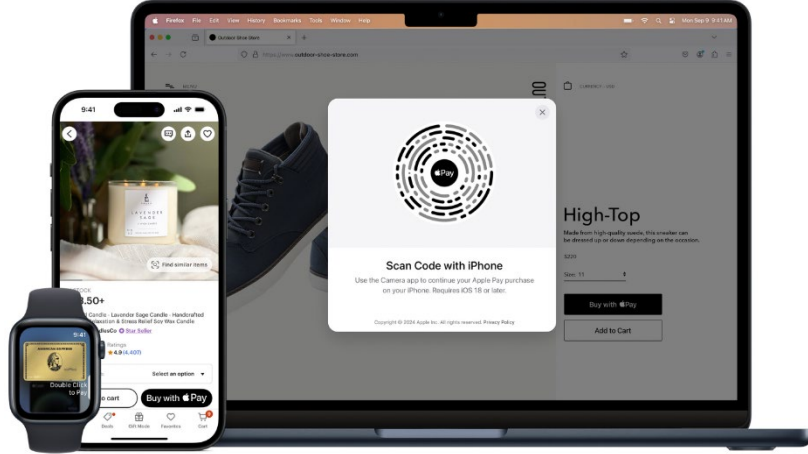
Claim No.	Accused Products
1[g] a computer readable medium having instructions stored thereon that, responsive to execution by the electronic device, cause the electronic device to perform operations comprising:	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, includes a computer readable medium (<i>e.g.</i>, memory as identified above) having instructions stored thereon (<i>e.g.</i>, Apple Pay and/or Apple Wallet apps) that, responsive to execution by the electronic device, cause the electronic device to perform the following operations. <i>See supra</i> limitation 1[e].   Personal data. Protected. When you make a purchase, Apple Pay uses a device-specific number and unique transaction code. So your card number is never stored on your device or on Apple servers. And when you pay, your card numbers are never shared by Apple with merchants. If you prefer not to share your email address with merchants when paying online, you can use Hide My Email to generate unique, random email addresses that automatically forward to your personal inbox. At stores and more. Apple Pay is accepted at over 85 percent of retailers in the U.S., so you can likely use it wherever and however you want. If you're not sure, just ask. Apple Pay works anywhere that takes contactless payments — from vending machines and grocery stores to taxis and subway stations. In apps and online. Use Apple Pay to seamlessly make purchases in Safari and other browsers — on iPhone, iPad, Mac, and other computers — without the lengthy checkout forms. On an Apple device, click or tap the Apple Pay button and pay with a touch or glance. On a non-Apple device, scan the Apple Pay code with your iPhone camera and use your iPhone to complete your purchase.* You can even use Apple Pay to subscribe to services like Apple Music, Apple News+, and Apple TV+, buy apps and games on the App Store, and upgrade your iCloud storage. <i>See, e.g., Apple Pay</i>, Apple, https://www.apple.com/apple-pay/; <i>Devices compatible with Apple Pay</i>, Apple (Mar. 6, 2024), https://support.apple.com/en-us/102896; Abby Ferguson, <i>How to set up Apple Pay</i>, Popular Sci. (May 12, 2024 3:04 PM EDT), https://www.popsci.com/diy/how-to-set-up-apple-pay/ (“[The Wallet app] is pre-installed on Apple devices, so you won’t need to install it first.”).

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
1[h] accepting a user input of issued payments information input at a touch screen display of the electronic device, wherein the information comprising an issuer provided payment information;	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, accepts a user input of issued payments information input at a touch screen display of the electronic device (<i>e.g.</i>, manual entry using via the touchscreen or confirmation via touchscreen of a scanned card information), wherein the information comprises an issuer provided payment information (<i>e.g.</i>, payment account number (“PAN”) or associated expiration date, or card security code/card identification number /card verification value (“CVV”)). <i>See supra</i> limitation 1[b]. How to add a debit or credit card on your iPhone If you have an eligible debit or credit card, you can tap your card on your iPhone to add it. Or, you can add your card manually. 1. In the Wallet app, tap the Add button . ◦ Tap Previous Cards to add a card that you used previously. ◦ Tap Debit or Credit Card to add a new card. 2. Tap Continue. 3. To add your card: ◦ Tap or hold your card close to your iPhone to add it. ◦ If you're unable to add your card by tapping or holding it close to your iPhone, position your debit or credit card in the frame to scan it. ◦ To manually add your card, tap Enter Card Details Manually and follow the onscreen instructions. <i>See, e.g., Set Up Apple Pay</i>, Apple Support (Dec. 17, 2024), https://support.apple.com/en-us/108398; iPhone User Guide – iOS 18, <i>Set up Apple Pay in Wallet on iPhone</i>, Apple, https://support.apple.com/guide/iphone/set-up-apple-pay-iph9b7f53382/18.0/ios/18.0 (last visited Dec. 29, 2024).

Claim No.	Accused Products
	See, e.g., Lance Whitney, <i>Pay With Your iPhone: How to Set Up and Use Apple Pay in-Store and Online</i>, PC Magazine (Sept. 14, 2023), https://www.pcmag.com/how-to/how-to-set-up-and-use-apple-pay. See also, e.g., Rain Kengly, <i>How to Add Cards to Apple Wallet on an iPhone and iPad</i>, wikiHow (May 1, 2024), https://www.wikihow.com/Add-Cards-to-Apple-Wallet; Apple, <i>Apple Pay – How to add a card on iPhone – Apple #Shorts</i>, YouTube (Sept. 21, 2017), https://youtu.be/rZbyRO20ZSk?si=AuvHz0d4_qW6wheo&t=20.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	Add a card to Apple Watch with your iPhone 1. Go to the Apple Watch app on your iPhone. 2. Tap My Watch, then tap Wallet & Apple Pay. 3. If you have cards on your other Apple devices, or cards that you recently removed, tap Add next to a card you want to add, then enter the card’s CVV. 4. For any other card, tap Add Card, then follow the onscreen instructions. Your card issuer may require additional steps to verify your identity. Add a card on Apple Watch You can add Apple Account, credit, debit, and transit cards, right on Apple Watch. 1. Go to the Wallet app  on your Apple Watch. 2. Tap , then tap Add Card. 3. Choose Apple Account, Debit or Credit Card, or Transit Card; then follow the onscreen instructions. <i>See, e.g., Apple Watch User Guide – WatchOS 11, Set up Apple Pay on Apple Watch, Apple, https://support.apple.com/guide/watch/set-up-apple-pay-apd285b3ae01/watchos (last visited Dec. 29, 2024); Christian Zibreg, <i>watchOS 10 lets you add new cards to Apple Watch’s Wallet app without iPhone</i>, iDownloadBlog (Jun. 24, 2023), https://www.idownloadblog.com/2023/06/14/watchos-10-add-card-apple-watch-no-iphone/ (“[T]he watchOS 10 update supports the full Apple Pay setup process, including entering a card’s number, expiration date and security code right on the watch, even if the card has not been already added to your iPhone.” (emphasis added)).</i> To the extent that adding new cards to an Apple Watch using a paired iPhone does not meet this limitation literally, CardWare contends that it is met under the doctrine of equivalents because it performs the same function in the same way to achieve the same result (<i>i.e.</i>, accepting user inputs of issuer provided payment information via a touchscreen (<i>i.e.</i>, iPhone touchscreen) to add a payment card to an Apple Watch).

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

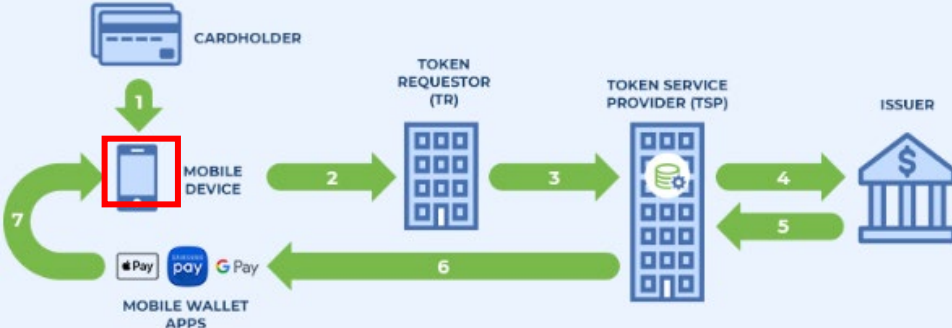
Claim No.	Accused Products
	In general terms, the process for registering a card in a mobile wallet is as follows: 1. The cardholder uses a device that supports the digital wallet application and registers a card, entering the data into the application. [...]  <i>See, e.g., Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details (captured May 9, 2024).</i>
1[i] wherein the memory comprises device-specific and user-specific information; and,	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, includes memory (<i>e.g.</i>, as identified above) that comprises device-specific information (<i>e.g.</i>, serial number, IMEI, etc.) and user-specific information (<i>e.g.</i>, as identified above.). <i>See supra</i> limitation 1[e]. 1. Go to Settings > General and tap About. 2. Look for the serial number. You might need to scroll down to find the IMEI/MEID, and ICCID.  <i>See, e.g., Find the serial number or IMEI on your iPhone, iPad, or iPod touch, Apple (Oct. 29, 2024), https://support.apple.com/en-us/108037; iPhone User Guide – iOS 18, Get information about your iPhone, Apple, https://support.apple.com/guide/iphone/get-information-about-your-iphone-iph3dd5fc7e/ios (last visited Dec. 29, 2024).</i>

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	1. On your Apple Watch, open the Settings app. 2. Tap General > About, then scroll down. 3. Look for Serial Number or IMEI. If you don't have your Apple Watch, you can use your iPhone instead: 1. On your iPhone, open the Apple Watch app. 2. Tap the My Watch tab, then tap General > About. 3. Look for Serial Number or IMEI. The IMEI is available on Apple Watch GPS + Cellular models only. See, e.g., <i>How to find the serial number or IMEI for your Apple Watch</i>, Apple (Oct. 23, 2024), https://support.apple.com/en-us/108040. To set up Apple Pay, add a debit or credit card to the Wallet app on your iPhone, Apple Watch, or other compatible device. To use Apple Pay, you need: • A compatible device¹ with the latest version of iOS or iPadOS, watchOS, macOS, or visionOS. • A supported card from a participating card issuer. • An Apple Account signed in to your Apple device. • Face ID, Touch ID, Optic ID, or a passcode set on your device. Learn if your country/region supports Apple Pay. To check if your card is compatible with Apple Pay, contact your card issuer. See, e.g., <i>Set up Apple Pay</i>, Apple (Dec. 17, 2024), https://support.apple.com/en-us/108398. Sign in with your Apple Account Use the same Apple Account every time you're asked to sign in on an Apple device or service. You can sign in to your Apple Account using any email addresses or phone numbers on file. You can find these email addresses and phone numbers in Settings (or System Settings) > [your name] > Sign-In & Security.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

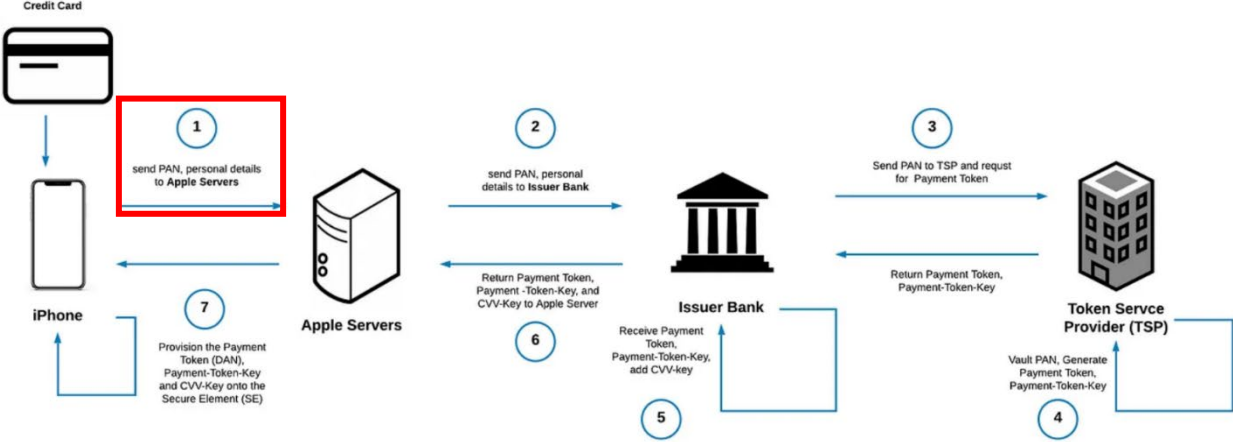
Claim No.	Accused Products
	Manage your Apple Account Because your Apple Account is used across all your devices and services, it’s important to keep your account information up to date. Simply sign in on account.apple.com² at any time to manage your account: • Update trusted phone numbers and devices that you’re currently signed in to with your Apple Account. • Change your password to help maintain the security of your account. • Update your Apple Account primary email address³ to make sure it’s an address that you use frequently. • Add additional email addresses and phone numbers to help people find and communicate with you on Apple services like FaceTime¹, iMessage, and Find My. You can also use these email addresses to sign in to your Apple Account. • Update the birth date associated with your Apple Account. • Change your Apple Account country or region. • Manage the payment methods associated with your Apple Account. • Manage subscriptions from the App Store and other Apple media services. You can also learn how to change or update your payment information or cancel subscriptions on your iPhone, iPad, or Mac. <i>See, e.g., Manage and use your Apple Account</i>, Apple (Nov. 15, 2024), https://support.apple.com/en-us/105023; Laura McCamy, <i>How to find the phone number associated with an iPhone in 3 different ways</i>, Business Insider (Sept. 8, 2022, 3:59 PM PDT), https://www.businessinsider.com/guides/tech/how-to-find-phone-number-on-iphone.
1[j] wherein the user provided payment information is communicated wirelessly; and,	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, wirelessly communicates (e.g., during card onboarding to a remote server (e.g., Apple’s or a token service provider’s (“TSP”)) via Wi-Fi or cellular network) the user provided payment information (e.g., PAN or associated expiration date, or CVV). Connect to a Wi-Fi network 1. From your Home screen, go to Settings > Wi-Fi. 2. Turn on Wi-Fi. Your device will automatically search for available Wi-Fi networks. 3. Tap the name of the Wi-Fi network that you want to join. Before you can join the network, you might be asked to enter the network’s password or agree to terms and conditions. After you join the network, you’ll see a blue checkmark ✓ next to the network and the connected Wi-Fi icon  in the upper corner of your display. If you don’t know the password to the Wi-Fi network, contact your network administrator. <i>See, e.g., Connect to Wi-Fi on your iPhone, iPad, or iPod touch</i>, Apple (Jun. 28, 2024), https://support.apple.com/en-us/111107. 

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	Turn cellular data on or off To turn cellular data on or off, go to Settings, then tap Cellular or Mobile Data. If you're using an iPad, you might see Settings > Cellular Data. Depending on your carrier and device, you might have additional options listed under Cellular Data Options: • Enable LTE, 4G, or 3G: You can select what type of network connection to use for voice and data. Learn more about these options. Learn about data options with 5G on your iPhone or iPad. • Turn Voice Roaming on or off: With CDMA networks, you can turn off Voice Roaming to avoid charges from using other carriers' networks. • Turn Data Roaming on or off: When you're traveling internationally, you can turn off data roaming to avoid roaming charges. If you have an international data plan, you may need to keep Data Roaming on. Learn more about traveling internationally with your iPhone or iPad. [. . .]  See, e.g., <i>Use cellular data on your iPhone or iPad</i>, Apple (Sept. 16, 2024), https://support.apple.com/en-us/109323. Choose a Wi-Fi network 1. Open the Settings app on your Apple Watch. 2. Tap Wi-Fi. Your device automatically searches for networks. 3. Tap the name of the network that you want to join. If you have Apple Watch Series 6 or later, you can connect to 2.4GHz or 5GHz Wi-Fi networks. Apple Watch Series 5 and earlier, and Apple Watch SE, can connect only to 2.4GHz Wi-Fi networks. 4. If asked, enter the password using Scribble or the Apple Watch keyboard. 5. Tap Join. [. . .]  See, e.g., <i>Connect your Apple Watch to Wi-Fi</i>, Apple (Apr. 26, 2024), https://support.apple.com/en-us/111818. Connect to a cellular network Your Apple Watch with cellular automatically switches to the most power-efficient wireless available: It can connect to your iPhone when it's nearby, a Wi-Fi network, or cellular. When your watch connects to cellular, it uses LTE networks. If LTE isn't available, your watch will try to connect to UMTS if your carrier supports it. When your watch connects to a cellular network, you can check the signal strength from Control Center or the Cellular complication that you can add to most watch faces. To open Control Center, touch and hold the bottom of the screen, then swipe up.  See, e.g., <i>Set up cellular on Apple Watch</i>, Apple (Jul. 10, 2024), https://support.apple.com/en-us/119601.

Claim No.	Accused Products
	When adding new cards to an Apple Watch using a paired iPhone, <i>see supra</i> limitation 1[h], the iPhone wirelessly communicates the user provided payment information. To the extent that this process does not meet this limitation literally, CardWare contends that it is met under the doctrine of equivalents because it performs the same function in the same way to achieve the same result (<i>i.e.</i>, as set out above, iPhone and Apple Watch can be used together for purposes of adding cards to Apple Pay or Apple Wallet). The combination of the iPhone and Apple Watch perform the same function (<i>i.e.</i>, providing user provided payment information (<i>e.g.</i>, to Apple or a TSP), in the same way (<i>i.e.</i>, over Wi-Fi or a cellular network) to achieve the same result (<i>i.e.</i>, receiving specific information (<i>e.g.</i>, from Apple or a TSP), <i>see infra</i> limitation 1[k])).  Starrirah Author Level 1 • 4 points Apple Wallet requires internet connection to add credit card? I am currently away from an internet connection. I tried to add a credit card to Apple Wallet, but get the message “Could Not Connect to Apple Pay - Make sure you are connected to the Internet.” Do I really need to be connected to the internet to add a credit card to Apple Wallet? Thanks <i>iPhone XS Max, iOS 12</i> Posted on Mar 29, 2019 9:53 AM  askbarnabas Level 10 • 103,453 points  Best reply Posted on Mar 29, 2019 7:22 PM Yes. <i>See, e.g., Starrirah, Apple Wallet requires internet connection to add credit card?</i>, Apple Support Community (Mar. 29, 2019), https://discussions.apple.com/thread/250267325?sortBy=best. Card provisioning security overview When a user adds a credit, debit, or prepaid card (including store cards) to Apple Wallet, 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 (usually the payment network). Using this information, the card issuer (or its service provider) determines whether to approve the user’s request to add the card to Apple Wallet. As part of the card provisioning process, Apple Pay uses three server-side calls to send and receive communication with the card issuer or payment network: • Required Fields • Check Card • Link and Provision The card issuer or payment network uses these calls to enable the card issuer to verify, approve, and add cards to Apple Wallet. These client-server sessions use TLS 1.2 or later to transfer the data. [...]

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	Users can add cards to Apple Watch for Apple Pay using either the Watch app on their iPhone or the card issuer’s app. To add a card to Apple Watch: • <i>When paired with an iPhone:</i> The watch must be within Bluetooth communications range • <i>When set up without an iPhone:</i> The watch must have internet access using Wi-Fi Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch. <i>See, e.g., Apple Platform Security</i>, at 179 (Dec. 2024), <i>available at</i> https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; <i>see also, e.g., Apple Platform Security, Card provisioning security overview</i>, Apple (May 7, 2024), https://support.apple.com/en-gb/guide/security/sec0f005981a/web. When a Payment Card is added to Apple Pay When you add a new payment card (<i>i.e. a credit or a debit card</i>) to Apple Pay, here are the steps that happen behind the scenes. 1. The payment card’s PAN (<i>Primary Account Number</i>), along with other card related personal details <i>i.e. Your Name, Card Expiration Date</i>, is sent by the <i>Apple Wallet App</i> to the <i>Apple Pay servers</i>.  When a Payment Card is Added to the Apple Pay Wallet <i>See, e.g., Prashant Ram, How Apple Pay works under the hood?</i>, codeburst (Nov. 5, 2019), https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7.

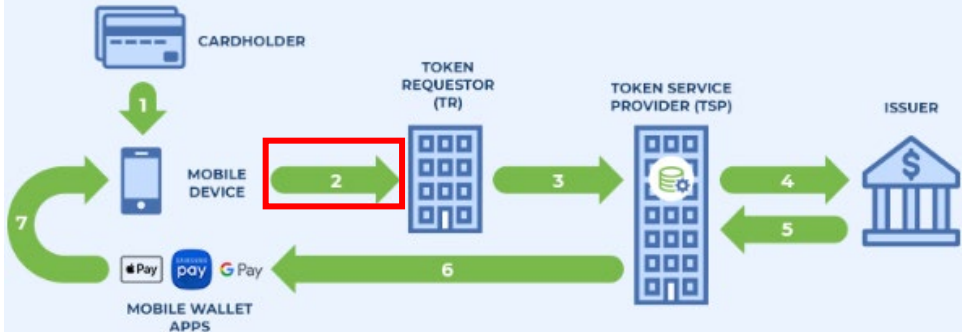
Claim No.	Accused Products
	In general terms, the process for registering a card in a mobile wallet is as follows: - The cardholder uses a device that supports the digital wallet application and registers a card, entering the data into the application. - The application sends the data to a <i>Token Requestor</i> (TR).  See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details (captured May 9, 2024). 3.1 In-Store EMV Contactless Payments with Device-Centric Digital Wallets Apple, Google, and Samsung were among the first to implement EMV payment tokens in digital wallets that hold credentials for several payments use cases. These device-centric digital wallets play the role of a token requestor; they may capture the cardholder’s PAN and request that it be replaced with a payment token from a TSP. Tokenization of payment credentials in digital wallets enables issuers to establish a secure presence on a wallet. [. . .] 5. End-to-End EMV Payment Tokenization Flows This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3): - In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) [. . .]

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

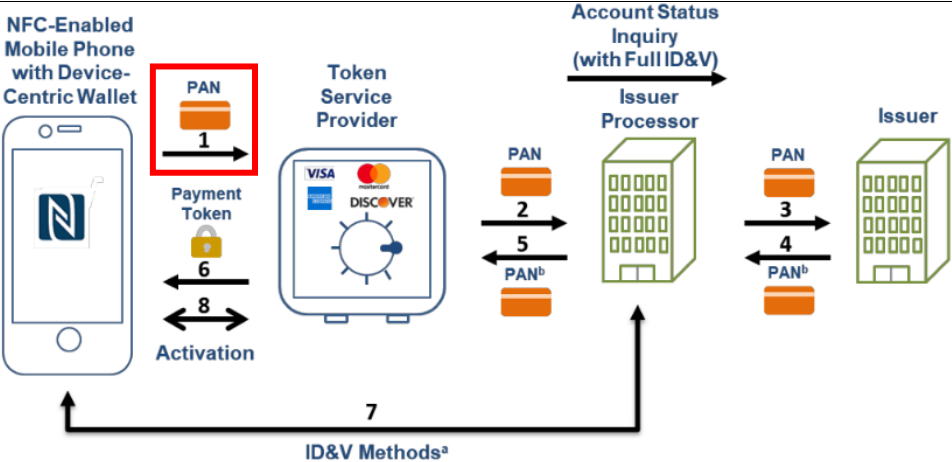
Claim No.	Accused Products
	 ^aID&V methods includes text or email or call. OTP is an example. ^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response. Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 12, 23 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.
1[k] wirelessly receiving a static device account number payment information for storage on the electronic device; and	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, wirelessly (e.g., during card onboarding from a remote server (e.g., Apple’s or a TSP’s) via Wi-Fi or cellular network) receives a static device account number payment information (e.g., a device-specific tokenized credit or debit card credentials/ payment token/ Device Account Number (“DAN”), and associated expiration date and keys) for storage on the electronic device (e.g., in the memory of secure element). When adding new cards to an Apple Watch using a paired iPhone, <i>see supra</i> limitation 1[h], the iPhone wirelessly receives the static device account number payment information and, on information and belief, wirelessly transmits it to the Apple Watch. To the extent that the Apple Watch does not meet this limitation literally, CardWare contends that it is met under the doctrine of equivalents because it performs the same function in the same way to achieve the same result (i.e., as set out above, iPhone and Apple Watch can be used together for purposes of adding cards to Apple Pay or Apple Wallet). The combination of the iPhone and Apple Watch perform the same function (i.e., providing user provided payment information (e.g., to a Token Service Provider (“TSP”)), <i>see supra</i> limitation 1[j]), in the same way (i.e., over a wireless connection, <i>see supra</i> limitation 1[j]) to achieve the same result (i.e., receiving static device account number payment information (e.g., from a TSP)).

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“’520 Patent”)

Claim No.	Accused Products
	 Starrirah Author Level 1 • 4 points Apple Wallet requires internet connection to add credit card? I am currently away from an internet connection. I tried to add a credit card to Apple Walket, but get the message “Could Not Connect to Apple Pay - Make sure you are connected to the Internet.” Do I really need to be connected to the internet to add a credit card to Apple Wallet? Thanks iPhone XS Max, iOS 12 Posted on Mar 29, 2019 9:53 AM  askbarnabas Level 10 • 103,453 points Posted on Mar 29, 2019 7:22 PM Yes. Best reply See, e.g., Starriah, <i>Apple Wallet requires internet connection to add credit card?</i>, Apple Support Community (Mar. 29, 2019), https://discussions.apple.com/thread/250267325?sortBy=best. Card provisioning security overview When a user adds a credit, debit, or prepaid card (including store cards) to Apple Wallet, 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 (usually the payment network). Using this information, the card issuer (or its service provider) determines whether to approve the user’s request to add the card to Apple Wallet. As part of the card provisioning process, Apple Pay uses three server-side calls to send and receive communication with the card issuer or payment network: • Required Fields • Check Card • Link and Provision The card issuer or payment network uses these calls to enable the card issuer to verify, approve, and add cards to Apple Wallet. These client-server sessions use TLS 1.2 or later to transfer the data. [...]

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	Users can add cards to Apple Watch for Apple Pay using either the Watch app on their iPhone or the card issuer’s app. To add a card to Apple Watch: • <i>When paired with an iPhone:</i> The watch must be within Bluetooth communications range • <i>When set up without an iPhone:</i> The watch must have internet access using Wi-Fi Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch. <i>See, e.g., Apple Platform Security</i>, at 179 (Dec. 2024), <i>available at</i> https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; <i>see also, e.g., Card provisioning security overview</i>, Apple (May 7, 2024), https://support.apple.com/en-gb/guide/security/sec0f005981a/web. When you add credit, debit, prepaid, or transit cards [. . .] After your card is approved, your bank, your bank’s authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such as the key used to generate dynamic security codes that are unique to each transaction) to Apple. The Device Account Number can’t be decrypted by Apple but is stored in the Secure Element—an industry-standard, certified chip designed to store your payment information safely—on your device. Unlike with usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS, watchOS, and macOS, is never stored on Apple servers, and is never backed up to iCloud. <i>See, e.g., Apple Pay security and privacy overview</i>, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554. When a Payment Card is added to Apple Pay When you add a new payment card (<i>i.e. a credit or a debit card</i>) to Apple Pay, here are the steps that happen behind the scenes. [. . .] 7. Apple Pay, uses its own Trusted Service Manager (TSM) and provisions the <i>Payment Token</i>, <i>Payment Token-Key</i> and <i>CVV-Key</i> and maybe other data onto the “Secure Element” <i>i.e.</i> the secure hardware chip on the physical iPhone device. This then is the “Payment Token” that Apple saves on its Secure Element (SE) and calls the <i>DAN (Device Account Number)</i>.

Claim No.	Accused Products
	When a Payment Card is Added to the Apple Pay Wallet See, e.g., Prashant Ram, <i>How Apple Pay works under the hood?</i>, codeburst (Nov. 5, 2019), https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7. In general terms, the process for registering a card in a mobile wallet is as follows: [. . .] 6. The TSP notifies the application of the newly generated token. 7. The application stores the generated token (<i>Device Account Number</i> (DAN) for Apple Pay or Digitized PAN (DPAN) for Samsung Pay) in a secure location (Secure Element (SE) or Host Card Emulation (HCE)). See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021) available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details (captured May 9, 2024).

Claim No.	Accused Products
	3.1 In-Store EMV Contactless Payments with Device-Centric Digital Wallets Apple, Google, and Samsung were among the first to implement EMV payment tokens in digital wallets that hold credentials for several payments use cases. These device-centric digital wallets play the role of a token requestor; they may capture the cardholder’s PAN and request that it be replaced with a payment token from a TSP. Tokenization of payment credentials in digital wallets enables issuers to establish a secure presence on a wallet. [. . .] 5. End-to-End EMV Payment Tokenization Flows This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3): In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) [. . .] ^a ID&V methods includes text or email or call. OTP is an example. ^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response. Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet <i>See, e.g., US Payments Forum, EMV Payment Tokenization Primer and Lessons Learned at 12, 23 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</i>

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	5.1.3.2 Token Generation Token Generation is the process of creating a Payment Token and its associated Token Expiry Date and mapping it to a specific underlying PAN, for use by a specific Token Requestor and Token Domain(s), as identified the Token Requestor ID. The Token Service Provider SHALL facilitate the generation of a Payment Token and related data. This may be in response to a Token Request from a registered Token Requestor with a valid Token Requestor ID or an existing Payment Token may be mapped to an underlying PAN in response to a Token Request from a registered Token Requestor with a valid Token Requestor ID. 5.1.3.3 Token Issuance Token Issuance is the process of issuing a Payment Token and related data in preparation for Token Provisioning. The Token Service Provider SHALL manage Token Requests based on the Token Requestor ID. Token Service Providers SHALL manage the issuance of Payment Tokens. Payment Tokens SHALL only be issued through the response to a Token Request from a registered Token Requestor with a valid Token Requestor ID. 5.1.3.4 Token Provisioning Token Provisioning is the process of delivering a Payment Token and related data to the Token Location. Token Provisioning SHOULD be carried out by the Token Service Provider or by other authorised entities on its behalf. The methodologies associated with Token Provisioning may be proprietary to each Token Programme and are outside the scope of this technical framework. <i>See, e.g., EMVCo, EMV® Payment Tokenisation Specification – Technical Framework v2.1 at 35–36 (Jun. 14, 2019).</i>
1[1] wherein at least a portion of the payment information is a limited-use number for limited-use by the device, in place of a issuer provided payment information; and,	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, uses payment information, wherein at least a portion of the payment information is a limited-use number for limited-use by the device (<i>e.g.</i>, the DAN, a unique transaction code/ transaction-specific dynamic security code/ payment cryptogram (“the dynamic cryptogram”), a dynamic security code/rotating Apple Card security code/ dynamic card verification value (“the dynamic security code”), or any combination thereof), in place of a issuer provided payment information (<i>e.g.</i>, PAN or associated expiration date or CVV). Personal data. Protected. When you make a purchase, Apple Pay uses a device-specific number and unique transaction code. So your card number is never stored on your device or on Apple servers. And when you pay, your card numbers are never shared by Apple with merchants. If you prefer not to share your email address with merchants when paying online, you can use Hide My Email to generate unique, random email addresses that automatically forward to your personal inbox. <i>See, e.g., Apple Pay, Apple, https://www.apple.com/apple-pay/ (last visited Dec. 29, 2024).</i>

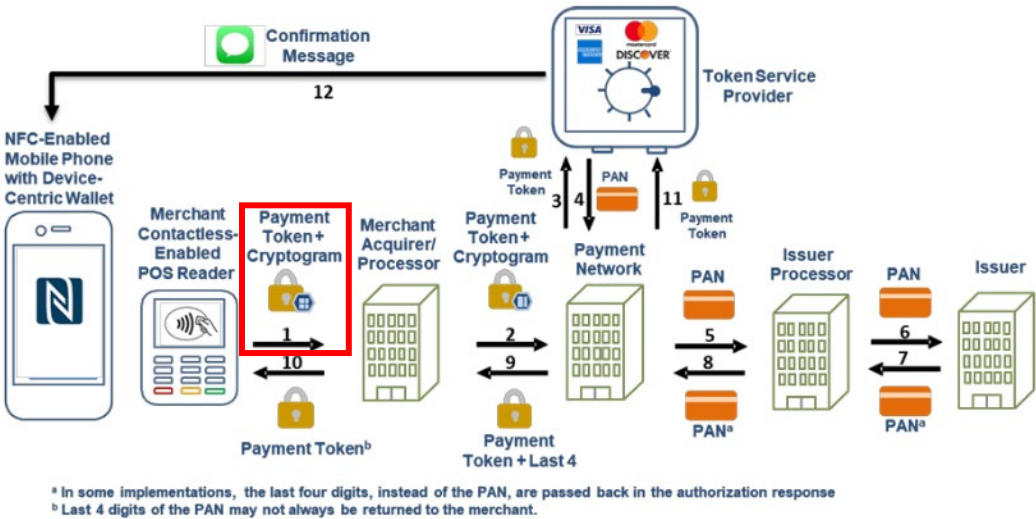
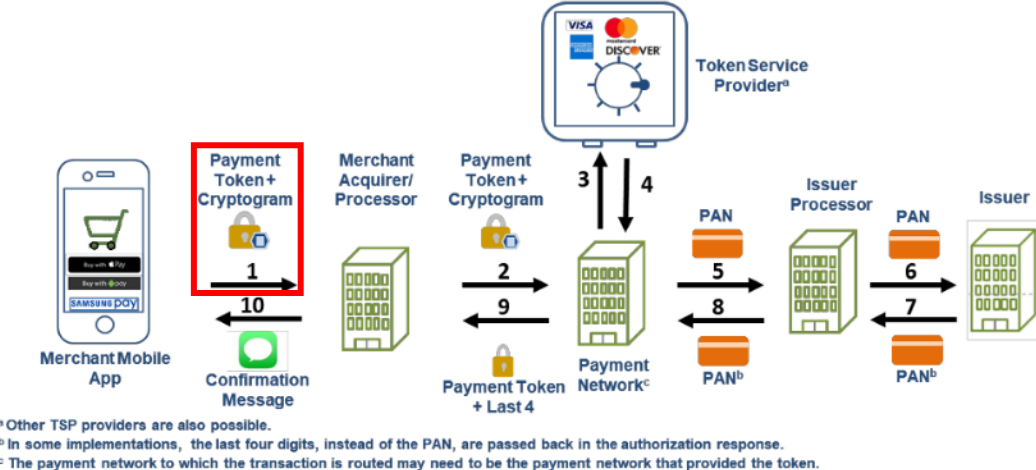
Claim No.	Accused Products
	When you use Apple Pay in stores [. . .] After you authenticate your transaction, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code to the store’s point of sale terminal along with additional information needed to complete the transaction. Again, neither Apple nor your device sends your actual payment 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 that it’s unique and tied to your device. When you use Apple Pay within apps or on the web [. . .] To securely transmit your payment information when you pay in apps or on the web, Apple Pay receives your encrypted transaction and re-encrypts it with a developer-specific key before the transaction information is sent to the developer or payment processor. This key helps ensure that only the app or the website that you’re purchasing from can access your encrypted payment information. Websites must verify their domain every time they offer Apple Pay as a payment option. Like with in-store payments, Apple sends your Device Account Number to the app or website along with the transaction-specific dynamic security code. Neither Apple nor your device sends your actual payment card number to the app. See, e.g., <i>Apple Pay security and privacy overview</i>, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554. Using a payment cryptogram for dynamic security Payment transactions originating from the payment applets include a payment cryptogram along with a Device Account Number. This cryptogram, a one-time code, is computed using a transaction counter and a key. The transaction counter is incremented for each new transaction. The key is provisioned in the payment applet during personalization and is known by the payment network or the card issuer or both. Depending on the payment scheme, other data may also be used in the calculation, including: • A Terminal Unpredictable Number, for near-field-communication (NFC) transactions • An Apple Pay server anti-replay value, for transactions within apps • User verification results, such as Cardholder Verification Method (CVM) information These security codes are provided to the payment network and to the card issuer, which allows the issuer to verify each transaction. The length of these security codes may vary based on the type of transaction. See, e.g., <i>Apple Platform Security</i>, at 183 (Dec. 2024) available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; see also, e.g., <i>Apple Platform Security, Payment authorization with Apple Pay</i>, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/payment-authorization-with-apple-pay-secc1f57e189/web.

Claim No.	Accused Products
	What is Advanced Fraud Protection? Advanced Fraud Protection is a way to keep your Apple Card information even more secure. After turning on Advanced Fraud Protection, your three-digit Apple Card security code will change periodically after it's been viewed in the Wallet app or after it's been auto-filled from Safari. You should check your security code each time you want to make a purchase with Apple Card to be sure you're using the most up-to-date code. You can also use Advanced Fraud Protection without affecting your recurring purchases and subscriptions, such as streaming services or memberships, because these merchants use your security code to authorize payment just once when you first sign up. <i>See, e.g., Use Advanced Fraud Protection with Apple Card</i>, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102427. How your virtual card number works Virtual card numbers are a way to keep your payment card information even more secure. For fraud protection, your 3-digit security code changes frequently with usage and over time. You can use your virtual card number online wherever Visa is accepted. <i>See, e.g., Use your virtual card number for Apple Cash</i>, Apple (Dec. 17, 2024), https://support.apple.com/en-us/119943. When you Pay using Apple Pay with your iPhone Apple Pay uses <i>NFC</i> to send payment data to the contactless POS terminal when you Tap & Pay . Apple Pay uses the <i>EMVCo's contactless suite of specifications</i> to pass the data from your iPhone to the contactless reader terminal. [. . .] 2. Once you authenticate yourself to the iPhone the Secure Element on the iPhone takes the following steps, [. . .] The Secure Element then passes the <i>Payment Token (DAN)</i>, the <i>Dynamic Cryptogram</i> (also called, the <i>One-time Unique Number</i>), the <i>Dynamic CVV Value</i> (also called, the <i>Dynamic Security Code</i>), and other payment and chip data elements to the POS terminal via NFC, using the EMVCo's contactless suite of specifications.

Claim No.	Accused Products
	When you Pay using Apple Pay with your iPhone See, e.g., Prashant Ram, <i>How Apple Pay works under the hood?</i>, codeburst (Nov. 5, 2019), https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7. The original PAN of the card is never stored on the end user's device. Instead, the payment token with which subsequent transactions are made is securely stored. Let's walk through this: 1. The cardholder (in this case, the same user of the digital wallet application) makes use of the payment application, presenting the payment token to the merchant from his/her device using any of the following channels: • EMV Contactless: If the Point of Sale (POS) terminal supports contactless payments via NFC (Near Field Communication), the EMV contactless specification is used to perform the data transfer. 2. The merchant sends the token and dynamic cryptogram data to the acquirer. [. . .]

Claim No.	Accused Products
	The diagram illustrates the EMV Payment Tokenization process. It shows a Mobile Device (1) interacting with a Merchant + Contactless Payment Terminal (2). The Merchant then interacts with an Acquirer (3), which interacts with a Payment Network (4). The Payment Network interacts with an Issuer (5). A Token Service Provider (TST) is also shown, interacting with the Mobile Device (6), Payment Network (7), and Issuer (8). The process is numbered 1 through 9, indicating the sequence of steps. See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details (captured May 9, 2024). 5. End-to-End EMV Payment Tokenization Flows This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3): In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	 ^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response ^b Last 4 digits of the PAN may not always be returned to the merchant. Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet  ^a Other TSP providers are also possible. ^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response. ^c The payment network to which the transaction is routed may need to be the payment network that provided the token. Figure 7. Processing an In-App Transaction Using a Merchant Mobile App with Tokens Provisioned in a Device-Centric Wallet See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 23–26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.

Claim No.	Accused Products
1[m] dynamically-generating a one-time limited-use numbers based on at least one of a set of information including: user-identifying information; user secrets; device information; device secrets; time; merchant; facility location; sequence count; payment information; account information; amount; and transaction information; and	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, dynamically-generates a one-time limited-use numbers (e.g., the dynamic cryptogram, or the dynamic security code) based on at least one of a set of information including: user-identifying information; user secrets; device information; device secrets (e.g., DAN); time; merchant; facility location (e.g., device location); sequence count (e.g., transaction counter); payment information; account information (e.g., payment token key, CVV-key); amount; and transaction information (e.g., Terminal Unpredictable Number). For example, the dynamic cryptogram is generated using at least a sequence count (e.g., a transaction counter), device secrets (e.g., DAN), and a key (e.g., a payment token key), and further could use facility location (e.g., device location) or transaction information (e.g., Terminal Unpredictable Number). The dynamic security code is generated using at least a key (e.g., a CVV-key). <i>See supra</i> limitation 1[e], 1[i]. When you use Apple Pay in stores [...] After you authenticate your transaction, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code to the store’s point of sale terminal along with additional information needed to complete the transaction. Again, neither Apple nor your device sends your actual payment 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 that it’s unique and tied to your device. When you add credit, debit, prepaid, or transit cards [...] To securely transmit your payment information when you pay in apps or on the web, Apple Pay receives your encrypted transaction and re-encrypts it with a developer-specific key before the transaction information is sent to the developer or payment processor. This key helps ensure that only the app or the website that you’re purchasing from can access your encrypted payment information. Websites must verify their domain every time they offer Apple Pay as a payment option. Like with in-store payments, Apple sends your Device Account Number to the app or website along with the transaction-specific dynamic security code. Neither Apple nor your device sends your actual payment card number to the app. <i>See, e.g., Apple Pay security and privacy overview</i>, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554.

Claim No.	Accused Products
	Using a payment cryptogram for dynamic security Payment transactions originating from the payment applets include a payment cryptogram along with a Device Account Number. This cryptogram, a one-time code, is computed using a transaction counter and a key. The transaction counter is incremented for each new transaction. The key is provisioned in the payment applet during personalization and is known by the payment network or the card issuer or both. Depending on the payment scheme, other data may also be used in the calculation, including: • A Terminal Unpredictable Number, for near-field-communication (NFC) transactions • An Apple Pay server anti-replay value, for transactions within apps • User verification results, such as Cardholder Verification Method (CVM) information These security codes are provided to the payment network and to the card issuer, which allows the issuer to verify each transaction. The length of these security codes may vary based on the type of transaction. <i>See, e.g., Apple Platform Security</i>, at 183 (Dec. 2024) available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; <i>see also, e.g., Apple Platform Security, Payment authorization with Apple Pay</i>, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/payment-authorization-with-apple-pay-secc1f57e189/web. What is Advanced Fraud Protection? Advanced Fraud Protection is a way to keep your Apple Card information even more secure. After turning on Advanced Fraud Protection, your three-digit Apple Card security code will change periodically after it's been viewed in the Wallet app or after it's been auto-filled from Safari. You should check your security code each time you want to make a purchase with Apple Card to be sure you're using the most up-to-date code. You can also use Advanced Fraud Protection without affecting your recurring purchases and subscriptions, such as streaming services or memberships, because these merchants use your security code to authorize payment just once when you first sign up. <i>See, e.g., Use Advanced Fraud Protection with Apple Card</i>, Apple (Dec. 17, 2023), https://support.apple.com/en-us/102427. How your virtual card number works Virtual card numbers are a way to keep your payment card information even more secure. For fraud protection, your 3-digit security code changes frequently with usage and over time. You can use your virtual card number online wherever Visa is accepted. <i>See, e.g., Use your virtual card number for Apple Cash</i>, Apple (Dec. 17, 2024), https://support.apple.com/en-us/119943.

Claim No.	Accused Products				
	Note: If you have Location Services turned on, the location of your iPhone at the time you make a payment may be sent to Apple and the card issuer to help prevent fraud. See Control the location information you share. See, e.g., iPhone User Guide – iOS 18, <i>Use Apple Pay for contactless payments on iPhone</i>, Apple, https://support.apple.com/guide/iphone/use-apple-pay-for-contactless-payments-iphbd4cf42b4/ios (last visited Dec. 23, 2024). 5. End-to-End EMV Payment Tokenization Flows This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3): In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 12, 23 (June 2019) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf. <table><tr><th>Term</th><th>Definition</th></tr><tr><td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr></table> See, e.g., EMVCo, <i>EMV® Payment Tokenisation Specification – Technical Framework v2.1</i> at 10 (Jun. 14, 2019).	Term	Definition	Token Cryptogram	A cryptogram, containing a transaction-unique value, typically generated using the Payment Token Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.
Term	Definition				
Token Cryptogram	A cryptogram, containing a transaction-unique value, typically generated using the Payment Token Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.				

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	When a Payment Card is added to Apple Pay When you add a new payment card (<i>i.e. a credit or a debit card</i>) to Apple Pay, here are the steps that happen behind the scenes. [. . .] 7. Apple Pay, uses its own Trusted Service Manager (TSM) and provisions the <i>Payment Token</i>, <i>Payment Token-Key</i> and <i>CVV-Key</i> and maybe other data onto the “Secure Element” <i>i.e.</i> the secure hardware chip on the physical iPhone device. This then is the “Payment Token” that Apple saves on its Secure Element (SE) and calls the <i>DAN (Device Account Number)</i>. [. . .] When you Pay using Apple Pay with your iPhone Apple Pay uses <i>NFC</i> to send payment data to the contactless POS terminal when you Tap & Pay . Apple Pay uses the <i>EMVCo’s contactless suite of specifications</i> to pass the data from your iPhone to the contactless reader terminal. [. . .] 2. Once you authenticate yourself to the iPhone the Secure Element on the iPhone takes the following steps, (a) <i>generates a Dynamic Cryptogram</i>, - which is a combination of the <i>Payment Token</i>, <i>transaction amount</i>, <i>transaction counter etc.</i> along with the <i>Payment-Token-Key</i> (<i>i.e.</i> the public key provided by the TSP). (b) <i>generates a Dynamic CVV</i>, - using the <i>CVV-key</i> (<i>i.e.</i> the public key provided by the Issuing Bank).

Claim No.	Accused Products
	The diagram illustrates the Apple Pay transaction process. It starts with a person authenticating on their iPhone (1). The iPhone then passes a Dynamic Authentication Number (DAN), Dynamic Cryptogram, and Dynamic CVV to a Contactless POS Terminal via NFC (2). The POS Terminal sends this information to the Merchant Bank (3). The Merchant Bank then passes the same information to the Payment Network (4). The Payment Network passes the DAN and Dynamic Cryptogram to the Token Service Provider (TSP) (5). The TSP returns the Real PAN to the Payment Network (6). The Payment Network then passes the PAN, transaction info, and Dynamic CVV to the Issuer Bank (7). The Issuer Bank validates the transaction and authorizes it (8). The transaction authorized response is then sent back through the chain from the Issuer Bank to the Payment Network, then to the Merchant Bank, and finally to the POS Terminal. When you Pay using Apple Pay with your iPhone See, e.g., Prashant Ram, <i>How Apple Pay works under the hood?</i>, codeburst (Nov. 5, 2019), https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7. The original PAN of the card is never stored on the end user's device. Instead, the payment token with which subsequent transactions are made is securely stored. Let's walk through this: - The cardholder (in this case, the same user of the digital wallet application) makes use of the payment application, presenting the payment token to the merchant from his/her device using any of the following channels: - EMV Contactless: If the Point of Sale (POS) terminal supports contactless payments via NFC (Near Field Communication), the EMV contactless specification is used to perform the data transfer. - The merchant sends the token and dynamic cryptogram data to the acquirer.

[. .]

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details (captured May 9, 2024).
1[n] using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction.	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, uses said static device account number (e.g., DAN) and said dynamically generated one-time limited-use number (e.g., the dynamic cryptogram, the dynamic security code, or any combination of the same) together in the place of issuer provided payment information (e.g., PAN or associated expiration date or CVV) for making a payment transaction. See <i>supra</i> limitation 1[1]. Personal data. Protected When you make a purchase, Apple Pay uses a device-specific number and unique transaction code. So your card number is never stored on your device or on Apple servers. And when you pay, your card numbers are never shared by Apple with merchants. If you prefer not to share your email address with merchants when paying online, you can use Hide My Email to generate unique, random email addresses that automatically forward to your personal inbox. See, e.g., <i>Apple Pay</i>, Apple, https://www.apple.com/apple-pay/ (last visited Dec. 29, 2024); see also, e.g., Apple, <i>Apple Pay Merchant Integration Guide</i> (Jan. 2024) available at https://developer.apple.com/apple-pay/Apple-Pay-Merchant-Integration-Guide.pdf (“Apple Pay uses device-specific tokenized credit or debit card credentials (DPAN) in place of a Payment Account Number (PAN).”).

Claim No.	Accused Products
	When you use Apple Pay in stores [...] After you authenticate your transaction, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code to the store's point of sale terminal along with additional information needed to complete the transaction. Again, neither Apple nor your device sends your actual payment 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 that it's unique and tied to your device. When you use Apple Pay within apps or on the web [...] To securely transmit your payment information when you pay in apps or on the web, Apple Pay receives your encrypted transaction and re-encrypts it with a developer-specific key before the transaction information is sent to the developer or payment processor. This key helps ensure that only the app or the website that you're purchasing from can access your encrypted payment information. Websites must verify their domain every time they offer Apple Pay as a payment option. Like with in-store payments, Apple sends your Device Account Number to the app or website along with the transaction-specific dynamic security code. Neither Apple nor your device sends your actual payment card number to the app. See, e.g., <i>Apple Pay security and privacy overview</i>, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554. Using a payment cryptogram for dynamic security Payment transactions originating from the payment applets include a payment cryptogram along with a Device Account Number. This cryptogram, a one-time code, is computed using a transaction counter and a key. The transaction counter is incremented for each new transaction. The key is provisioned in the payment applet during personalization and is known by the payment network or the card issuer or both. Depending on the payment scheme, other data may also be used in the calculation, including: • A Terminal Unpredictable Number, for near-field-communication (NFC) transactions • An Apple Pay server anti-replay value, for transactions within apps • User verification results, such as Cardholder Verification Method (CVM) information These security codes are provided to the payment network and to the card issuer, which allows the issuer to verify each transaction. The length of these security codes may vary based on the type of transaction. See, e.g., <i>Apple Platform Security</i>, at 183 (Dec. 2024) available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; see also, e.g., <i>Apple Platform Security, Payment authorization with Apple Pay</i>, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/payment-authorization-with-apple-pay-secc1f57e189/web.

Claim No.	Accused Products						
	What is Advanced Fraud Protection? Advanced Fraud Protection is a way to keep your Apple Card information even more secure. After turning on Advanced Fraud Protection, your three-digit Apple Card security code will change periodically after it's been viewed in the Wallet app or after it's been auto-filled from Safari. You should check your security code each time you want to make a purchase with Apple Card to be sure you're using the most up-to-date code. You can also use Advanced Fraud Protection without affecting your recurring purchases and subscriptions, such as streaming services or memberships, because these merchants use your security code to authorize payment just once when you first sign up. See, e.g., <i>Use Advanced Fraud Protection with Apple Card</i>, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102427. How your virtual card number works Virtual card numbers are a way to keep your payment card information even more secure. For fraud protection, your 3-digit security code changes frequently with usage and over time. You can use your virtual card number online wherever Visa is accepted. See, e.g., <i>Use your virtual card number for Apple Cash</i>, Apple (Dec. 17, 2024), https://support.apple.com/en-us/119943. Overview Apple Pay is available on all iOS devices with a Secure Element — an industry-standard, certified chip designed to store payment information safely. In macOS, users must have an iPhone or Apple Watch that supports Apple Pay to authorize the payment, or have a Mac with Touch ID. The Secure Element creates a payment object when an app or website that uses Apple Pay sends a payment request. The payment object has a nested structure that contains a payment token with encrypted payment data, as shown in the figure below. The Secure Element encrypts the token's payment data using either elliptic curve cryptography (ECC) or RSA encryption. The Secure Element selects the encryption algorithm based on the merchant capabilities that the payment request indicates. Most regions use ECC encryption. Other regions use RSA encryption if ECC encryption is unavailable due to regulatory concerns. Payment token structure The paymentData property of PKPaymentToken (or the paymentData property of ApplePayPaymentToken, for Apple Pay on the Web) contains a UTF-8 serialization of a plaintext JSON dictionary with the following keys and values: <table><tr><th>Key</th><th>Value</th><th>Description</th></tr><tr><td>data</td><td>payment data dictionary, Base64 encoded as a string</td><td>Encrypted payment data See Payment Data Keys below for the decrypted payment data keys and values.</td></tr></table> [...]	Key	Value	Description	data	payment data dictionary, Base64 encoded as a string	Encrypted payment data See Payment Data Keys below for the decrypted payment data keys and values.
Key	Value	Description					
data	payment data dictionary, Base64 encoded as a string	Encrypted payment data See Payment Data Keys below for the decrypted payment data keys and values.					

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products																								
	Payment data keys The decrypted payment data in the data value contains the following keys and values: <table><tr><th>Key</th><th>Value</th><th>Description</th></tr><tr><td>applicationPrimaryAccountNumber</td><td>string</td><td>Device-specific account number of the card that funds this transaction</td></tr><tr><td>applicationExpirationDate</td><td>date as a string</td><td>Card expiration date in the format YYMMDD</td></tr></table> [...] <table><tr><td>paymentDataType</td><td>string</td><td>Either "3DSecure" or "EMV"</td></tr><tr><td>paymentData</td><td>payment data dictionary</td><td>Detailed payment data; see Detailed Payment Data Keys (3D Secure) and Detailed Payment Data Keys (EMV) below</td></tr></table> [...] Detailed payment data keys (EMV) If the paymentDataType value is "EMV" in the Payment Data Keys information, the payment data dictionary in paymentData contains the following keys and values: <table><tr><th>Key</th><th>Value</th><th>Description</th></tr><tr><td>emvData</td><td>The Europay, Mastercard, and Visa (EMV) payment structure, as a Base64-encoded string</td><td>Output from the Secure Element</td></tr><tr><td>encryptedPINData</td><td>The encrypted PIN, as a hex-encoded string</td><td>The PIN is encrypted using the bank's key. RSA_v1 only.</td></tr></table> [...] See, e.g., Payment token format reference, Apple Developer, https://developer.apple.com/documentation/passkit_apple_pay_and_wallet/apple_pay/payment_token_format_reference (last visited Dec. 29, 2024); PKPayment, Apple Developer, https://developer.apple.com/documentation/passkit_apple_pay_and_wallet/pkpayment (last visited Dec. 29, 2024). When a Payment Card is added to Apple Pay When you add a new payment card (i.e. a credit or a debit card) to Apple Pay, here are the steps that happen behind the scenes. [...]	Key	Value	Description	applicationPrimaryAccountNumber	string	Device-specific account number of the card that funds this transaction	applicationExpirationDate	date as a string	Card expiration date in the format YYMMDD	paymentDataType	string	Either "3DSecure" or "EMV"	paymentData	payment data dictionary	Detailed payment data; see Detailed Payment Data Keys (3D Secure) and Detailed Payment Data Keys (EMV) below	Key	Value	Description	emvData	The Europay, Mastercard, and Visa (EMV) payment structure, as a Base64-encoded string	Output from the Secure Element	encryptedPINData	The encrypted PIN, as a hex-encoded string	The PIN is encrypted using the bank's key. RSA_v1 only.
Key	Value	Description																							
applicationPrimaryAccountNumber	string	Device-specific account number of the card that funds this transaction																							
applicationExpirationDate	date as a string	Card expiration date in the format YYMMDD																							
paymentDataType	string	Either "3DSecure" or "EMV"																							
paymentData	payment data dictionary	Detailed payment data; see Detailed Payment Data Keys (3D Secure) and Detailed Payment Data Keys (EMV) below																							
Key	Value	Description																							
emvData	The Europay, Mastercard, and Visa (EMV) payment structure, as a Base64-encoded string	Output from the Secure Element																							
encryptedPINData	The encrypted PIN, as a hex-encoded string	The PIN is encrypted using the bank's key. RSA_v1 only.																							

Claim No.	Accused Products
	7. Apple Pay, uses its own Trusted Service Manager (TSM) and provisions the <i>Payment Token</i>, <i>Payment Token-Key</i> and <i>CVV-Key</i> and maybe other data onto the “Secure Element” i.e. the secure hardware chip on the physical iPhone device. This then is the “Payment Token” that Apple saves on its Secure Element (SE) and calls the <i>DAN (Device Account Number)</i>. [. . .] When you Pay using Apple Pay with your iPhone Apple Pay uses <i>NFC</i> to send payment data to the contactless POS terminal when you Tap & Pay . Apple Pay uses the <i>EMVCo’s contactless suite of specifications</i> to pass the data from your iPhone to the contactless reader terminal. 2. Once you authenticate yourself to the iPhone the Secure Element on the iPhone takes the following steps, [. . .] The Secure Element then passes the <i>Payment Token (DAN)</i>, the <i>Dynamic Cryptogram</i> (also called, the <i>One-time Unique Number</i>), the <i>Dynamic CVV Value</i> (also called, the <i>Dynamic Security Code</i>), and other payment and chip data elements to the POS terminal via NFC, using the EMVCo’s contactless suite of specifications.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 ("520 Patent")

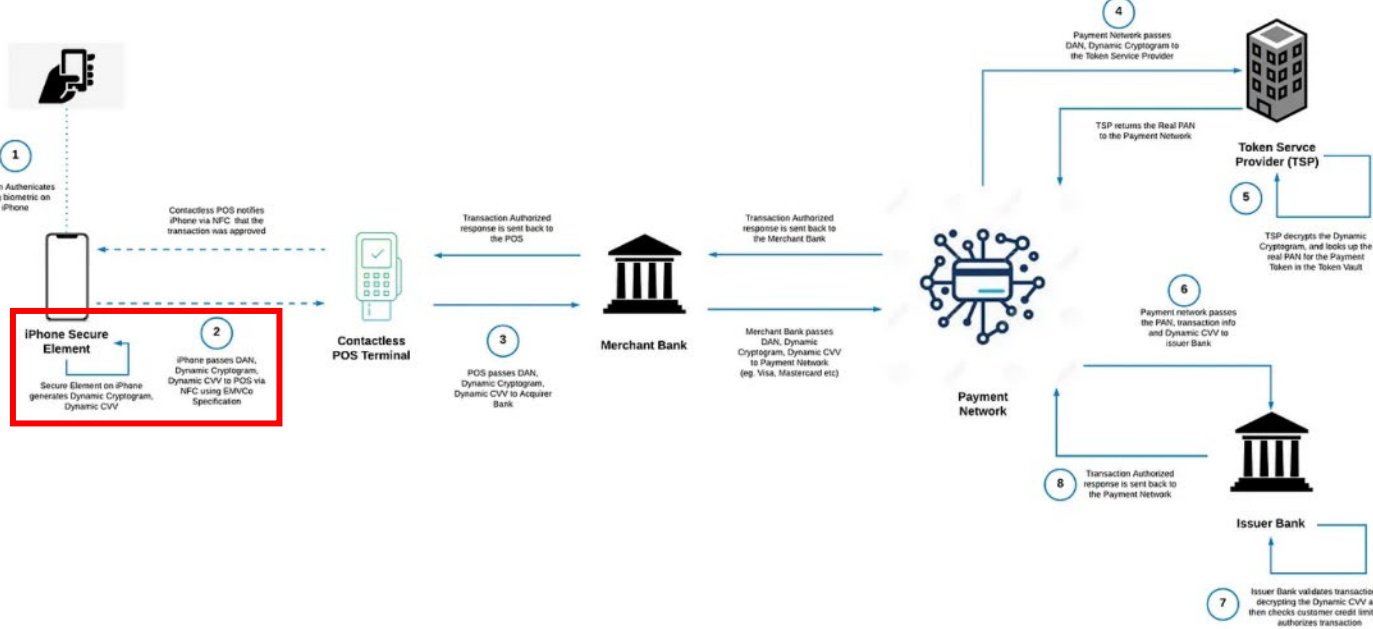
Claim No.	Accused Products
	 The diagram illustrates the Apple Pay transaction flow with the following steps: 1 Person Authenticates using Biometric on iPhone 2 iPhone passes DAN, Dynamic Cryptogram, Dynamic CVV to POS via NFC using EuiVce Specification. (This step and the iPhone Secure Element are highlighted with a red box in the original image.) 3 POS passes DAN, Dynamic Cryptogram, Dynamic CVV to Acquirer Bank 4 Payment Network passes DAN, Dynamic Cryptogram to the Token Service Provider 5 TSP returns the Real PAN to the Payment Network 6 Payment network passes the PAN, transaction info and Dynamic CVV to Issuer Bank 7 Issuer Bank validates transaction by decrypting the Dynamic CVV and then checks customer credit limit and authorizes transaction 8 Transaction Authorized response is sent back to the Payment Network Additional components and flows shown include: iPhone Secure Element: Secure Element on iPhone generates Dynamic Cryptogram, Dynamic CVV. Contactless POS Terminal: Contactless POS notifies iPhone via NFC that the transaction was approved. Merchant Bank: Transaction Authorized response is sent back to the POS; Merchant Bank passes DAN, Dynamic Cryptogram, Dynamic CVV to Payment Network (e.g., Visa, Mastercard etc). Payment Network: Transaction Authorized response is sent back to the Payment Network. Token Service Provider (TSP): TSP decrypts the Dynamic Cryptogram, and looks up the real PAN for the Payment Token in the Token Vault. Issuer Bank: Issuer Bank validates transaction by decrypting the Dynamic CVV and then checks customer credit limit and authorizes transaction. When you Pay using Apple Pay with your iPhone See, e.g., Prashant Ram, <i>How Apple Pay works under the hood?</i>, codeburst (Nov. 5, 2019), https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7. 5. End-to-End EMV Payment Tokenization Flows This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3): - In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

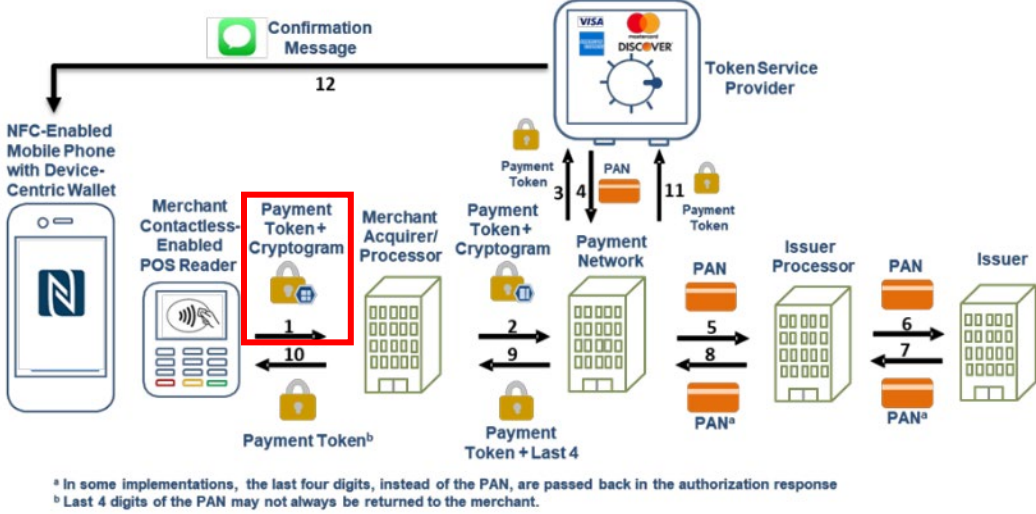
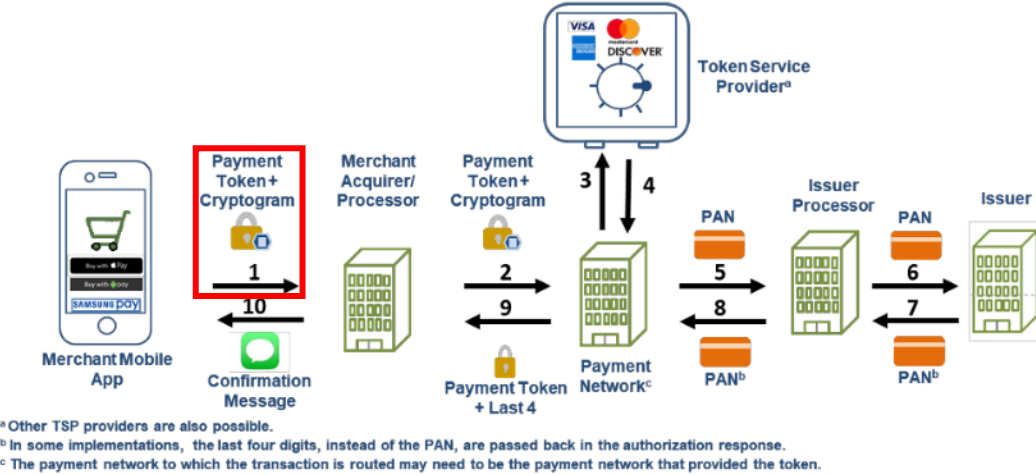
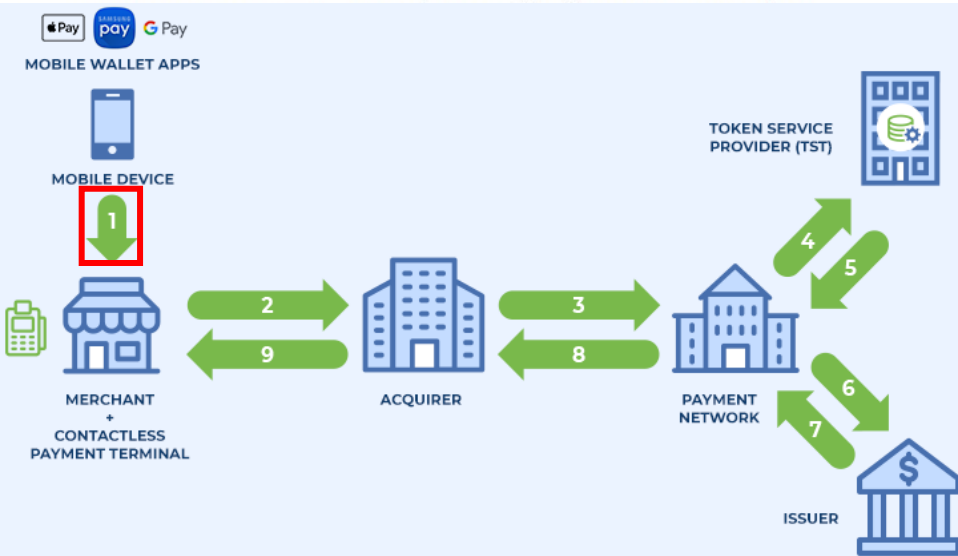
Claim No.	Accused Products
	 ^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response ^b Last 4 digits of the PAN may not always be returned to the merchant. Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet  ^a Other TSP providers are also possible. ^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response. ^c The payment network to which the transaction is routed may need to be the payment network that provided the token. Figure 7. Processing an In-App Transaction Using a Merchant Mobile App with Tokens Provisioned in a Device-Centric Wallet See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 12, 23-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	The original PAN of the card is never stored on the end user's device. Instead, the payment token with which subsequent transactions are made is securely stored. Let's walk through this: - The cardholder (in this case, the same user of the digital wallet application) makes use of the payment application, presenting the payment token to the merchant from his/her device using any of the following channels: - EMV Contactless: If the Point of Sale (POS) terminal supports contactless payments via NFC (Near Field Communication), the EMV contactless specification is used to perform the data transfer. - The merchant sends the token and dynamic cryptogram data to the acquirer. [...]  See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details (captured May 9, 2024).

Claim No.	Accused Products
2. The electronic device of claim 1, wherein the motion rate detection array comprises a set of motion rate detection units, wherein the set comprises: a plurality of inductor coils and companion magnetic-field pickup coils; an optical sensor array; and a plurality of accelerometers, and wherein a detected proximity between the electronic device and a second electronic device is determined from at least one of the set of motion rate detection units.	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, includes a motion rate detection array comprises a set of motion rate detection units, wherein the set comprises: a plurality of inductor coils and companion magnetic-field pickup coils; an optical sensor array; and a plurality of accelerometers (<i>e.g.</i>, accelerometers), and wherein a detected proximity between the electronic device and a second electronic device is determined from at least one of the set of motion rate detection units (<i>e.g.</i>, on information and belief, when Express Mode is used). <i>See supra</i> limitation 1[d]. Select Express Mode for a transit or payment card, pass, or key When you add an eligible transit card or other compatible card, pass, or key to Apple Wallet, Express Mode is turned on by default. You can also change which card, pass, or key is set to Express Mode. [. . .] - For transit, you can set one transit card to Express Mode for each transit network. You can also set a payment card that can be used to pay your fare in locations where your Express Transit card isn't accepted. How to select Express Mode for a transit or payment card, pass, or key on your iPhone - Open the Wallet app and select a card, pass, or key. - Tap the More button ⓘ, then tap Card Details. - Tap Express Transit Settings or Express Mode. - Select your preferred transit card, payment card, or other compatible pass or key. You can select a different transit or payment card for Express Transit Mode on your Apple Watch: On your iPhone, open the Apple Watch app. In the My Watch tab, tap Wallet & Apple Pay. Then tap Express Transit Card, select a transit or payment card, and authenticate on your Apple Watch with your passcode. <i>See, e.g., Use Express Mode with transit cards, passes, and keys in Apple Wallet</i>, Apple Support (Oct. 10, 2024), https://support.apple.com/en-us/105123.
3. The electronic device of claim 2, wherein the plurality of accelerometers generate an indication of the detected proximity in response to a contact between said electronic device and said second electronic device.	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, includes a plurality of accelerometers that generate an indication of the detected proximity in response to a contact between said electronic device and said second electronic device (<i>e.g.</i>, on information and belief, when Express Mode is used). <i>See supra</i> claim 2.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

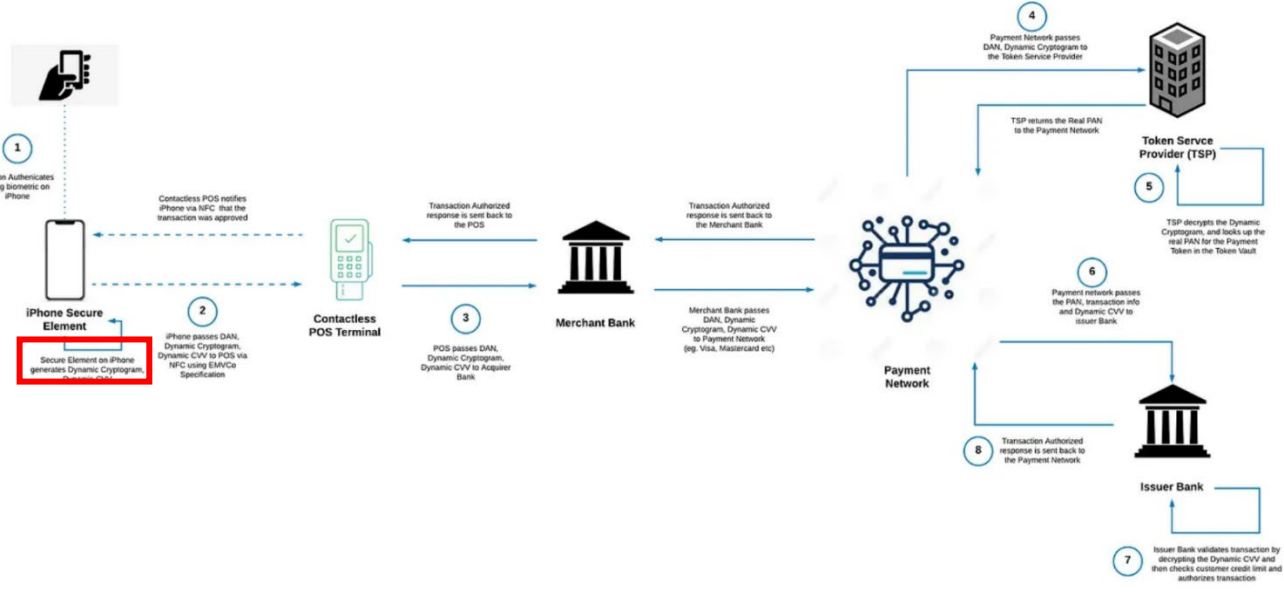
Claim No.	Accused Products
4 The electronic device of claim 1, wherein the user input comprises one or more of: an introduction of a transaction-specific identifier; a confirmation or a denial of an indicated transaction; and a lock/unlock command determining operation of the electronic device according to an input sequence or a gesture across the plurality of touch sensors.	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, accepts a user input of issued payments information input, wherein the user input comprises one or more of an introduction of a transaction-specific identifier, a confirmation or a denial of an indicated transaction (<i>e.g.</i>, tapping “Next” when entering the PAN and associated expiration date, and CVV), and, a lock/unlock command determining operation of the electronic device according to an input sequence or a gesture across the plurality of touch sensors (<i>e.g.</i>, passcode or password entry to access apps). How to add a debit or credit card on your iPhone If you have an eligible card, you can tap your card on your iPhone to add it. Or, you can add your card manually. If you have any issues adding a card, contact your card issuer. 1. In the Wallet app, tap the Add button . ◦ Tap Previous Cards to add a card that you used previously. ◦ Tap Debit or Credit Card to add a new card. 2. Tap Continue. 3. To add your card: ◦ Tap or hold your card close to your iPhone to add it. ◦ To manually add your card, tap Enter Card Details Manually and follow the onscreen instructions. 4. Some banks or card issuers might require further authentication. They might ask you to provide more information or to download an app before approving your card for use with Apple Pay. <i>See, e.g., Set Up Apple Pay</i>, Apple (Dec. 17, 2024), https://support.apple.com/en-us/108398; iPhone User Guide – iOS 18, <i>Set up Apple Pay in Wallet on iPhone</i>, Apple, https://support.apple.com/guide/iphone/set-up-apple-pay-iph9b7f53382/18.0/ios/18.0 (last visited Dec. 30, 2024).

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“’520 Patent”)

Claim No.	Accused Products
	Add a card on Apple Watch You can add Apple Account, credit, debit, and transit cards, right on Apple Watch. 1. Go to the Wallet app  on your Apple Watch. 2. Tap , then tap Add Card. 3. Choose Apple Account, Debit or Credit Card, or Transit Card; then follow the onscreen instructions. <i>See, e.g., Apple Watch User Guide – WatchOS 11, Set up Apple Pay on Apple Watch, Apple, https://support.apple.com/guide/watch/set-up-apple-pay-apd285b3ae01/watchos (last visited Dec. 29, 2024); Christian Zibreg, <i>watchOS 10 lets you add new cards to Apple Watch’s Wallet app without iPhone</i>, iDownloadBlog (Jun. 24, 2023), https://www.idownloadblog.com/2023/06/14/watchos-10-add-card-apple-watch-no-iphone/ (“[T]he watchOS 10 update supports the full Apple Pay setup process, including entering a card’s number, expiration date and security code right on the watch, even if the card has not been already added to your iPhone.” (emphasis added)).</i> Set a passcode on iPhone For better security, set a passcode that needs to be entered to unlock iPhone when you turn it on or wake it. Setting a passcode also turns on data protection, which encrypts your iPhone data with 256-bit AES encryption. (Some apps may opt out of using data protection.) <i>See, e.g., iPhone User Guide – iOS 18, Set a passcode on iPhone, Apple https://support.apple.com/guide/iphone/set-a-passcode-iph14a867ae/ios (last visited Jan. 7, 2025).</i> Unlock Apple Watch You can unlock Apple Watch manually, by entering the passcode, or set it to unlock automatically when you unlock your iPhone. • <i>Enter the passcode:</i> Wake Apple Watch, then enter the watch passcode. • <i>Unlock Apple Watch when you unlock your iPhone:</i> Go to the Apple Watch app on your iPhone, tap My Watch, tap Passcode, then turn on Unlock with iPhone. Your iPhone must be within normal Bluetooth range (about 33 feet or 10 meters) of your Apple Watch to unlock it. If Bluetooth is off on Apple Watch, enter the passcode on your watch to unlock it.  Tip: Your Apple Watch passcode can be different from your iPhone passcode—in fact, it’s better to use different passcodes. <i>See, e.g., Apple Watch User Guide – watchOS 11, Lock or unlock Apple Watch, Apple, https://support.apple.com/guide/watch/lock-or-unlock-apple-watch-apd0e1e73b6f/watchos (last visited Jan. 7, 2025).</i>

Claim No.	Accused Products
5 The electronic device of claim 1, further comprising a sequence counter which generates a sequential parameter when the processor initiates a transaction, wherein the sequential parameter is combined with any of a user information, a transaction identifier, a user secret, and a credit card authority secret and the processor is operable to generate a limited-duration credit card number therefrom.	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, comprises a sequence counter (<i>e.g.</i>, transaction counter) which generates a sequential parameter when the processor initiates a transaction, wherein the sequential parameter is combined with any of a user information (<i>e.g.</i>, as identified above), a transaction identifier, a user secret, and a credit card authority secret (<i>e.g.</i>, keys) and the processor is operable to generate a limited-duration (<i>e.g.</i>, one-time use) credit card number therefrom (<i>e.g.</i>, the dynamic cryptogram, the dynamic security code). <i>See supra</i> limitations 1[e], 1[i], 1[m]. Using a payment cryptogram for dynamic security Payment transactions originating from the payment applets include a payment cryptogram along with a Device Account Number. This cryptogram, a one-time code, is computed using a transaction counter and a key. The transaction counter is incremented for each new transaction. The key is provisioned in the payment applet during personalization and is known by the payment network or the card issuer or both. Depending on the payment scheme, other data may also be used in the calculation, including: • A Terminal Unpredictable Number, for near-field-communication (NFC) transactions • An Apple Pay server anti-replay value, for transactions within apps • User verification results, such as Cardholder Verification Method (CVM) information These security codes are provided to the payment network and to the card issuer, which allows the issuer to verify each transaction. The length of these security codes may vary based on the type of transaction. <i>See, e.g., Apple Platform Security</i>, at 183 (Dec. 2024) available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; <i>see also, e.g., Apple Platform Security, Payment authorization with Apple Pay</i>, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/payment-authorization-with-apple-pay-secc1f57e189/web. What is Advanced Fraud Protection? Advanced Fraud Protection is a way to keep your Apple Card information even more secure. After turning on Advanced Fraud Protection, your three-digit Apple Card security code will change periodically after it's been viewed in the Wallet app or after it's been auto-filled from Safari. You should check your security code each time you want to make a purchase with Apple Card to be sure you're using the most up-to-date code. You can also use Advanced Fraud Protection without affecting your recurring purchases and subscriptions, such as streaming services or memberships, because these merchants use your security code to authorize payment just once when you first sign up. <i>See, e.g., Use Advanced Fraud Protection with Apple Card</i>, Apple (Dec. 17, 2023), https://support.apple.com/en-us/102427.

Claim No.	Accused Products
	How your virtual card number works Virtual card numbers are a way to keep your payment card information even more secure. For fraud protection, your 3-digit security code changes frequently with usage and over time. You can use your virtual card number online wherever Visa is accepted. <i>See, e.g., Use your virtual card number for Apple Cash</i>, Apple (Dec. 17, 2024), https://support.apple.com/en-us/119943. When you Pay using Apple Pay with your iPhone Apple Pay uses <i>NFC</i> to send payment data to the contactless POS terminal when you Tap & Pay . Apple Pay uses the <i>EMVCo’s contactless suite of specifications</i> to pass the data from your iPhone to the contactless reader terminal. [. . .] 2. Once you authenticate yourself to the iPhone the Secure Element on the iPhone takes the following steps, (a) <i>generates a Dynamic Cryptogram</i>, - which is a combination of the <i>Payment Token</i>, <i>transaction amount</i>, <i>transaction counter etc.</i> along with the <i>Payment-Token-Key</i> (i.e. the public key provided by the TSP). (b) <i>generates a Dynamic CVV</i>, - using the <i>CVV-key</i> (i.e. the public key provided by the Issuing Bank).

Claim No.	Accused Products
	 The diagram illustrates the Apple Pay transaction process. It starts with a person authenticating on their iPhone (1). The iPhone's Secure Element generates a Dynamic Cryptogram (2). This cryptogram is sent to a Contactless POS Terminal (3). The terminal sends a Transaction Authorized response back to the iPhone (4). The iPhone then sends the response to the Merchant Bank (5). The Merchant Bank passes the DAN, Dynamic Cryptogram, and Dynamic CVV to the Payment Network (6). The Payment Network passes the DAN and Dynamic Cryptogram to the Token Service Provider (TSP) (7). The TSP returns the Real PAN to the Payment Network (8). The Payment Network then passes the Real PAN, transaction info, and Dynamic CVV to the Issuer Bank (9). Finally, the Issuer Bank validates the transaction by decrypting the Dynamic CVV and checks the customer's credit limit to authorize the transaction (10). When you Pay using Apple Pay with your iPhone See, e.g., Prashant Ram, <i>How Apple Pay works under the hood?</i>, codeburst (Nov. 5, 2019), https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7.
6 The electronic device of claim 1, wherein the limited-use number has a limited recurrence, and is limited in scope of use to a predetermined number of authorized transactions.	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, generates a limited-use number that has a limited recurrence, and is limited in scope of use to a predetermined number of authorized transactions (e.g., the dynamic cryptogram is transaction specific and thus one-time use by the device, the dynamic security code, on information and belief, has a limited recurrence and is limited in scope of use to a predetermined number of authorized transactions, or combination thereof with the DAN). When you use Apple Pay in stores After you authenticate your transaction, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code to the store's point of sale terminal along with additional information needed to complete the transaction. Again, neither Apple nor your device sends your actual payment 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 that it's unique and tied to your device.

Claim No.	Accused Products
	When you use Apple Pay within apps or on the web [. . .] To securely transmit your payment information when you pay in apps or on the web, Apple Pay receives your encrypted transaction and re-encrypts it with a developer-specific key before the transaction information is sent to the developer or payment processor. This key helps ensure that only the app or the website that you’re purchasing from can access your encrypted payment information. Websites must verify their domain every time they offer Apple Pay as a payment option. Like with in-store payments, Apple sends your Device Account Number to the app or website along with the transaction-specific dynamic security code. Neither Apple nor your device sends your actual payment card number to the app. See, e.g., <i>Apple Pay security and privacy overview</i>, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554. Using a payment cryptogram for dynamic security Payment transactions originating from the payment applets include a payment cryptogram along with a Device Account Number. This cryptogram, a one-time code, is computed using a transaction counter and a key. The transaction counter is incremented for each new transaction. The key is provisioned in the payment applet during personalization and is known by the payment network or the card issuer or both. Depending on the payment scheme, other data may also be used in the calculation, including: • A Terminal Unpredictable Number, for near-field-communication (NFC) transactions • An Apple Pay server anti-replay value, for transactions within apps • User verification results, such as Cardholder Verification Method (CVM) information These security codes are provided to the payment network and to the card issuer, which allows the issuer to verify each transaction. The length of these security codes may vary based on the type of transaction. See, e.g., <i>Apple Platform Security</i>, at 183 (Dec. 2024) available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; see also, e.g., <i>Apple Platform Security, Payment authorization with Apple Pay</i>, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/payment-authorization-with-apple-pay-secc1f57e189/web. What is Advanced Fraud Protection? Advanced Fraud Protection is a way to keep your Apple Card information even more secure. After turning on Advanced Fraud Protection, your three-digit Apple Card security code will change periodically after it's been viewed in the Wallet app or after it's been auto-filled from Safari. You should check your security code each time you want to make a purchase with Apple Card to be sure you're using the most up-to-date code. You can also use Advanced Fraud Protection without affecting your recurring purchases and subscriptions, such as streaming services or memberships, because these merchants use your security code to authorize payment just once when you first sign up. See, e.g., <i>Use Advanced Fraud Protection with Apple Card</i>, Apple (Dec. 17, 2023), https://support.apple.com/en-us/102427.

Claim No.	Accused Products
	How your virtual card number works Virtual card numbers are a way to keep your payment card information even more secure. For fraud protection, your 3-digit security code changes frequently with usage and over time. You can use your virtual card number online wherever Visa is accepted. <i>See, e.g., Use your virtual card number for Apple Cash, Apple (Dec. 17, 2024), https://support.apple.com/en-us/119943.</i>
7 The electronic device of claim 1, wherein the display enables information to be displayed regarding the limited-use number, the time, a passcode, a sequence code, a currency amount, and other credit card transaction information of the user, a merchant, a bank or a credit card authority.	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, displays information regarding the limited-use number (<i>e.g.</i>, dynamic security code), the time, a passcode, a sequence code, a currency amount, and other credit card transaction information of the user, a merchant, a bank or a credit card authority. Find your virtual card number, security code, and expiration date To make purchases online with Apple Card where Apple Pay isn't accepted yet, use your virtual card number. You can find your virtual card number on a compatible iPhone, iPad, or Apple Watch with the latest version of iOS, iPadOS, or watchOS. You can also see the last four digits of your titanium card number and your Apple Pay card number. On your iPhone 1. Open the Wallet app and tap Apple Card. 2. Tap the card number icon , then authenticate with Face ID, Touch ID, or your passcode. If you don't see the card number icon, you need to update to the latest version of iOS. 3. Next to Card Number, you can see your virtual card number. To see the last four digits of your titanium card number or Apple Pay card number, tap Additional Card Numbers. On your Apple Watch 1. Open the Wallet App and tap Apple Card. 2. Scroll down and tap Card Information, then enter your passcode. 3. Next to Card Number, you can see your virtual card number. To see the last four digits of your titanium card number or Apple Pay card number, tap Additional Card Numbers. <i>See, e.g., How to find the card numbers associated with your Apple Card, Apple (Mar. 4, 2024), https://support.apple.com/en-us/118544; Use Advanced Fraud Protection with Apple Card, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102427; Use your virtual card number for Apple Cash, Apple (Dec. 17, 2024), https://support.apple.com/en-us/119943.</i>

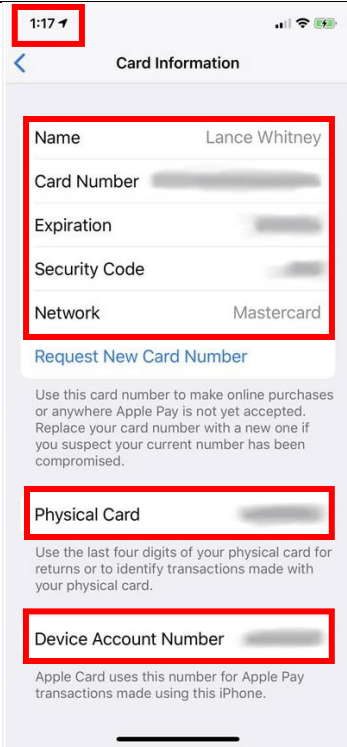
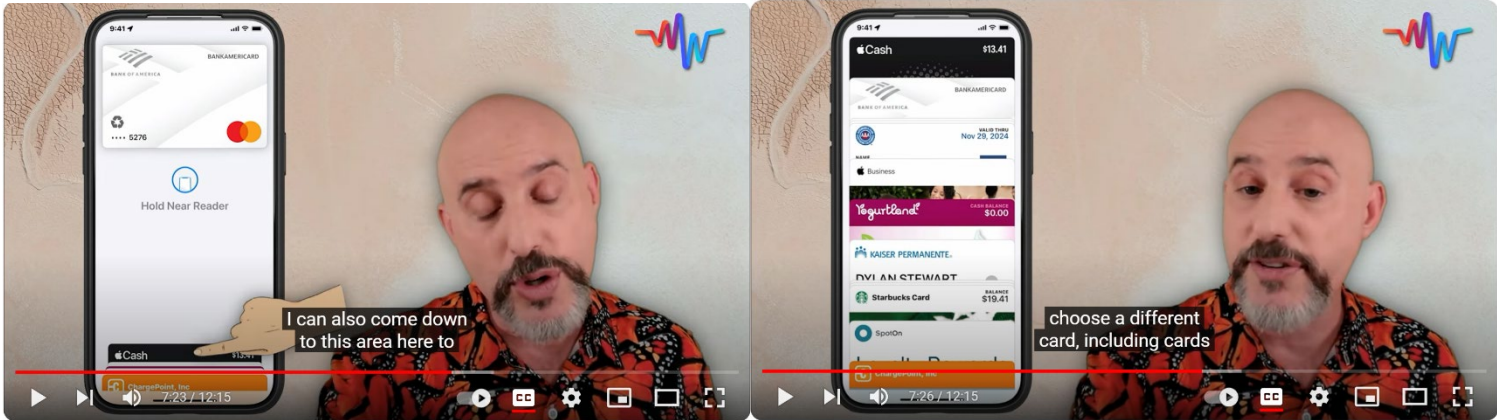
Claim No.	Accused Products
	To use your physical card at an online store or to use your virtual card online if you don't have a physical card, you'll need to have the card number, expiration, date, and security code. To get that information, turn to the Wallet app once again. Open the Wallet app on your iPhone. Select your Apple Card. Tap on the More button. At the Apple Card screen, tap the entry for Card Information. The app authenticates you via Face ID or Touch ID. The Card Information screen then displays the card number, expiration date, and security code (Figure C). Enter that information at the checkout or payment screen for the online store. See, e.g., Lance Whitney, <i>How to use your Apple Card without Apple Pay</i>, TechRepublic (Oct. 1, 2019), https://www.techrepublic.com/article/how-to-use-your-apple-card-without-apple-pay/.   See, e.g., The MacWhisperer Academy, <i>How to Use Apple Pay</i>, YouTube (Aug. 3, 2024), https://www.youtube.com/watch?v=v7hJuzw8FC0.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

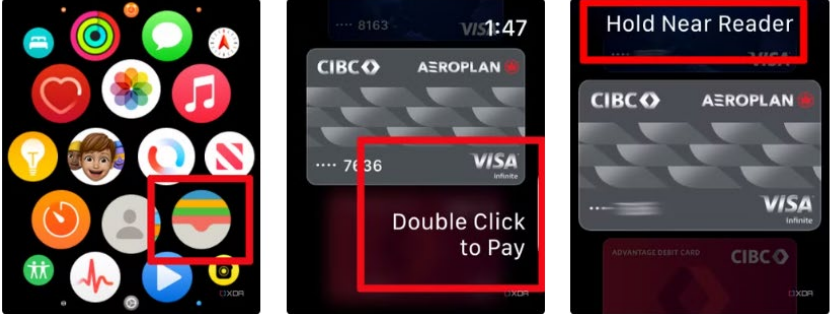
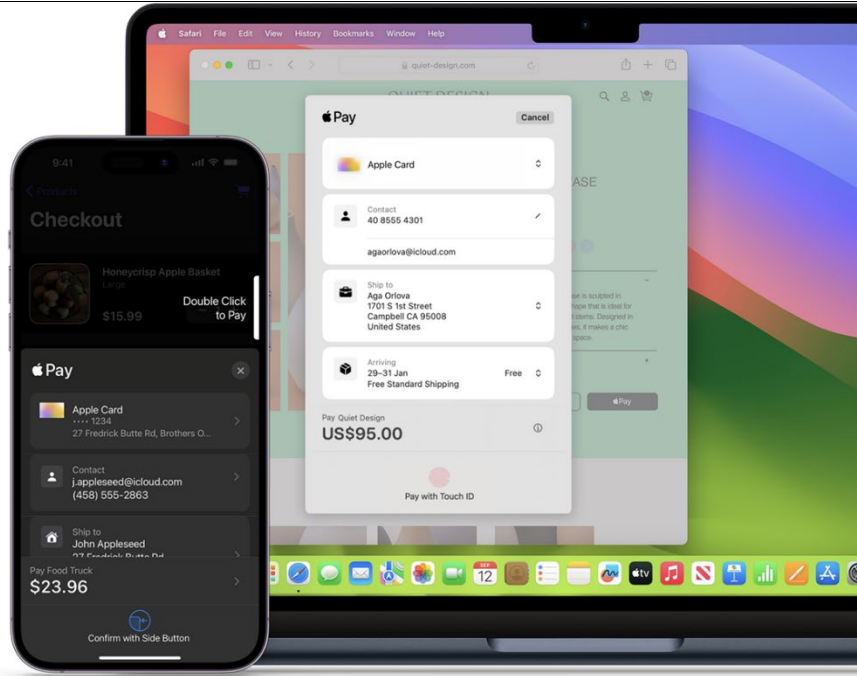
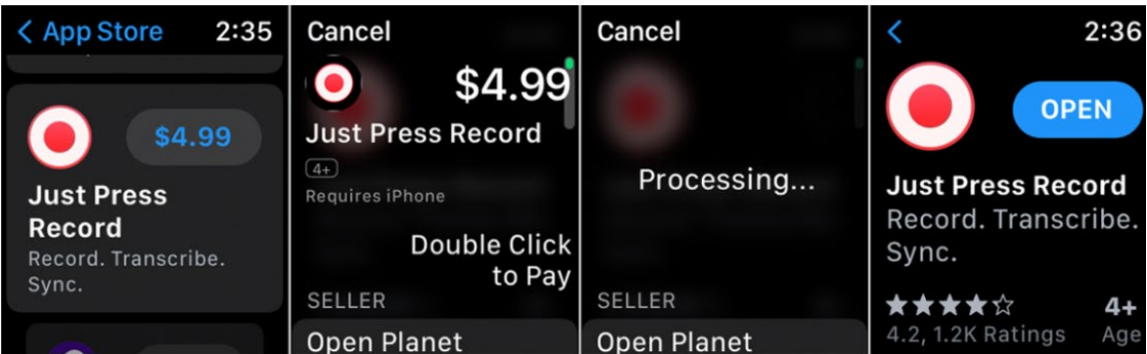
Claim No.	Accused Products
	3. Alternatively, you can manually open the Wallet app on your Apple Watch. 4. You’ll see a miniature digital version of the card you loaded or flip through multiple cards by scrolling up and down on the screen. When the card you want is on the screen, double-click the side button. 5. The message Hold Near Reader will appear at the top. 6. Twist your arm and hold the Watch face close to the contactless payment terminal at the store or venue where you’re trying to purchase something. 7. You’ll hear the confirmation beep, and the transaction will go through.  See, e.g., Christine Persaud, <i>How to use Apple Pay on your Apple Watch</i>, XDA Developers (Oct. 24, 2023), https://www.xda-developers.com/how-pay-on-apple-watch/.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	 See, e.g., Apple, <i>Apple Pay Merchant Integration Guide</i> at 3 (Jan. 2024) available at http://developer.apple.com/apple-pay/Apple-Pay-Merchant-Integration-Guide.pdf; <i>Get started with Apple Pay on the Web</i>, Apple Developer, https://developer.apple.com/videos/play/tech-talks/111381/ (last visited Dec. 20, 2024).  (Credit: Lance Whitney / Apple)

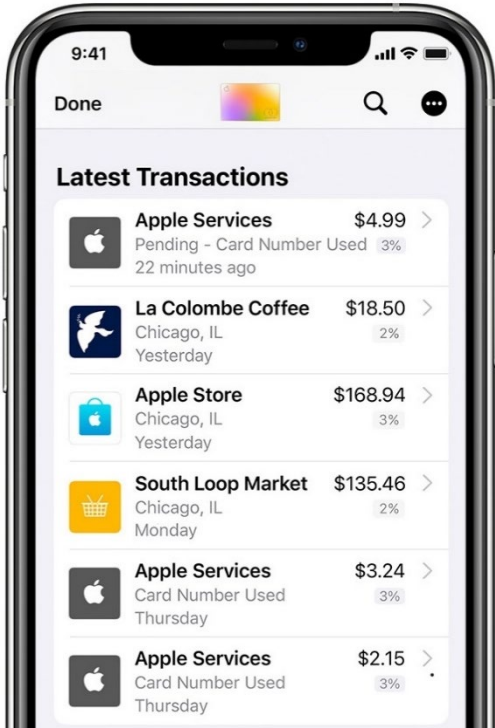
Claim No.	Accused Products
	If you want to pay for an item in a physical store or a website with your Apple Watch, double-tap the Side button on the watch to display your debit and credit cards. Tap the card you wish to use and then double-tap the Side button to purchase the item. See, e.g., Lance Whitney, <i>Pay With Your iPhone: How to Set Up and Use Apple Pay in-Store and Online</i>, PC Magazine (Sept. 14, 2023), https://www.pcmag.com/how-to/how-to-set-up-and-use-apple-pay.  See, e.g., John M Evans, <i>Apple Pay History</i>, Apple Community (Aug. 23, 2021 1:02 PM), https://discussions.apple.com/thread/253075944?sortBy=rank.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
8 The electronic device of claim 1, wherein the payment transaction comprises a cryptographic hash of the transaction unit, wherein the cryptographic hash is processed and stored in said memory.	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, makes a payment transaction comprising a cryptographic hash of the transaction unit, wherein the cryptographic hash is processed and stored in said memory. Using a shared pairing key The Secure Enclave and Secure Element communicate through a serial interface. The Secure Element links to the NFC controller, which connects to the Application Processor. Although the Secure Element and Secure Enclave don’t connect directly, they can, however, communicate securely using a secret created during runtime. In the factory, both are set up with each other’s long-term public keys. The Secure Enclave’s public key comes from its UID key and the Secure Element’s identifier. The corresponding private key is stored in hardware, hidden from software. During runtime, the long-term public keys create a shared secret using the Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol. This shared secret ensures secure communication. Authorizing a secure transaction When the user authorizes a transaction, which includes a physical gesture communicated directly to the Secure Enclave, the Secure Enclave then 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 value is generated in the Secure Enclave when a user first provisions a credit card and persists while Apple Pay is enabled, protected by the Secure Enclave encryption and anti-rollback mechanism. It’s securely delivered to the Secure Element by leveraging the pairing key. On receipt of a new AR value, the Secure Element marks any previously added cards as terminated. <i>See, e.g., Apple Platform Security</i>, at 182 (Dec. 2024) available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; <i>see also, e.g., Apple Platform Security, Payment authorization with Apple Pay</i>, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/payment-authorization-with-apple-pay-secc1f57e189/web.

Claim No.

Accused Products

Overview

Apple Pay is available on all iOS devices with a Secure Element — an industry-standard, certified chip designed to store payment information safely. In macOS, users must have an iPhone or Apple Watch that supports Apple Pay to authorize the payment, or have a Mac with Touch ID. The Secure Element creates a payment object when an app or website that uses Apple Pay sends a payment request.

The payment object has a nested structure that contains a payment token with encrypted payment data, as shown in the figure below.

The Secure Element encrypts the token's payment data using either elliptic curve cryptography (ECC) or RSA encryption. The Secure Element selects the encryption algorithm based on the merchant capabilities that the payment request indicates. Most regions use ECC encryption. Other regions use RSA encryption if ECC encryption is unavailable due to regulatory concerns.

Payment token structure

The `paymentData` property of `PKPaymentToken` (or the `paymentData` property of `ApplePayPaymentToken`, for Apple Pay on the Web) contains a UTF-8 serialization of a plaintext JSON dictionary with the following keys and values:

Key	Value	Description
header	header dictionary	Additional version-dependent information you use to decrypt and verify the payment See Header Keys and Values below.

Header keys and values

The `header` contains the following keys and values:

applicationData	SHA-256 hash, hex encoded as a string	Optional. Hash of the <code>applicationData</code> property of the original <code>PKPaymentRequest</code> object for transactions that initiate in apps. For transactions that initiate in Apple Pay on the Web, the value is the hash of <code>applicationData</code> in <code>ApplePayPaymentRequest</code> or of <code>applicationData</code> in <code>ApplePayRequest</code> . This key is omitted if the value of that property is <code>nil</code> .
publicKeyHash	SHA-256 hash, Base64 encoded as a string	Hash of the X.509 encoded public key bytes of the merchant's certificate

PKPaymentToken Object

Transaction ID

Payment network

Payment token data

Signature Header

Encrypted Payment data

Amount

Cardholder name

⋮

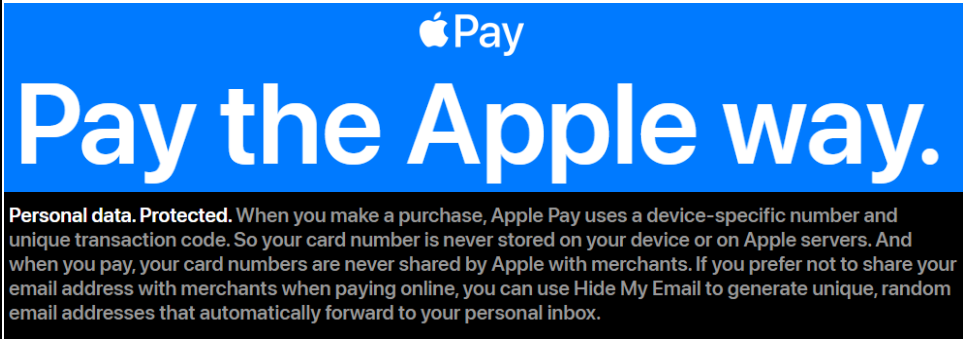
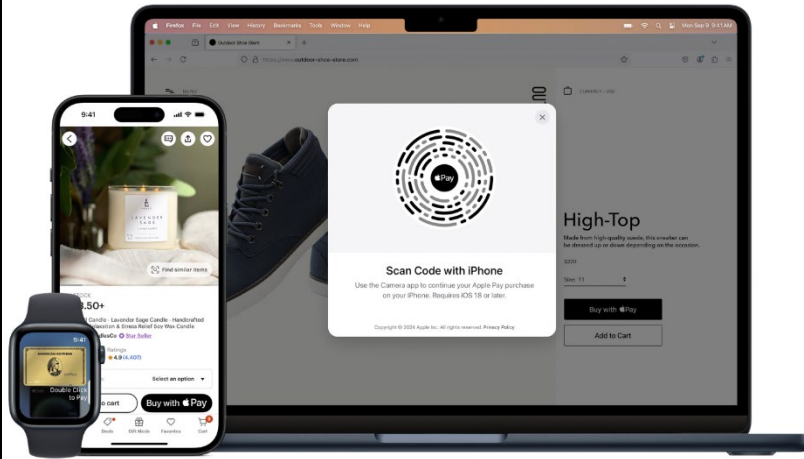
Payment processing data

See, e.g., *Payment token format reference*, Apple Developer, https://developer.apple.com/documentation/passkit_apple_pay_and_wallet/apple_pay/payment_token_format_reference (last visited Dec.. 30, 2024).

See, e.g., *Payment token format reference*, Apple Developer, https://developer.apple.com/documentation/passkit_apple_pay_and_wallet/apple_pay/payment_token_format_reference (last visited Dec.. 30, 2024).

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
9 The electronic device of claim 1, further comprising a USB connector for connection to a standard computing device.	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone, comprises a USB connector for connection to a standard computing device. iPhone 16 Pro Max   USB-C Supports USB 3 for up to 20x faster transfers^o iPhone 16 Pro   USB-C Supports USB 3 for up to 20x faster transfers^o iPhone 16   USB-C Supports USB 2 See, e.g., <i>Compare iPhone Models</i>, Apple, https://www.apple.com/iphone/compare/ (last visited Dec. 29, 2024). Connect iPhone and your computer with a cable You can use a cable to directly connect your iPhone to a Mac with OS X 10.9 or later, or to a Windows device with Windows 7 or later. Using the charging cable for your iPhone, connect iPhone to the USB port on your computer. If the cable isn't compatible with the port on your computer, you'll need to use an adapter (sold separately). See, e.g., iPhone User Guide – iOS 18, <i>Connect iPhone and your computer with a cable</i>, Apple, https://support.apple.com/guide/iphone/connect-iphone-and-your-computer-with-a-cable-iph42d9b3178/ios (last visited Dec. 30, 2024).

Claim No.	Accused Products
10 [Pre]: A method of storing and generating payment information in an electronic device, the method comprising:	To the extent the preamble is limiting, an Apple Pay- and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—is an electronic device that practices a method of storing payment information (e.g., a DAN and associated expiration date and keys) and generating payment information (e.g., a dynamic cryptogram, dynamic security code, or any combination including one or more of these, e.g., with the DAN) comprising the following limitations.  Personal data. Protected. When you make a purchase, Apple Pay uses a device-specific number and unique transaction code. So your card number is never stored on your device or on Apple servers. And when you pay, your card numbers are never shared by Apple with merchants. If you prefer not to share your email address with merchants when paying online, you can use Hide My Email to generate unique, random email addresses that automatically forward to your personal inbox.  At stores and more. Apple Pay is accepted at over 85 percent of retailers in the U.S., so you can likely use it wherever and however you want. If you’re not sure, just ask. Apple Pay works anywhere that takes contactless payments — from vending machines and grocery stores to taxis and subway stations. In apps and online. Use Apple Pay to seamlessly make purchases in Safari and other browsers — on iPhone, iPad, Mac, and other computers — without the lengthy checkout forms. On an Apple device, click or tap the Apple Pay button and pay with a touch or glance. On a non-Apple device, scan the Apple Pay code with your iPhone camera and use your iPhone to complete your purchase.⁵ You can even use Apple Pay to subscribe to services like Apple Music, Apple News+, and Apple TV+, buy apps and games on the App Store, and upgrade your iCloud storage. See, e.g., <i>Apple Pay</i>, Apple, https://www.apple.com/apple-pay/ (last visited Dec. 29, 2024); <i>Devices compatible with Apple Pay</i>, Apple (Nov. 22, 2024), https://support.apple.com/en-us/102896; Abby Ferguson, <i>How to set up Apple Pay</i>, Popular Sci. (May 12, 2024 3:04 PM EDT), https://www.popsoci.com/diy/how-to-set-up-apple-pay/ (“[The Wallet app] is pre-installed on Apple devices, so you won’t need to install it first.”).

Claim No.	Accused Products
	When you add credit, debit, prepaid, or transit cards [. . .] After your card is approved, your bank, your bank’s authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such as the key used to generate dynamic security codes that are unique to each transaction) to Apple. The Device Account Number can’t be decrypted by Apple but is stored in the Secure Element—an industry-standard, certified chip designed to store your payment information safely—on your device. Unlike with usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS, watchOS, and macOS, is never stored on Apple servers, and is never backed up to iCloud. When you use Apple Pay in stores [. . .] After you authenticate your transaction, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code to the store’s point of sale terminal along with additional information needed to complete the transaction. Again, neither Apple nor your device sends your actual payment 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 that it’s unique and tied to your device. When you use Apple Pay within apps or on the web [. . .] To securely transmit your payment information when you pay in apps or on the web, Apple Pay receives your encrypted transaction and re-encrypts it with a developer-specific key before the transaction information is sent to the developer or payment processor. This key helps ensure that only the app or the website that you’re purchasing from can access your encrypted payment information. Websites must verify their domain every time they offer Apple Pay as a payment option. Like with in-store payments, Apple sends your Device Account Number to the app or website along with the transaction-specific dynamic security code. Neither Apple nor your device sends your actual payment card number to the app. <i>See, e.g., Apple Pay security and privacy overview, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554.</i> Understanding Apple Pay Most active Apple devices are compatible with Apple Pay. It works in apps, on Safari and in web views on iOS or iPadOS devices, and through Safari on macOS. Any transaction type you currently support for regular debit and credit cards can be performed with Apple Pay, including refunds.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	Payment flow Apple Pay uses device-specific tokenized credit or debit card credentials (DPAN) in place of a Payment Account Number (PAN). When users authenticate the payment using Face ID, Touch ID or their passcode, the tokenized card data is returned to your app or website. This token can then be passed to your Payment Service Provider (PSP) to process as you would for a typical online credit or debit card payment. See, e.g., Apple, <i>Apple Pay Merchant Integration Guide</i> (Jan. 2024) available at https://developer.apple.com/apple-pay/Apple-Pay-Merchant-Integration-Guide.pdf; Apple Vision Pro User Guide, <i>Set up Apple Pay on your Apple Vision Pro</i>, Apple, https://support.apple.com/guide/apple-vision-pro/set-up-apple-pay-tanecad663c3/visionos (last visited Dec. 30, 2024) (“After you set up Apple Pay, you can make secure payments in apps and on websites that support Apple Pay. You can also send and receive money from friends and family in Messages and make purchases from participating businesses.”). 5. End-to-End EMV Payment Tokenization Flows This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3): In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) [...] Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet ^aID&V methods includes text or email or call. OTP is an example. ^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

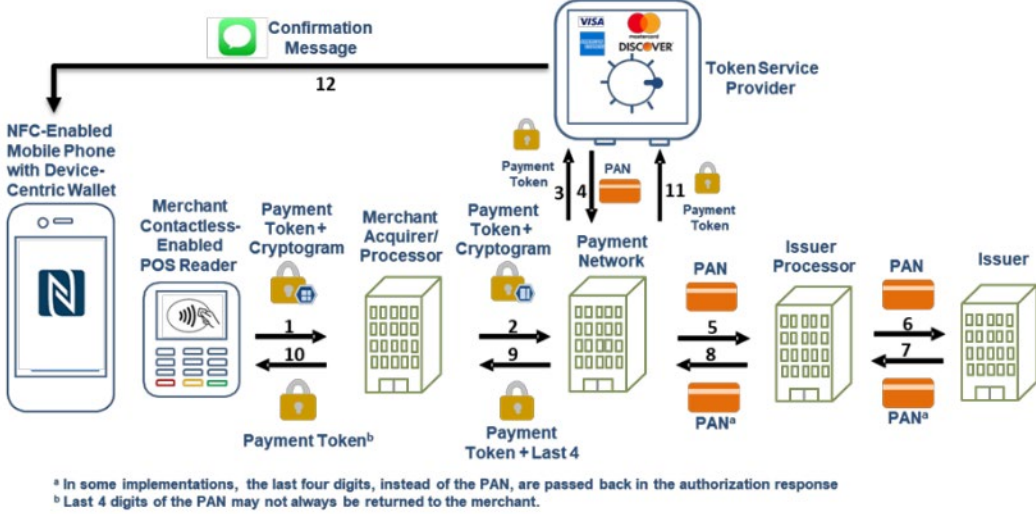
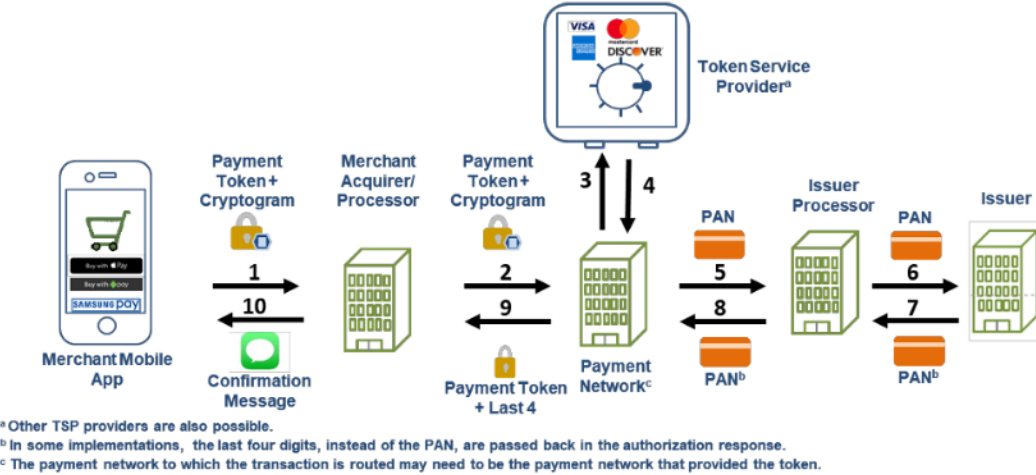
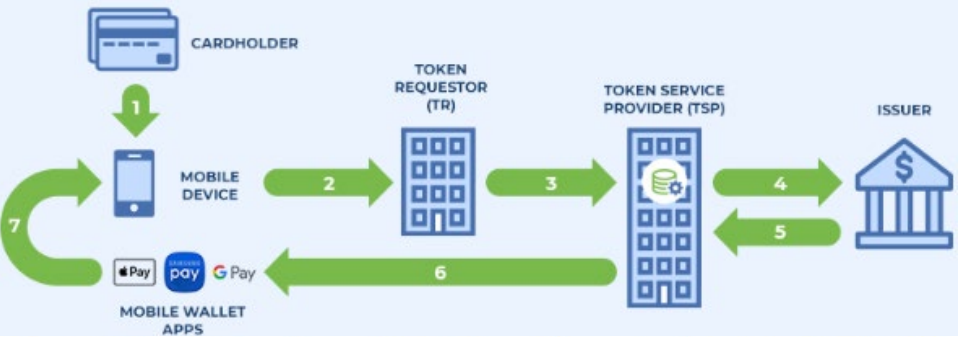
Claim No.	Accused Products
	 ^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response ^b Last 4 digits of the PAN may not always be returned to the merchant. Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet  ^a Other TSP providers are also possible. ^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response. ^c The payment network to which the transaction is routed may need to be the payment network that provided the token. Figure 7. Processing an In-App Transaction Using a Merchant Mobile App with Tokens Provisioned in a Device-Centric Wallet See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 12, 23-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	5. If everything is correct, the TSP registers the PAN and links it to a new token in a secure database (<i>Token Vault</i>). Along with the TR identifier, the token expiration date, and a number of additional security features called <i>Token Domain</i>, including restrictions on the use of the new token on certain channels, use by a particular merchant, limitation on the number of permitted uses, and verification of the cryptogram. 6. The TSP notifies the application of the newly generated token. 7. The application stores the generated token (<i>Device Account Number</i> (DAN) for Apple Pay or Digitized PAN (DPAN) for Samsung Pay) in a secure location (Secure Element (SE) or Host Card Emulation (HCE)).  The original PAN of the card is never stored on the end user's device. Instead, the payment token with which subsequent transactions are made is securely stored. Let's walk through this: 1. The cardholder (in this case, the same user of the digital wallet application) makes use of the payment application, presenting the payment token to the merchant from his/her device using any of the following channels: • EMV Contactless: If the Point of Sale (POS) terminal supports contactless payments via NFC (Near Field Communication), the EMV contactless specification is used to perform the data transfer. [...] 2. The merchant sends the token and dynamic cryptogram data to the acquirer.

Claim No.	Accused Products
	The diagram illustrates the tokenization process for mobile payments. It shows the flow between Mobile Wallet Apps (Apple Pay, Google Pay), Mobile Device, Merchant (Contactless Payment Terminal), Acquirer, Payment Network, Token Service Provider (TST), and Issuer. The process is numbered 1 through 9, showing the generation and use of a payment token. See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details (captured May 9, 2024). 5.1.3.2 Token Generation Token Generation is the process of creating a Payment Token and its associated Token Expiry Date and mapping it to a specific underlying PAN, for use by a specific Token Requestor and Token Domain(s), as identified the Token Requestor ID. The Token Service Provider SHALL facilitate the generation of a Payment Token and related data. This may be in response to a Token Request from a registered Token Requestor with a valid Token Requestor ID or an existing Payment Token may be mapped to an underlying PAN in response to a Token Request from a registered Token Requestor with a valid Token Requestor ID. 5.1.3.3 Token Issuance Token Issuance is the process of issuing a Payment Token and related data in preparation for Token Provisioning. The Token Service Provider SHALL manage Token Requests based on the Token Requestor ID. Token Service Providers SHALL manage the issuance of Payment Tokens. Payment

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	Tokens SHALL only be issued through the response to a Token Request from a registered Token Requestor with a valid Token Requestor ID. 5.1.3.4 Token Provisioning Token Provisioning is the process of delivering a Payment Token and related data to the Token Location. Token Provisioning SHOULD be carried out by the Token Service Provider or by other authorised entities on its behalf. The methodologies associated with Token Provisioning may be proprietary to each Token Programme and are outside the scope of this technical framework. <i>See, e.g., EMVCo, EMV® Payment Tokenisation Specification – Technical Framework v2.1 at 35–36 (Jun. 14, 2019).</i>
10[a]: accepting a user input of issued payment information input at a touch screen display of the electronic device, wherein the information comprises an issuer provided payment information;	An Apple Pay- and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—accepts a user input of issued payment information input at a touch screen display of the electronic device (<i>e.g.</i>, manual entry using via the touchscreen or confirmation via touchscreen of a scanned card information), wherein the information comprises an issuer provided payment information (<i>e.g.</i>, PAN or associated expiration date, or CVV). <i>See supra</i> limitation 1[h]. To the extent that adding new cards to an Apple Watch using a paired iPhone does not meet this limitation literally, CardWare contends that it is met under the doctrine of equivalents because it performs the same function in the same way to achieve the same result (<i>i.e.</i>, accepting user inputs of issuer provided payment information via a touchscreen (<i>i.e.</i>, iPhone touchscreen) to add a payment card to an Apple Watch). How to add a debit or credit card for Apple Pay on your Mac, iPad, or Apple Vision Pro - On your device, open Wallet & Apple Pay settings. - On your Mac model with Touch ID, go to System Settings (or System Preferences) > Wallet & Apple Pay. - On your iPad or Vision Pro, go to Settings > Wallet & Apple Pay. - Select Add Card.^{3,4} - Follow the steps on the screen to add a card. - Verify your information with your bank or card issuer. They might ask you to provide information. <i>See, e.g., Set Up Apple Pay, Apple</i> (Dec. 17, 2024), https://support.apple.com/en-us/108398; <i>see also, e.g., Mac User Guide – macOS Sequoia 15, Use Wallet & Apple Pay on Mac, Apple</i> https://support.apple.com/en-mide/guide/mac-help/mchl4773988b/mac (last visited Dec. 30, 2024); <i>iPad User Guide – iPadOS 18, Set up Apple Pay on iPad, Apple</i>, https://support.apple.com/en-mide/guide/ipad/ipade9607428/ipados (last visited Dec. 30, 2024); <i>Apple Vision Pro User Guide</i>,

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“’520 Patent”)

Claim No.	Accused Products
	<i>Set up Apple Pay on your Apple Vision Pro</i>, Apple, https://support.apple.com/guide/apple-vision-pro/set-up-apple-pay-tanecad663c3/visionos (last visited Dec. 30, 2024).
10[b]: wherein the electronic device comprises device-specific and user-specific information; and	An Apple Pay- and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—comprises device-specific information (<i>e.g.</i>, serial number, IMEI, etc.) and user-specific information (<i>e.g.</i>, phone number, account information, birthdate, etc.). <i>See supra</i> limitation 1[i]. See the name, model, iPadOS version, serial number, and more Go to Settings  > General > About. The items you can view include: • Name • iPadOS software version • Model name • Part and model numbers. To the right of Model, the part number appears. To see the model number, tap the part number. • Serial number • Network (Wi-Fi + Cellular models) • Number of songs, videos, photos, and apps • Capacity and available storage space • Capacity and available storage space • Carrier (Wi-Fi + Cellular models) • Cellular Data Number (Wi-Fi + Cellular models) • Wi-Fi and Bluetooth® addresses • ICCID (Integrated Circuit Card Identifier, or Smart Card) for GSM networks (Wi-Fi + Cellular models) • MEID (Mobile Equipment Identifier) for CDMA networks (Wi-Fi + Cellular models) • Modem firmware <i>See, e.g.</i>, iPad User Guide – iPadOS 18, <i>Get information about your iPad</i>, Apple, https://support.apple.com/guide/ipad/get-information-about-your-ipad-ipad63858994/ipados (last visited Dec. 30, 2024).
10[c]: wherein the issuer provided payment information is communicated wirelessly; and	An Apple Pay- and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—wirelessly (<i>e.g.</i>, via Wi-Fi or cellular network) communicates issuer provided payment information (<i>e.g.</i>, PAN or associated expiration date, or CVV).

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	<i>See supra</i> limitation 1[j]. When adding new cards to an Apple Watch using a paired iPhone, <i>see supra</i> limitations 1[h], 10[a], the iPhone wirelessly communicates the user provided payment information. To the extent that this process does not meet this limitation literally, CardWare contends that it is met under the doctrine of equivalents because it performs the same function in the same way to achieve the same result (<i>i.e.</i>, as set out above, iPhone and Apple Watch can be used together for purposes of adding cards to Apple Pay or Apple Wallet). The combination of the iPhone and Apple Watch perform the same function (<i>i.e.</i>, providing user provided payment information (<i>e.g.</i>, to Apple or a TSP), in the same way (<i>i.e.</i>, over Wi-Fi or a cellular network) to achieve the same result (<i>i.e.</i>, receiving specific information (<i>e.g.</i>, from Apple or a TSP), <i>see infra</i> limitation 1[k], 10[d])).
10[d]: receiving wirelessly a static device account number payment information for storage on the electronic device; and wherein	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—wirelessly (<i>e.g.</i>, during card onboarding from a remote server (<i>e.g.</i>, Apple’s or a TSP’s) via Wi-Fi or cellular network) receives a static device account number payment information (<i>e.g.</i>, the DAN, and associated expiration date and keys) for storage on the electronic device (<i>e.g.</i>, in the memory of secure element). <i>See supra</i> limitations 1[j], 1[k]. When adding new cards to an Apple Watch using a paired iPhone, <i>see supra</i> limitations 1[h], 10[a], the iPhone wirelessly receives the static device account number payment information and, on information and belief, wirelessly transmits it to the Apple Watch. To the extent that the Apple Watch does not meet this limitation literally, CardWare contends that it is met under the doctrine of equivalents because it performs the same function in the same way to achieve the same result (<i>i.e.</i>, as set out above, iPhone and Apple Watch can be used together for purposes of adding cards to Apple Pay or Apple Wallet). The combination of the iPhone and Apple Watch perform the same function (<i>i.e.</i>, providing user provided payment information (<i>e.g.</i>, to a Token Service Provider (“TSP”)), <i>see supra</i> limitation 1[j], 10[c]), in the same way (<i>i.e.</i>, over a wireless connection, <i>see supra</i> limitation 1[j], 10[c]) to achieve the same result (<i>i.e.</i>, receiving static device account number payment information (<i>e.g.</i>, from a TSP)).
10[e]: at least a portion of the payment information is a limited use number for limited use by the device, in place of a issuer provided payment information; and,	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—generates payment information, at least a portion of which is a limited use number for limited use by the device (<i>e.g.</i>, the DAN, the dynamic cryptogram, the dynamic security code, or any combination thereof), in place of a issuer provided payment information (<i>e.g.</i>, PAN or associated expiration date or CVV). <i>See supra</i> limitation 1[l].
10[f]: dynamically generating a one-time limited-use number based on at least one of a set of information including: user-identifying information; user secrets; device information; device secrets; time; merchant; facility location; sequence count; payment information;	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—dynamically generates a one-time limited-use number (<i>e.g.</i>, the dynamic cryptogram or the dynamic security code) based on at least one of a set of information including: user-identifying information; user secrets; device information; device secrets (<i>e.g.</i>, DAN); time; merchant; facility location (<i>e.g.</i>, device location); sequence count (<i>e.g.</i>, transaction counter); payment information; account information (<i>e.g.</i>, payment token key, CVV-key); amount; and transaction information (<i>e.g.</i>, Terminal Unpredictable Number). <i>See supra</i> limitations 1[e], 1[i], 1[m]. For example, the dynamic cryptogram is generated using at least a sequence count (<i>e.g.</i>, a transaction counter), device secrets (<i>e.g.</i>, DAN), and a key (<i>e.g.</i>, a payment token key), and further could use facility location

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“’520 Patent”)

Claim No.	Accused Products
account information; amount; and transaction information; and	(e.g., device location) or transaction information (e.g., Terminal Unpredictable Number). The dynamic security code is generated using at least a key (e.g., a CVV-key).
10[g]: using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction.	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—uses said static device account number (e.g., the DAN) and said dynamically generated one-time limited-use number (e.g., the dynamic cryptogram or the dynamic security code) together in the place of issuer provided payment information (e.g., PAN or associated expiration date or CVV) for making a payment transaction. <i>See supra</i> limitations 1[l], 1[n].
11. The method of claim 10, wherein the electronic device is configured to accept the user input by at least one of a means comprising: a touch sensor array; a touch screen; a keypad; buttons; device motion; an accelerometer; a biometric input; a proximity contact sensor; optical sensors; an NFC unit; a wireless interface; a wired connection; a USB connection; an RF antenna; an inductor assembly.	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—is configured to accept the user input by at least one of a means comprising: a touch sensor array (e.g., manual entry using via the touchscreen or confirmation via touchscreen of a scanned card information); a touch screen (e.g., manual entry using via the touchscreen or confirmation via touchscreen of a scanned card information); a keypad; buttons; device motion; an accelerometer; a biometric input; a proximity contact sensor; optical sensors; an NFC unit; a wireless interface; a wired connection; a USB connection; an RF antenna; an inductor assembly. <i>See supra</i> limitation 1[h], 10[a]. To the extent that adding new cards to an Apple Watch using a paired iPhone does not meet this limitation literally, CardWare contends that it is met under the doctrine of equivalents because it performs the same function in the same way to achieve the same result (<i>i.e.</i>, accepting user inputs of issuer provided payment information via a touchscreen (<i>i.e.</i>, iPhone touchscreen) to add a payment card to an Apple Watch).

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
12. The method of claim 10, wherein the device-specific information comprises at least one of a set including: device identifiers; device secrets; devices keys; device usage sequence counters; and device account numbers.	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—comprises device-specific information that comprises at least one of a set including: device identifiers; device secrets; devices keys (<i>e.g.</i>, associated with previously added payment methods); device usage sequence counters (<i>e.g.</i>, transaction counter); and device account numbers (<i>e.g.</i>, DANs associated with previously added payment methods). <i>See supra</i> limitation 1[i], 10[b]. Using a payment cryptogram for dynamic security Payment transactions originating from the payment applets include a payment cryptogram along with a Device Account Number. This cryptogram, a one-time code, is computed using a transaction counter and a key. The transaction counter is incremented for each new transaction. The key is provisioned in the payment applet during personalization and is known by the payment network or the card issuer or both. Depending on the payment scheme, other data may also be used in the calculation, including: • A Terminal Unpredictable Number, for near-field-communication (NFC) transactions • An Apple Pay server anti-replay value, for transactions within apps • User verification results, such as Cardholder Verification Method (CVM) information These security codes are provided to the payment network and to the card issuer, which allows the issuer to verify each transaction. The length of these security codes may vary based on the type of transaction. <i>See, e.g., Apple Platform Security</i>, at 183 (Dec. 2024) available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; <i>see also, e.g., Apple Platform Security, Payment authorization with Apple Pay</i>, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/payment-authorization-with-apple-pay-secc1f57e189/web.
13. The method of claim 10, wherein the user-specific information comprises at least one of a set comprising: an email address; a username; a password; a PIN; a passcode; gestures; user information; bank accounts; payment information; device account numbers; merchant accounts; online accounts; currency amount; currency type; cryptocurrency address; cryptocurrency keys;	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—comprises user-specific information that comprises at least one of a set comprising: an email address; a username; a password; a PIN; a passcode; gestures; user information; bank accounts; payment information; device account numbers; merchant accounts; online accounts; currency amount; currency type; cryptocurrency address; cryptocurrency keys; private/public keys; signature information; and user secrets. <i>See supra</i> limitation 1[i], 10[b].

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
private/public keys; signature information; and user secrets.	Manage your Apple Account Because your Apple Account is used across all your devices and services, it’s important to keep your account information up to date. Simply sign in on account.apple.com² at any time to manage your account: • Update trusted phone numbers and devices that you’re currently signed in to with your Apple Account. • Change your password to help maintain the security of your account. • Update your Apple Account primary email address³ to make sure it’s an address that you use frequently. • Add additional email addresses and phone numbers to help people find and communicate with you on Apple services like FaceTime⁴, iMessage, and Find My. You can also use these email addresses to sign in to your Apple Account. • Update the birth date associated with your Apple Account. • Change your Apple Account country or region. • Manage the payment methods associated with your Apple Account. • Manage subscriptions from the App Store and other Apple media services. You can also learn how to change or update your payment information or cancel subscriptions on your iPhone, iPad, or Mac. <i>See, e.g., Manage and use your Apple Account</i>, Apple (Nov. 15, 2024), https://support.apple.com/en-us/105023; Laura McCamy, <i>How to find the phone number associated with an iPhone in 3 different ways</i>, Business Insider (Sept. 8, 2022, 3:59 PM PDT), https://www.businessinsider.com/guides/tech/how-to-find-phone-number-on-iphone.
14. The method of claim 10, further comprising rendering on the display of the electronic device the payment method types stored in the electronic device, wherein said rendering comprises rendering with images, alphanumeric characters and iconography including at least one of a set comprising: a bank logo; an issuer logo; card network icons; payment network icons; a portion of the account number; and a cardholder name.	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—renders on the display of the electronic device the payment method types stored in the electronic device, wherein said rendering comprises rendering with images, alphanumeric characters and iconography including at least one of a set comprising: a bank logo; an issuer logo; card network icons; payment network icons; a portion of the account number; and a cardholder name. How to pay using Apple Pay in stores and other places With your iPhone or Apple Watch, you can use Apple Pay in stores, restaurants, gas stations, taxis, or wherever you see the appropriate contactless payment symbols.¹

Claim No.	Accused Products
	Pay with your iPhone - To use your default card: - If your iPhone has Face ID, double-click the side button. If prompted, authenticate with Face ID or enter your passcode to open Apple Wallet. - If your iPhone has Touch ID, double-click the Home button. - To use a different card, tap your default card to see your other cards. Tap a new card and authenticate. - Hold the top of your iPhone near the contactless reader until Done and a checkmark appear on the display.  Pay with your Apple Watch - Double-click the side button. - Your default card opens automatically. Scroll down to choose another card. - Hold the display of your Apple Watch near the contactless reader until you feel a gentle tap and hear a beep. 

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

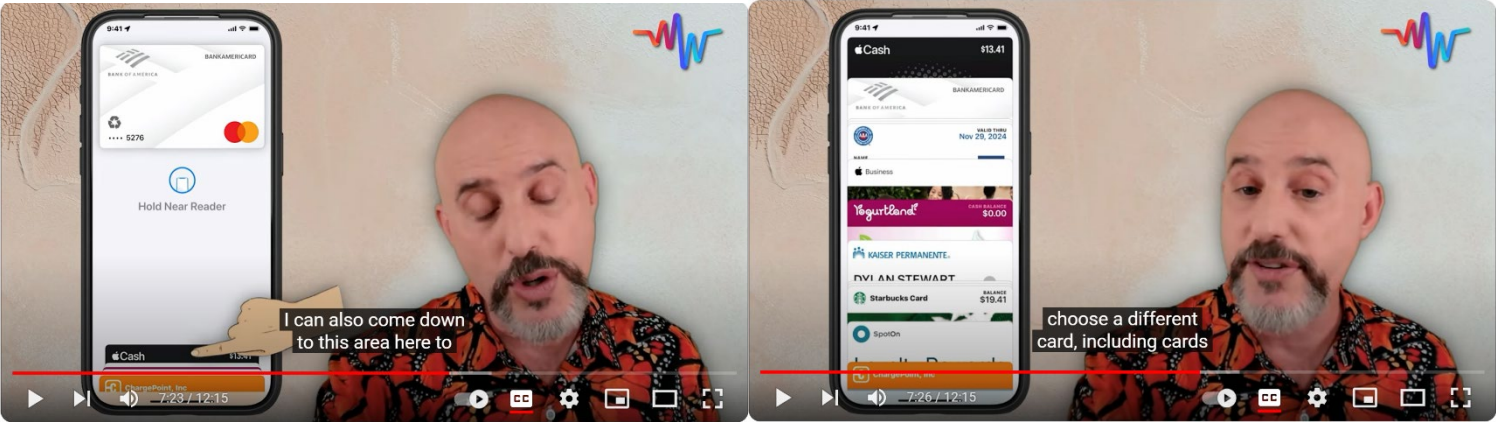
Claim No.	Accused Products
	How to use Apple Pay online or in apps You can use Apple Pay to pay online or in apps when you see Apple Pay as a payment option.^{2,3} 1. Tap the Apple Pay button or choose Apple Pay as your payment method. 2. To pay with a different card, tap Other Cards & Pay Later Options or Change Payment Method to change your default card. 3. If necessary, enter your billing, shipping, and contact information. Apple Pay stores that information, so you won't need to enter it again. 4. Confirm the payment. - o iPhone or iPad with Face ID: Double-click the side button, then use Face ID or your passcode. - o iPhone or iPad without Face ID: Use Touch ID or your passcode. - o Apple Vision Pro: Use Optic ID or your passcode. - o Apple Watch: Double-click the side button. - o Mac with Touch ID: Place your finger on Touch ID. - o Mac without Touch ID: Confirm the payment on your Bluetooth-connected iPhone or Apple Watch. Make sure that you're signed in to the same Apple Account on all devices. 5. When your payment is successful, you'll see Done and a checkmark on the screen. See, e.g., <i>Make purchases using Apple Pay</i>, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102626; Lance Whitney, <i>Pay With Your iPhone: How to Set Up and Use Apple Pay in-Store and Online</i>, PC Magazine (Sept. 14, 2023), https://www.pcmag.com/how-to/how-to-set-up-and-use-apple-pay.  See, e.g., The MacWhisperer Academy, <i>How to Use Apple Pay</i>, YouTube (Aug. 3, 2024), https://www.youtube.com/watch?v=v7hJuzw8FC0.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

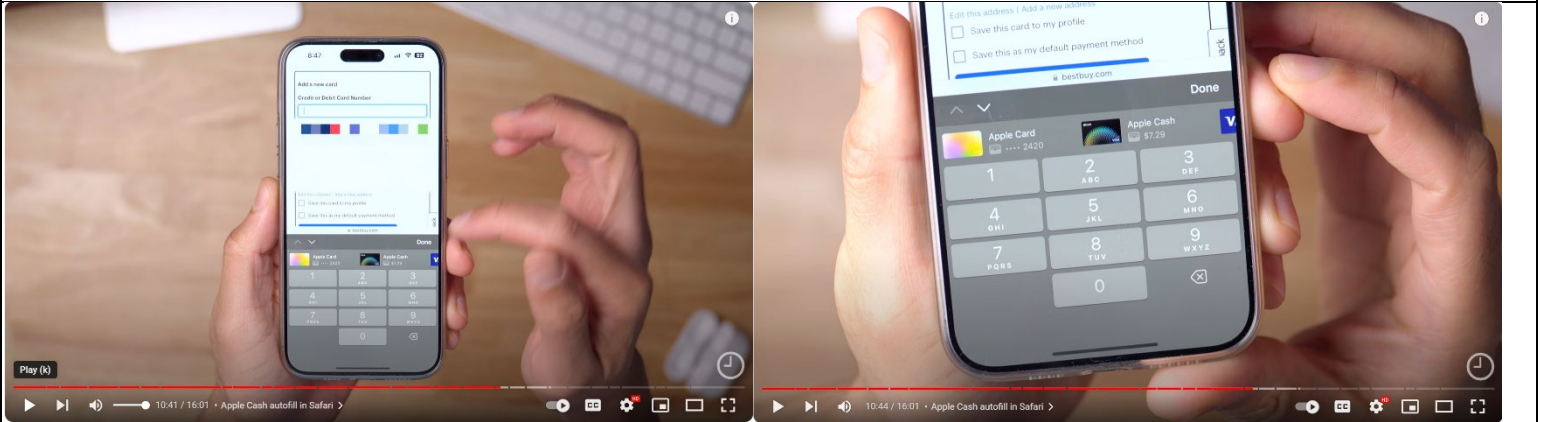
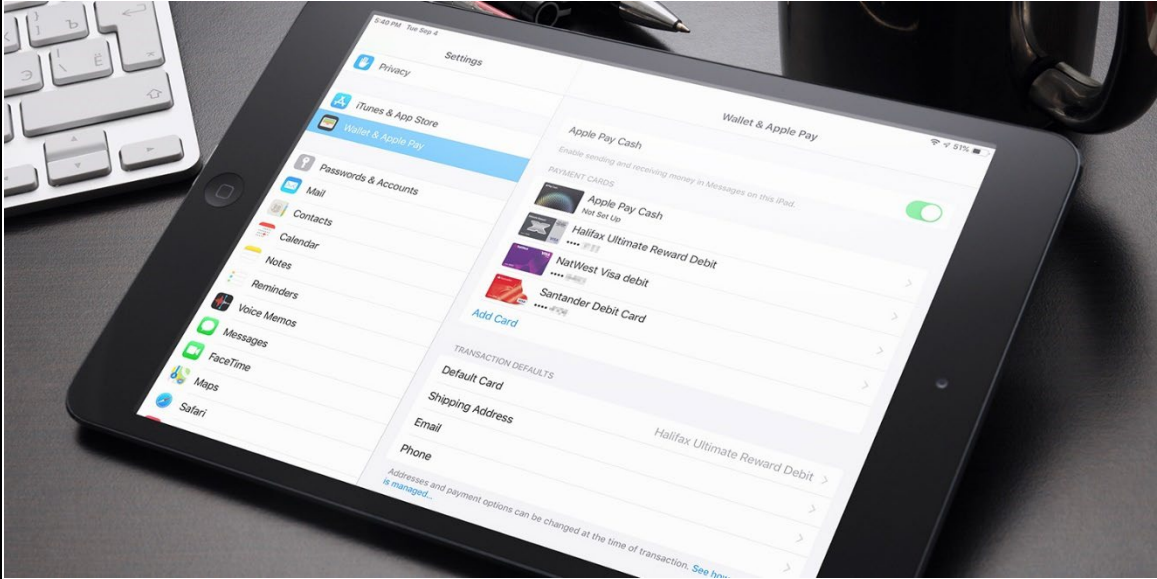
Claim No.	Accused Products
	 See, e.g., 9to5Mac, <i>iOS 17.4 – 30+ New Changes and Features</i>, YouTube (Feb. 28, 2024), https://www.youtube.com/watch?v=wT5osIMpyuQ&t=635s.  See, e.g., Tom Rolfe, <i>Apple Pay: Set Up Your Digital Wallet iPadOS 17 Guide</i>, TapSmart (Jan. 31, 2022), https://www.tapsmart.com/tips-and-tricks/ipad-apple-pay/.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
15. The method of claim 14, further comprising accepting a user selection of a payment method type for use in a transaction responsive to a user selection from a list of payment method images rendered the display and using a touch screen interface for the user selection.	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—accepts a user selection of a payment method type (<i>e.g.</i>, confirming use of the default payment method or selecting a different payment method) for use in a transaction responsive to a user selection from a list of payment method images rendered the display and using a touch screen interface for the user selection. Change your default card The first payment card that you add to Apple Wallet on a device becomes your default card for that device. When you add more cards, you can change your default card. How to change the default card for Apple Pay on your iPhone 1. Open the Wallet app. 2. Touch and hold the payment card that you want to set as your default card. 3. Drag the card in front of your other cards. How to change the default card for Apple Pay on your Apple Watch 1. On your iPhone, open the Apple Watch app. 2. In the My Watch tab, tap Wallet & Apple Pay. 3. Under Transaction Defaults, tap Default Card. 4. Tap a card to set it as your default card. How to change the default card for Apple Pay on your Mac, iPad, or Apple Vision Pro 1. On your device, open Wallet & Apple Pay settings. ◦ On your Mac with Touch ID, go to System Settings (or System Preferences) > Wallet & Apple Pay. ◦ On your iPad or Vision Pro, go to Settings > Wallet & Apple Pay. 2. Select a new default card. ◦ On your Mac with Touch ID, choose a card from the menu. ◦ On your iPad or Vision Pro, scroll down to Transaction Defaults, then tap Default Card and choose a card. <i>See, e.g., Change or remove the payment cards that you use with Apple Pay, Apple (Dec. 16, 2024), https://support.apple.com/en-us/118219.</i>

Claim No.	Accused Products
	Pay with your iPhone - To use your default card: - If your iPhone has Face ID, double-click the side button. If prompted, authenticate with Face ID or enter your passcode to open Apple Wallet. - If your iPhone has Touch ID, double-click the Home button. - To use a different card, tap your default card to see your other cards. Tap a new card and authenticate. - Hold the top of your iPhone near the contactless reader until Done and a checkmark appear on the display.  Pay with your Apple Watch - Double-click the side button. - Your default card opens automatically. Scroll down to choose another card. - Hold the display of your Apple Watch near the contactless reader until you feel a gentle tap and hear a beep. 

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

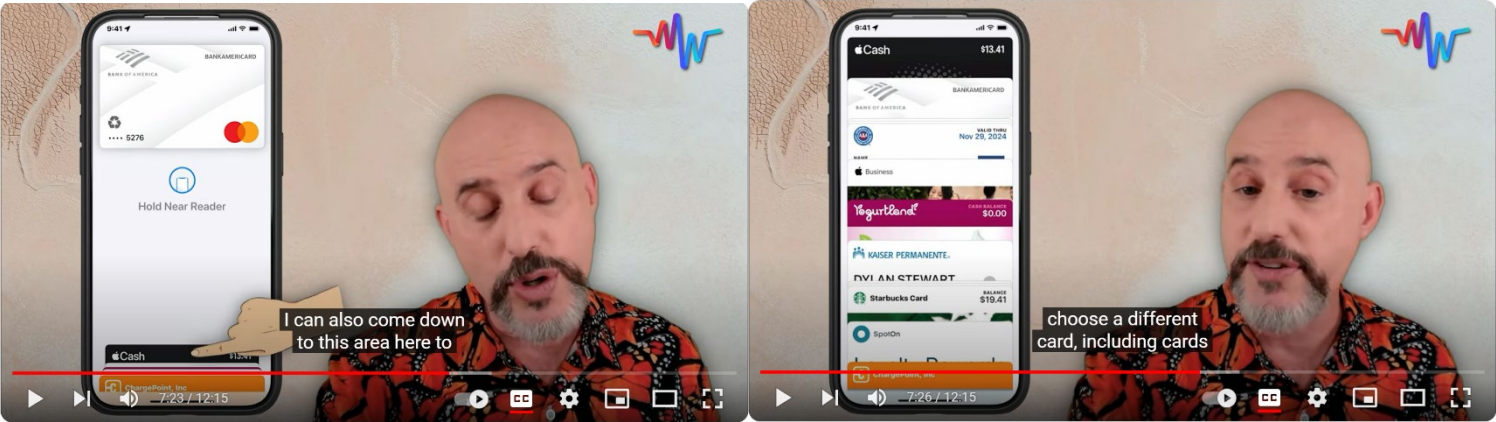
Claim No.	Accused Products
	How to use Apple Pay online or in apps You can use Apple Pay to pay online or in apps when you see Apple Pay as a payment option.^{2,3} 1. Tap the Apple Pay button or choose Apple Pay as your payment method. 2. To pay with a different card, tap Other Cards & Pay Later Options or Change Payment Method to change your default card. 3. If necessary, enter your billing, shipping, and contact information. Apple Pay stores that information, so you won't need to enter it again. 4. Confirm the payment. - o iPhone or iPad with Face ID: Double-click the side button, then use Face ID or your passcode. - o iPhone or iPad without Face ID: Use Touch ID or your passcode. - o Apple Vision Pro: Use Optic ID or your passcode. - o Apple Watch: Double-click the side button. - o Mac with Touch ID: Place your finger on Touch ID. - o Mac without Touch ID: Confirm the payment on your Bluetooth-connected iPhone or Apple Watch. Make sure that you're signed in to the same Apple Account on all devices. 5. When your payment is successful, you'll see Done and a checkmark on the screen. See, e.g., <i>Make purchases using Apple Pay</i>, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102626; Lance Whitney, <i>Pay With Your iPhone: How to Set Up and Use Apple Pay in-Store and Online</i>, PC Magazine (Sept. 14, 2023), https://www.pcmag.com/how-to/how-to-set-up-and-use-apple-pay.  See, e.g., The MacWhisperer Academy, <i>How to Use Apple Pay</i>, YouTube (Aug. 3, 2024), https://www.youtube.com/watch?v=v7hJuzw8FC0.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

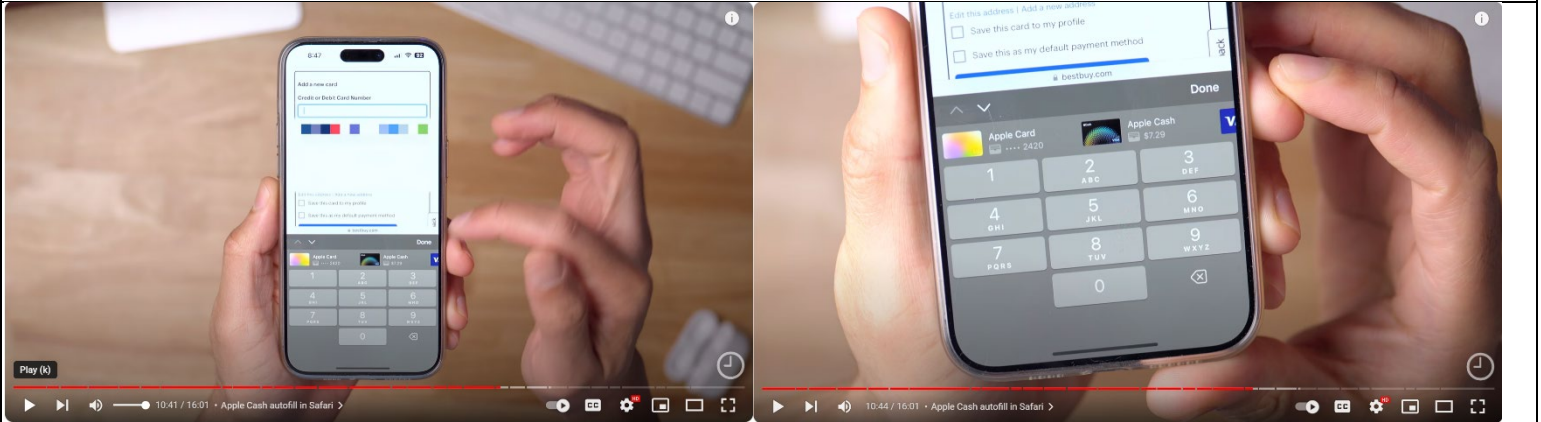
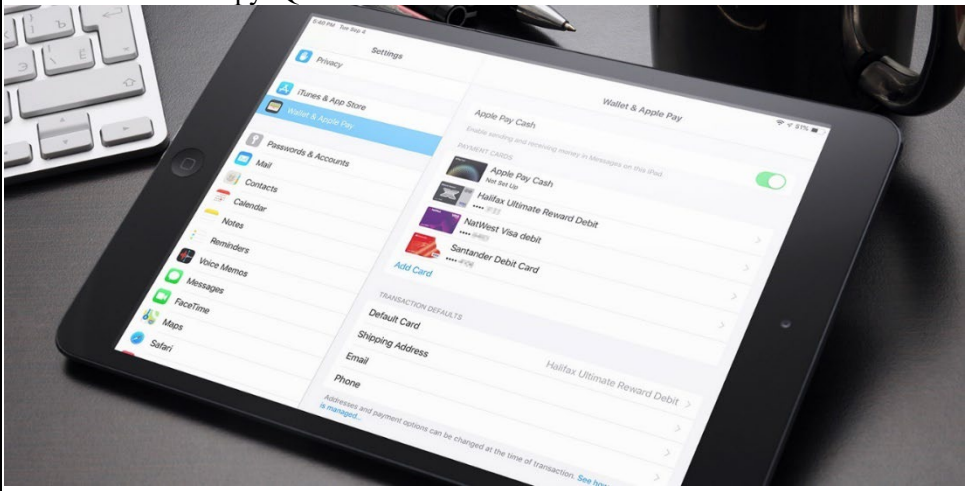
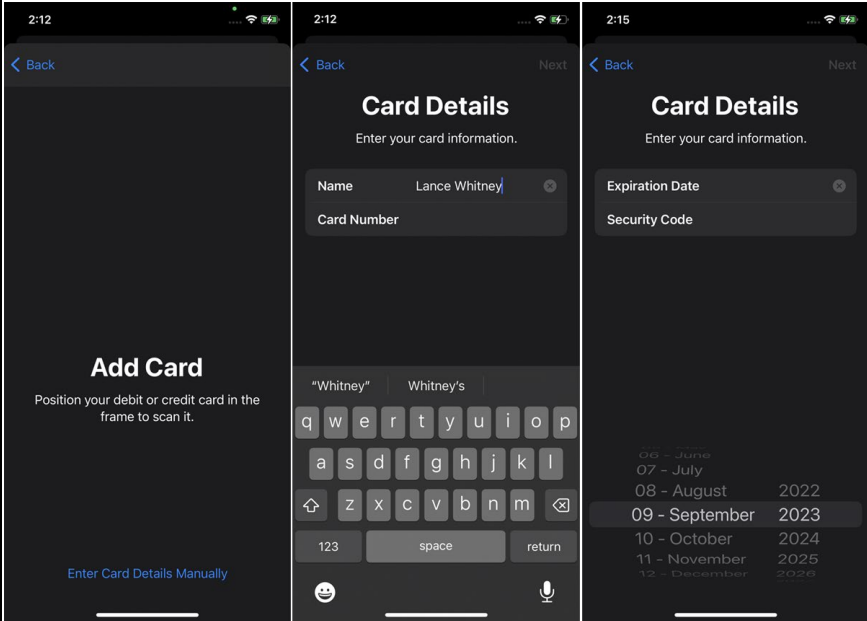
Claim No.	Accused Products
	 See, e.g., 9to5Mac, <i>iOS 17.4 – 30+ New Changes and Features</i>, YouTube (Feb. 28, 2024), https://www.youtube.com/watch?v=wT5osIMpyuQ&t=635s.  See, e.g., Tom Rolfe, <i>Apple Pay: Set Up Your Digital Wallet iPadOS 17 Guide</i>, TapSmart (Jan. 31, 2022), https://www.tapsmart.com/tips-and-tricks/ipad-apple-pay/.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
16. The method of claim 15, wherein the user selection is a default payment method to be used in transactions.	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—accepts a user selection of a default payment method to be used in transactions. Change your default card The first payment card that you add to Apple Wallet on a device becomes your default card for that device. When you add more cards, you can change your default card. How to change the default card for Apple Pay on your iPhone 1. Open the Wallet app. 2. Touch and hold the payment card that you want to set as your default card. 3. Drag the card in front of your other cards. How to change the default card for Apple Pay on your Apple Watch 1. On your iPhone, open the Apple Watch app. 2. In the My Watch tab, tap Wallet & Apple Pay. 3. Under Transaction Defaults, tap Default Card. 4. Tap a card to set it as your default card. How to change the default card for Apple Pay on your Mac, iPad, or Apple Vision Pro 1. On your device, open Wallet & Apple Pay settings. ◦ On your Mac with Touch ID, go to System Settings (or System Preferences) > Wallet & Apple Pay. ◦ On your iPad or Vision Pro, go to Settings > Wallet & Apple Pay. 2. Select a new default card. ◦ On your Mac with Touch ID, choose a card from the menu. ◦ On your iPad or Vision Pro, scroll down to Transaction Defaults, then tap Default Card and choose a card. See, e.g., <i>Change or remove the payment cards that you use with Apple Pay</i>, Apple (Dec. 16, 2024), https://support.apple.com/en-us/118219.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“’520 Patent”)

Claim No.	Accused Products
17. The method of claim 15, wherein the issuer provided payment information is selected from at least one of a set comprising: account number; card number; device account number; expiration date; card security codes; card validation values; card identification numbers; cardholder name; payment method type; merchant account; online account; an account type; a direction of transaction; the payment issuing authority; the amount of currency; the unit of currency; a funds type; cryptocurrency address; cryptocurrency key; cryptocurrency network; and card-type information.	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, or tablet—accepts a user input of issuer provided payment information selected from at least one of a set comprising: account number (<i>e.g.</i>, PAN); card number (<i>e.g.</i>, PAN); device account number; expiration date (<i>e.g.</i>, expiration date associated with PAN); card security codes (<i>e.g.</i>, CVV associated with PAN); card validation values (<i>e.g.</i>, CVV associated with PAN); card identification numbers (<i>e.g.</i>, PAN); cardholder name (<i>e.g.</i>, Name); payment method type; merchant account; online account; an account type; a direction of transaction; the payment issuing authority; the amount of currency; the unit of currency; a funds type; cryptocurrency address; cryptocurrency key; cryptocurrency network; and card-type information. <i>See supra</i> limitations 1[h], 10[a].  <i>See, e.g.</i>, Lance Whitney, <i>Pay With Your iPhone: How to Set Up and Use Apple Pay in-Store and Online</i>, PC Magazine (Sept. 14, 2023), https://www.pcmag.com/how-to/how-to-set-up-and-use-apple-pay.

Claim No.	Accused Products
18[pre] A method of facilitating and authorizing an automated teller machine (ATM) transaction involving an electronic device, wherein an electronic device transacts wirelessly with an ATM, the method comprising:	To the extent the preamble is limiting, an Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, is an electronic device that practices a method of facilitating and authorizing an automated teller machine (ATM) transaction, wherein it transacts wirelessly (e.g., via an NFC interface) with an ATM, the method comprising the following limitations. Cardless/contactless ATMs Cardless technology is found on contactless ATMs, which allow customers to tap their phones to activate an RFID reader. The machine uses a variety of technologies to read the data, but the most common one for cardless ATMs is near-field communication. Finder.com identifies other ways ATMs can connect with customer's phones including app-generated codes, QR codes or at times biometric authentication that scans fingerprints or eyes. How to use Apple/Google Pay at an ATM In order to use Apple or Google Pay at a cardless ATM, customers simply need to open their Google or Apple Pay Wallet, make sure the right debit card is selected and then tap the phone against the contactless symbol for the ATM. From there, the customer will need to enter their PIN number as usual. Of course, this will only work on ATMs that have near-field communication readers. See, e.g., Bradley Cooper, <i>Cardless ATMs deliver Google/Apple Pay</i>, atm marketplace (May 14, 2024), https://www.atmmarketplace.com/articles/cardless-atms-deliver-googleapple-pay/. Using Apple Pay at an ATM <i>With your iPhone</i> 1. If your iPhone is locked, double-click the home button to open Apple Pay. Otherwise, tap Wallet and tap your debit card. 2. Hold your iPhone near the contactless reader symbol on the ATM and keep your finger on the home button to activate Touch ID. [. . .] 3. Enter your PIN on the ATM's keypad.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	<i>With your Apple Watch</i> 1. Double-click the side button to open Apple Pay. An image for your default card will appear. If this is not your debit card, swipe to display it. 2. Hold Apple Watch near the contactless reader symbol. A gentle tap on your wrist and a beep will confirm a successful transmission. [. . .] 3. Enter your PIN on the ATM’s keypad. <i>See, e.g., Mike Matthews, How to use your iPhone and Apple Watch at an ATM, The App Factor (Dec. 7, 2016), https://theappfactor.com/using-iphone-apple-watch-atm/.</i> How to use Chase ATMs without your card To start using cardless Chase ATM access, be sure you’ve added your eligible Chase debit card to your phone’s mobile wallet app.  Step 1 Access your mobile wallet on your phone and choose your virtual Chase Debit Card.  Step 2 Look for the  symbol on the ATM, and tap it with your phone.  Step 3 Enter your PIN as usual.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	How to add a card to your phone's mobile wallet Choose your mobile wallet below or open the mobile wallet app on your phone and follow the instructions.    Apple Pay® Google Wallet™ Samsung Pay <i>See, e.g., Cardless ATM Access, Chase, https://www.chase.com/digital/atms/cardless-nfc (last visited Dec. 30, 2024).</i>
18[a] providing, by the electronic device, at least one of account information; identification; and authorization, for the ATM transaction; and,	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, provides, by the electronic device, at least one of account information (e.g., dynamic cryptogram, dynamic security code, DAN, or any combination including one or more of the same); identification (e.g., name, password, email address); and authorization (e.g., user verification results based on, e.g., passcode, password, Face ID, Touch ID, or wrist detection, or, on information and belief, Optic ID), for the ATM transaction. <i>See supra</i> claim 6. When you use Apple Pay in stores [. . .] After you authenticate your transaction, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code to the store's point of sale terminal along with additional information needed to complete the transaction. Again, neither Apple nor your device sends your actual payment 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 that it's unique and tied to your device. <i>See, e.g., Apple Pay security and privacy overview, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554.</i>

Claim No.	Accused Products
	Payment authorization with Apple Pay For devices with the Secure Element, a payment can be made only after it receives authorization from the Secure Enclave. This involves verifying that the user has confirmed their intent to pay and that the user has authenticated themselves using one of the following methods: • Biometric authentication • Device passcode or password • Double-clicking the side button of an unlocked Apple Watch Biometric authentication, if available, is the default method, but the passcode or password can be used at any time and is automatically offered after three unsuccessful attempts to match a fingerprint, or two unsuccessful attempts to match a face. After five unsuccessful attempts, the passcode or password is required. A passcode or password is also required when biometric authentication isn’t configured or turned on for Apple Pay. Using a payment cryptogram for dynamic security Payment transactions originating from the payment applets include a payment cryptogram along with a Device Account Number. This cryptogram, a one-time code, is computed using a transaction counter and a key. The transaction counter is incremented for each new transaction. The key is provisioned in the payment applet during personalization and is known by the payment network or the card issuer or both. Depending on the payment scheme, other data may also be used in the calculation, including: • A Terminal Unpredictable Number, for near-field-communication (NFC) transactions • An Apple Pay server anti-replay value, for transactions within apps • User verification results, such as Cardholder Verification Method (CVM) information These security codes are provided to the payment network and to the card issuer, which allows the issuer to verify each transaction. The length of these security codes may vary based on the type of transaction. See, e.g., <i>Apple Platform Security</i>, at 182, 183 (Dec. 2024) available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; see also, e.g., <i>Apple Platform Security, Payment authorization with Apple Pay</i>, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/payment-authorization-with-apple-pay-secc1f57e189/web.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

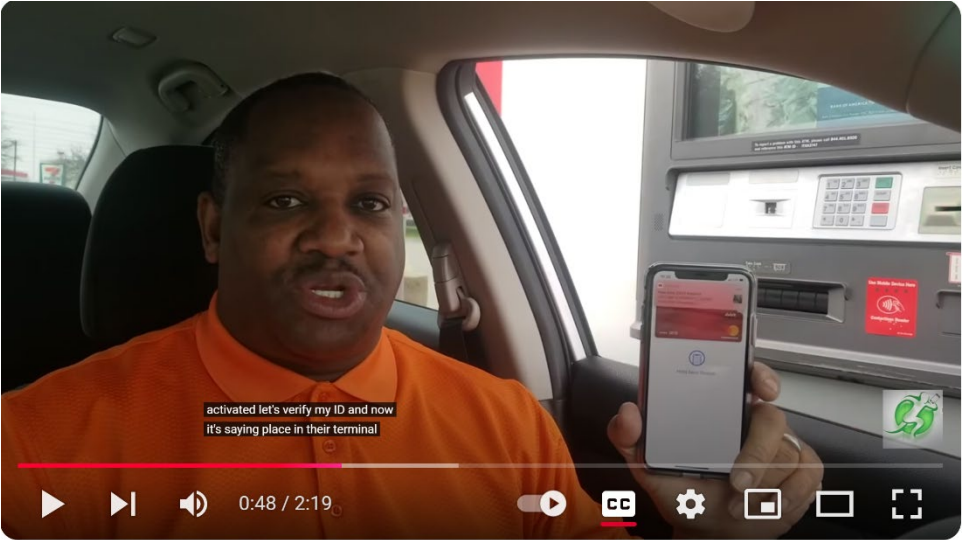
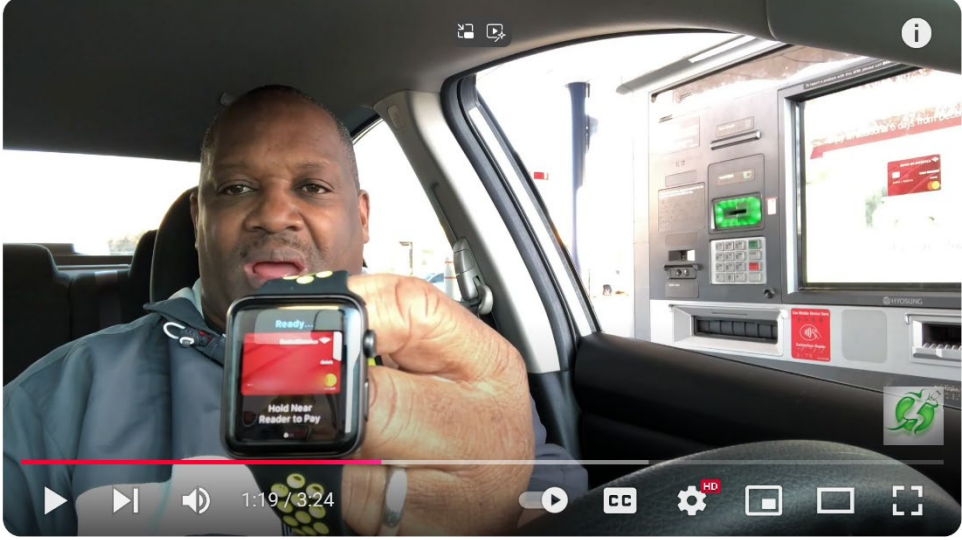
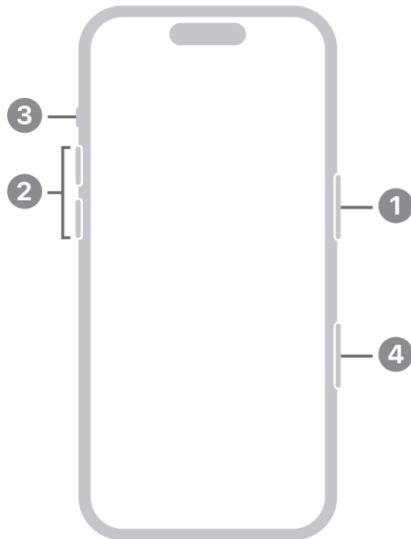
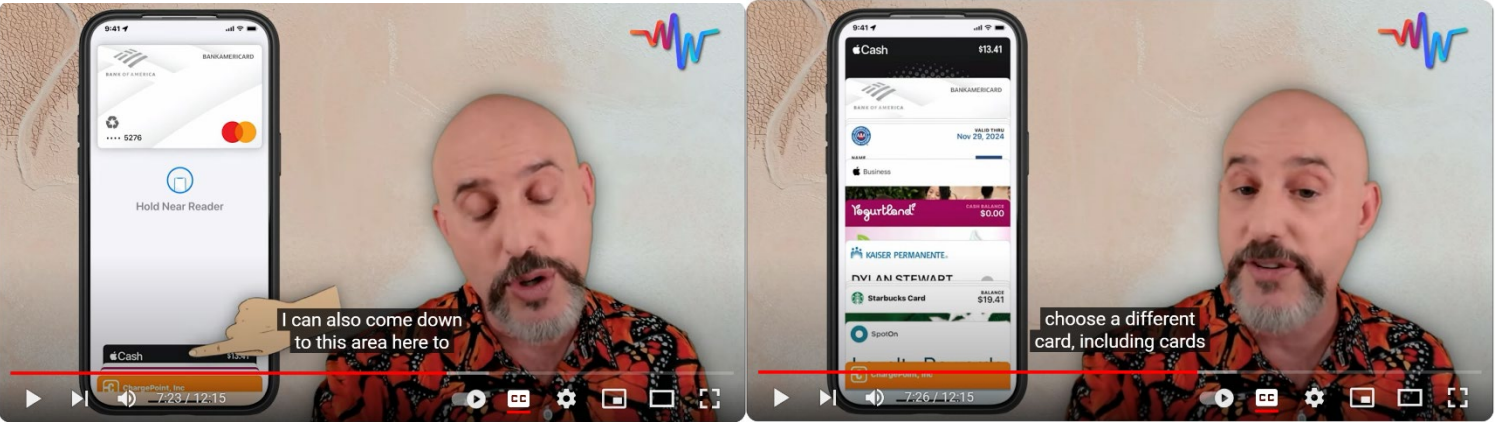
Claim No.	Accused Products
	How to use Chase ATMs without your card To start using cardless Chase ATM access, be sure you've added your eligible Chase debit card to your phone's mobile wallet app.  Step 1 Access your mobile wallet on your phone and choose your virtual Chase Debit Card.  Step 2 Look for the  symbol on the ATM, and tap it with your phone.  Step 3 Enter your PIN as usual. See, e.g., <i>Cardless ATM Access</i>, Chase, https://www.chase.com/digital/atms/cardless-nfc (last visited Dec. 30, 2024).  See, e.g., Melvin Thompson (TechRunin247), <i>How To Get Cash Out Of An ATM With Apple Pay!</i>, YouTube (Mar. 2, 2019) at 0:48, https://www.youtube.com/watch?v=axL1AJnG2Sg&t=48s.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“’520 Patent”)

Claim No.	Accused Products
	 <i>See, e.g.,</i> Melvin Thompson (TechRunin247), <i>How To Get Cash Out Of An ATM With Apple Pay and Your Apple Watch</i>, YouTube (Dec. 18, 2019) at 1:19, https://www.youtube.com/watch?v=...
18[b] wherein the electronic device comprises a user interface comprising: displays; touch sensors; and buttons; and,	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, comprises a user interface comprising: displays; touch sensors; and buttons. <i>See supra</i> limitations 1[b] and 1[c], discussing displays and touch sensors on Apple Pay and/or Apple Wallet-enabled computing devices.

Claim No.	Accused Products
	On iPhone 16 models  1: Side button: Use the side button to turn off your iPhone and to lock your iPhone. 2: Volume buttons: Use the volume up/down buttons to adjust the volume when listening to music, watching videos, or playing games. When you're not using other apps, the buttons will adjust the ringer volume. 3: Action button: You can choose what you want this button to do, including opening the Camera app or turning on the flashlight. By default, the Action button turns Silent mode on or off. Learn more about the Action button. 4: Camera Control: Use the Camera Control to quickly open your iPhone camera, capture photos or videos, and access camera settings. Learn more about the Camera Control. See, e.g., <i>Use the side button, Home button, and other controls on your iPhone</i>, Apple (Sept. 19, 2024), https://support.apple.com/en-us/105103. Press or turn the Digital Crown  • Press to see the watch face or Home screen. • Double-click to open the App Switcher. • Press and hold to use Siri. • Turn while on the watch face to use the Smart Stack. • Turn to zoom, scroll, or adjust what's on the screen. • Press and hold to unlock the screen after a water workout.

Claim No.	Accused Products
	Press the side button  • Press to show or hide Control Center. • Press and hold to use Emergency SOS. • Double-click to use Apple Pay. • Press and hold to turn your watch on or off. <i>See, e.g., Use the buttons and screen on your Apple Watch, Apple (Nov. 6, 2024), https://support.apple.com/en-us/105063.</i>
18[c] recording a user selection from the user interface of the electronic device of a user selected account from which the electronic device is operable to wirelessly convey with an ATM; and,	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, records a user selection from the user interface of the electronic device of a user selected account (e.g., the default card or another user-selected payment method) from which the electronic device is operable to wirelessly convey with an ATM.  <i>See, e.g., The MacWhisperer Academy, How to Use Apple Pay, YouTube (Aug. 3, 2024), https://www.youtube.com/watch?v=v7hJuzw8FC0.</i> 3. Alternatively, you can manually open the Wallet app on your Apple Watch. 4. You'll see a miniature digital version of the card you loaded or flip through multiple cards by scrolling up and down on the screen. When the card you want is on the screen, double-click the side button. [...]

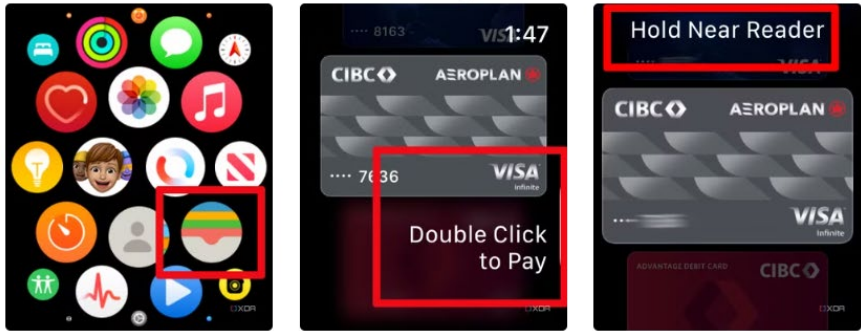
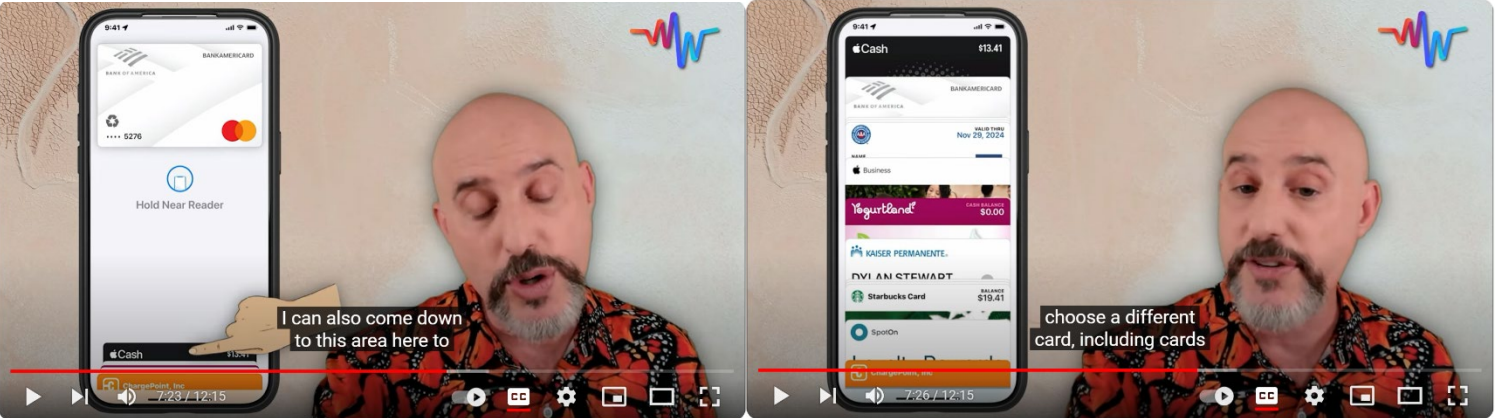
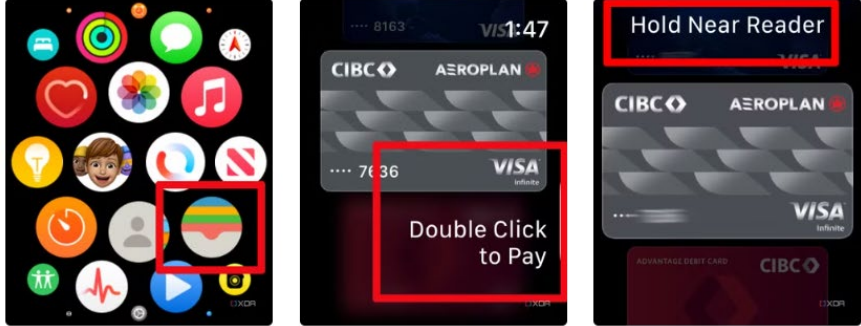
Claim No.	Accused Products
	 See, e.g., Christine Persaud, <i>How to use Apple Pay on your Apple Watch</i>, XDA Developers (Oct. 24, 2023), https://www.xda-developers.com/how-pay-on-apple-watch/.
18[d] recording a user selection from the user interface of the electronic device of a user selected account operation, wherein said user selected account operation is selected from a list of funds transfer operations; and,	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, recording a user selection from the user interface of the electronic device of a user selected account operation (e.g., contactless transaction), wherein said user selected account operation is selected from a list of funds transfer operations.  See, e.g., The MacWhisperer Academy, <i>How to Use Apple Pay</i>, YouTube (Aug. 3, 2024), https://www.youtube.com/watch?v=v7hJuzw8FC0. 3. Alternatively, you can manually open the Wallet app on your Apple Watch. 4. You'll see a miniature digital version of the card you loaded or flip through multiple cards by scrolling up and down on the screen. When the card you want is on the screen, double-click the side button. [...]

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	 See, e.g., Christine Persaud, <i>How to use Apple Pay on your Apple Watch</i>, XDA Developers (Oct. 24, 2023), https://www.xda-developers.com/how-pay-on-apple-watch/.
18[e] wherein user input information from the user interface includes at least one of a set comprising: identification, account, amount of currency, operation and authorizing information; and,	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, receives user input from the user interface including at least one of a set comprising: identification (e.g., as identified above), account, amount of currency, operation and authorizing information (e.g., as identified above). How to pay using Apple Pay in stores and other places With your iPhone or Apple Watch, you can use Apple Pay in stores, restaurants, gas stations, taxis, or wherever you see the appropriate contactless payment symbols.¹ Pay with your iPhone - To use your default card: - If your iPhone has Face ID, double-click the side button. If prompted, authenticate with Face ID or enter your passcode to open Apple Wallet. - If your iPhone has Touch ID, double-click the Home button. - To use a different card, tap your default card to see your other cards. Tap a new card and authenticate. - Hold the top of your iPhone near the contactless reader until Done and a checkmark appear on the display. 

Claim No.	Accused Products
	Pay with your Apple Watch 1. Double-click the side button. 2. Your default card opens automatically. Scroll down to choose another card. 3. Hold the display of your Apple Watch near the contactless reader until you feel a gentle tap and hear a beep.  <i>See, e.g., Make purchases using Apple Pay, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102626.</i> Pay with your default card on an iPhone with Face ID 1. Double-click the side button. 2. When your default card appears, glance at iPhone to authenticate with Face ID, or enter your passcode. 3. Hold the top of your iPhone near the card reader until you see Done or a checkmark on the screen. Pay with your default card on an iPhone with Touch ID 1. Rest your finger on Touch ID. 2. Hold the top of your iPhone near the card reader until you see Done or a checkmark on the screen. <i>See, e.g., iPhone User Guide – iOS 18, Use Apple Pay for contactless payments on iPhone, Apple, https://support.apple.com/guide/iphone/use-apple-pay-for-contactless-payments-iphbd4cf42b4/ios (last visited Dec. 27, 2024).</i> To set up Apple Pay, add a debit or credit card to the Wallet app on your iPhone, Apple Watch, or other compatible device. To use Apple Pay, you need: • A compatible device¹ with the latest version of iOS or iPadOS, watchOS, macOS, or visionOS. • A supported card from a participating card issuer. • An Apple Account signed in to your Apple device. • Face ID, Touch ID, Optic ID, or a passcode set on your device. Learn if your country/region supports Apple Pay. To check if your card is compatible with Apple Pay, contact your card issuer. <i>See, e.g., Set up Apple Pay, Apple (Sept. 25, 2024), https://support.apple.com/en-us/108398.</i>

Claim No.	Accused Products
	Use Apple Pay on Apple Watch Apple Pay offers an easy, secure, and private way to pay on your Apple Watch. With your cards stored in the Wallet app  on your iPhone and added to Apple Watch, you can use Apple Pay in the following ways: • <i>Contactless payments and apps:</i> Use the credit, debit, and prepaid cards you add to the Wallet app to make purchases in stores that accept contactless payments, and in apps that support Apple Pay. Once you set up Apple Pay in the Apple Watch app on your iPhone, you’re ready to make store purchases—even when you don’t have your iPhone with you. (Apple Pay isn’t available in all countries and regions.) [. . .] <i>Note:</i> You can’t use Apple Pay, and any cards you added to Wallet are removed, if you unpair your Apple Watch or turn off your passcode. If you turn off wrist detection, you must enter your passcode each time you use Apple Pay. <i>See, e.g.,</i> Apple Watch User Guide – watchOS 11, <i>Use Apple Pay on Apple Watch</i>, Apple, https://support.apple.com/guide/watch/apple-pay-apd76424826d/watchos (last visited Dec. 27, 2024). Press the side button  • Press to show or hide Control Center. • Press and hold to use Emergency SOS. • Double-click to use Apple Pay. • Press and hold to turn your watch on or off. <i>See, e.g.,</i> <i>Use the buttons and screen on your Apple Watch</i>, Apple (Nov. 6, 2024), https://support.apple.com/en-us/105063.

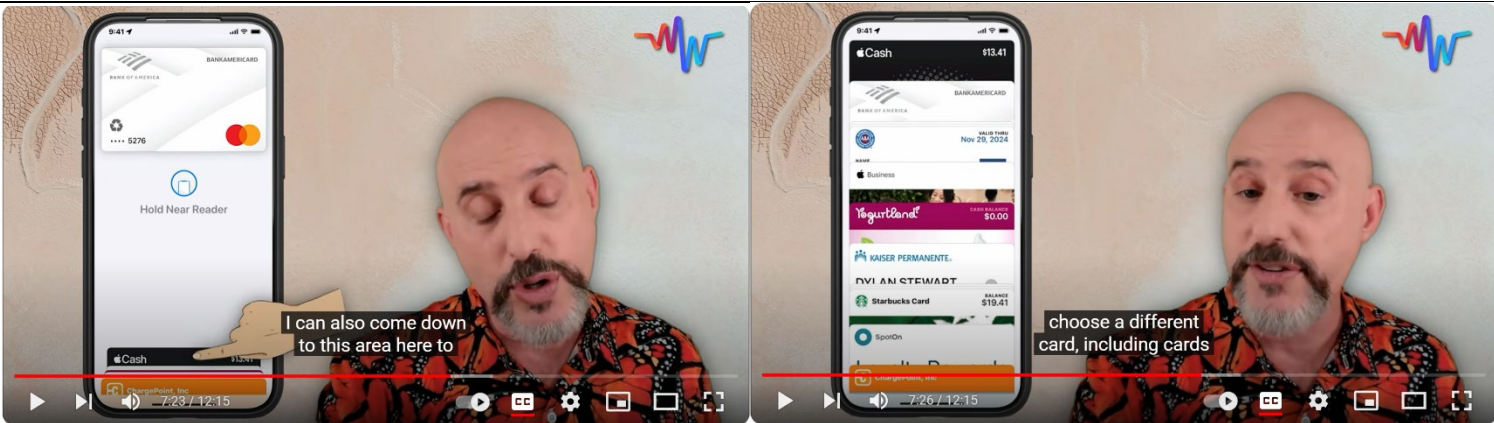
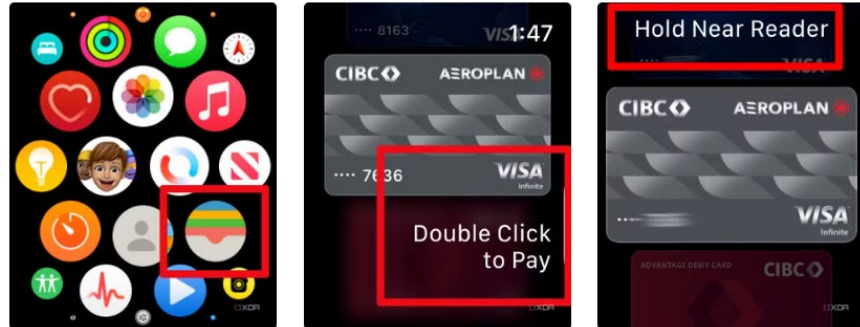
Claim No.	Accused Products
	 See, e.g., The MacWhisperer Academy, <i>How to Use Apple Pay</i>, YouTube (Aug. 3, 2024), https://www.youtube.com/watch?v=v7hJuzw8FC0. 3. Alternatively, you can manually open the Wallet app on your Apple Watch. 4. You'll see a miniature digital version of the card you loaded or flip through multiple cards by scrolling up and down on the screen. When the card you want is on the screen, double-click the side button. [...]  See, e.g., Christine Persaud, <i>How to use Apple Pay on your Apple Watch</i>, XDA Developers (Oct. 24, 2023), https://www.xda-developers.com/how-pay-on-apple-watch/.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
18[f] wherein the identification, selection, information and authorizing operations are exchanged wirelessly between the electronic device and the ATM via NFC; and,	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, exchanges identification (<i>e.g.</i>, as identified above), selection (<i>e.g.</i>, as identified above), information and authorizing operations (<i>e.g.</i>, as identified above) wirelessly between the electronic device and the ATM via NFC. <i>See supra</i> limitation 18[a]. Cardless/contactless ATMs Cardless technology is found on contactless ATMs, which allow customers to tap their phones to activate an RFID reader. The machine uses a variety of technologies to read the data, but the most common one for cardless ATMs is near-field communication. Finder.com identifies other ways ATMs can connect with customer's phones including app-generated codes, QR codes or at times biometric authentication that scans fingerprints or eyes. How to use Apple/Google Pay at an ATM In order to use Apple or Google Pay at a cardless ATM, customers simply need to open their Google or Apple Pay Wallet, make sure the right debit card is selected and then tap the phone against the contactless symbol for the ATM. From there, the customer will need to enter their PIN number as usual. Of course, this will only work on ATMs that have near-field communication readers. <i>See, e.g.</i>, Bradley Cooper, <i>Cardless ATMs deliver Google/Apple Pay</i>, atm marketplace (May 14, 2024), https://www.atmmarketplace.com/articles/cardless-atms-deliver-googleapple-pay/. Using Apple Pay at an ATM <i>With your iPhone</i> 1. If your iPhone is locked, double-click the home button to open Apple Pay. Otherwise, tap Wallet and tap your debit card. 2. Hold your iPhone near the contactless reader symbol on the ATM and keep your finger on the home button to activate Touch ID. [. . .] 3. Enter your PIN on the ATM's keypad.

Claim No.	Accused Products
	<i>With your Apple Watch</i> 1. Double-click the side button to open Apple Pay. An image for your default card will appear. If this is not your debit card, swipe to display it. 2. Hold Apple Watch near the contactless reader symbol. A gentle tap on your wrist and a beep will confirm a successful transmission. [. . .] 3. Enter your PIN on the ATM’s keypad. <i>See, e.g., Mike Matthews, How to use your iPhone and Apple Watch at an ATM, The App Factor (Dec. 7, 2016), https://theappfactor.com/using-iphone-apple-watch-atm/</i> How to use Chase ATMs without your card To start using cardless Chase ATM access, be sure you’ve added your eligible Chase debit card to your phone’s mobile wallet app.  Step 1 Access your mobile wallet on your phone and choose your virtual Chase Debit Card.  Step 2 Look for the  symbol on the ATM, and tap it with your phone.  Step 3 Enter your PIN as usual.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	How to add a card to your phone's mobile wallet Choose your mobile wallet below or open the mobile wallet app on your phone and follow the instructions.   Google Wallet SAMSUNG Pay Apple Pay[®] Google Wallet[™] Samsung Pay <i>See, e.g., Cardless ATM Access, Chase, https://www.chase.com/digital/atms/cardless-nfc (last visited Dec. 30, 2024).</i>
18[g] wherein the ATM is configured for performing the user selected account operation using the identification and authorizing information; and,	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, transacts wirelessly (e.g., via NFC interface) with an ATM, wherein the ATM is configured for performing the user selected account operation using the identification (e.g., as identified above) and authorizing (e.g., as identified above) information. <i>See supra</i> limitation 18[a]. How to use Chase ATMs without your card To start using cardless Chase ATM access, be sure you've added your eligible Chase debit card to your phone's mobile wallet app.  Step 1 Access your mobile wallet on your phone and choose your virtual Chase Debit Card.  Step 2 Look for the  symbol on the ATM, and tap it with your phone.  Step 3 Enter your PIN as usual.

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	How to add a card to your phone's mobile wallet Choose your mobile wallet below or open the mobile wallet app on your phone and follow the instructions.   Google Wallet SAMSUNG Pay Apple Pay[®] Google Wallet[™] Samsung Pay <i>See, e.g., Cardless ATM Access, Chase, https://www.chase.com/digital/atms/cardless-nfc (last visited Dec. 30, 2024).</i>
18[h] wherein the identification and authorizing information exchanged wirelessly between the electronic device and the ATM comprises: statically and dynamically generated limited-use number portions; and, wherein said static and dynamic information is combined to perform the user selected ATM operation.	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, wirelessly exchanges identification and authorizing information between the electronic device and the ATM comprising: statically (<i>e.g.</i>, DAN) and dynamically generated (<i>e.g.</i>, dynamic cryptogram or dynamic security code, or any combination including one or more of the same) limited-use number portions and wherein said static and dynamic information is combined to perform the user selected ATM operation. When you use Apple Pay in stores [. . .] After you authenticate your transaction, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code to the store's point of sale terminal along with additional information needed to complete the transaction. Again, neither Apple nor your device sends your actual payment 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 that it's unique and tied to your device. <i>See, e.g., Apple Pay security and privacy overview, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554.</i>

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	Using a payment cryptogram for dynamic security Payment transactions originating from the payment applets include a payment cryptogram along with a Device Account Number. This cryptogram, a one-time code, is computed using a transaction counter and a key. The transaction counter is incremented for each new transaction. The key is provisioned in the payment applet during personalization and is known by the payment network or the card issuer or both. Depending on the payment scheme, other data may also be used in the calculation, including: • A Terminal Unpredictable Number, for near-field-communication (NFC) transactions • An Apple Pay server anti-replay value, for transactions within apps • User verification results, such as Cardholder Verification Method (CVM) information These security codes are provided to the payment network and to the card issuer, which allows the issuer to verify each transaction. The length of these security codes may vary based on the type of transaction. <i>See, e.g., Apple Platform Security</i>, at 183 (Dec. 2024) available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; <i>see also, e.g., Apple Platform Security, Payment authorization with Apple Pay</i>, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/payment-authorization-with-apple-pay-secc1f57e189/web.
19[a] A method of claim 18, wherein the identification and authorizing information is generated from at least one of a set identification and data comprising: ATM accounts; user identification; biometric user identification; device-identifiers; email address; username; transactional information; merchant identifiers; facility location; user accounts; cryptocurrency address; cryptocurrency keys; merchant accounts; online accounts; bank accounts; device account numbers; payment numbers; card issuing authority; and payment-issuer; and	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, wirelessly exchanges identification and authorizing information generated from at least one of a set identification and data comprising: ATM accounts; user identification; biometric user identification; device-identifiers; email address; username; transactional information; merchant identifiers; facility location; user accounts; cryptocurrency address; cryptocurrency keys; merchant accounts; online accounts; bank accounts; device account numbers; payment numbers; card issuing authority; and payment-issuer. <i>See supra</i> limitation 18[a].

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
19[b] wherein further the data includes at least one of time; duration; passwords; passcodes; device position; device motion; device-specifics; secrets; keys; a currency; currency amounts; cryptocurrency amount; transaction limits; transaction records; usage duration; and usage sequence counts.	An Apple Pay- and/or Apple Wallet-enabled computing device wirelessly exchanges identification and authorizing information generated from at least one of a set identification and data, the data further including at least one of time; duration; passwords; passcodes; device position; device motion; device-specifics; secrets; keys; a currency; currency amounts; cryptocurrency amount; transaction limits; transaction records; usage duration; and usage sequence counts. <i>See supra</i> limitation 18[a].
20 A method of claim 18, wherein user entered identification and authorizing information is recorded through the user interface of the electronic device from at least one of set including: a plurality of button-press actions; a swipe gesture received at a touch sensor of the electronic device; a key press sequence received at the touch sensor; a passcode sequence received at the buttons; a plurality of swipe gestures received at a touch sensor of the electronic device; a key press PIN sequence received at the touch sensor; a passcode sequence received at the touch sensor; an accelerometer sensor indicating a user motion of the electronic device; an action and sequence of motions of the electronic device as performed by a user; an action of the user to move the electronic device into a specific orientation; a biometric sensor confirming the electronic device is in a grip of the user; and a biometric sensor confirming the electronic device has remained in the possession of the user from activation to transaction.	An Apple Pay- and/or Apple Wallet-enabled computing device receives user entered identification and authorizing information is recorded through the user interface of the electronic device from at least one of the set including: a plurality of button-press actions; a swipe gesture received at a touch sensor of the electronic device; a key press sequence received at the touch sensor; a passcode sequence received at the buttons; a plurality of swipe gestures received at a touch sensor of the electronic device; a key press PIN sequence received at the touch sensor; a passcode sequence received at the touch sensor; an accelerometer sensor indicating a user motion of the electronic device; an action and sequence of motions of the electronic device as performed by a user; an action of the user to move the electronic device into a specific orientation; a biometric sensor confirming the electronic device is in a grip of the user; and a biometric sensor confirming the electronic device has remained in the possession of the user from activation to transaction. <i>See supra</i> limitation 18[a].

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

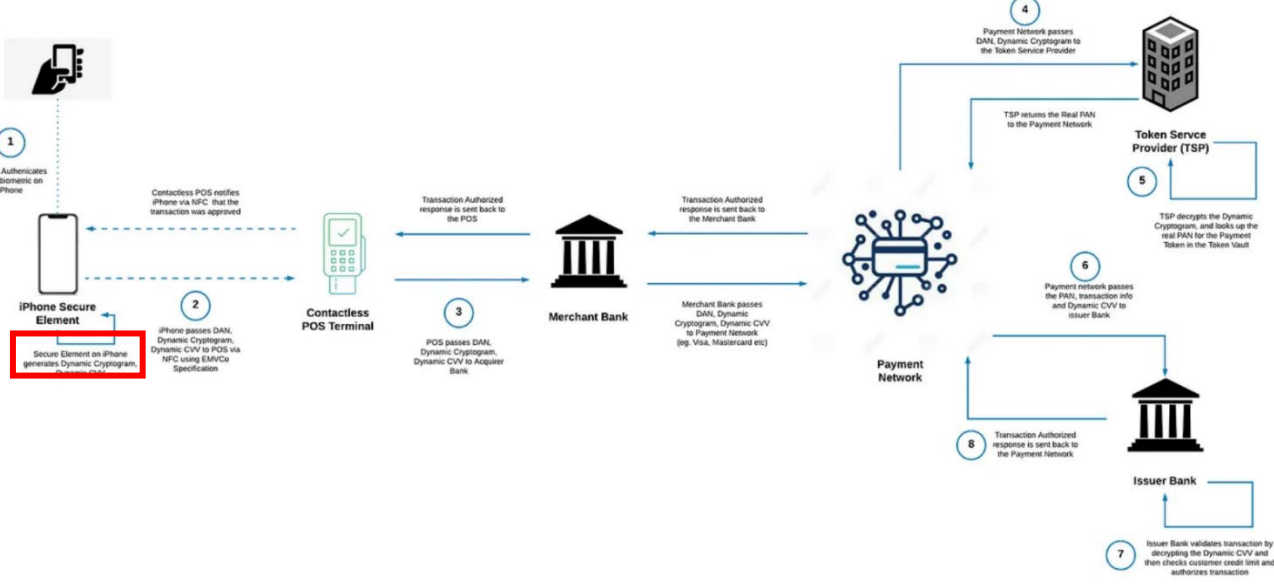
Claim No.	Accused Products
into a specific orientation; a biometric sensor confirming the electronic device is in a grip of the user; and a biometric sensor confirming the electronic device has remained in the possession of the user from activation to transaction.	
22. The method of claim 18, wherein the limited-use number dynamically generated in the device is based on cryptographically combining data selected from the group consisting of an ATM information, the locality of an ATM reader facility, information regarding the facility performing the transaction, bank information, a time of day, a date, a transaction amount, a count of past transactions, a sequence count, a historical record of transactions, a merchant account, a user's location, an online address, a device-internal secret, a device unique identifier, a payment authority key, a payment issuer authority secret, a method and direction of payment, deposit, transfer and receipt, a cryptocurrency server, a cryptocurrency type, a cryptocurrency private key, a cryptocurrency public key, a cryptocurrency address, a touch gesture, a biometrically sensed user	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, dynamically generates the limited-use number (<i>e.g.</i>, dynamic cryptogram or dynamic CVV) based on cryptographically combining data selected from the group consisting of an ATM information, the locality of an ATM reader facility (<i>e.g.</i>, device location), information regarding the facility performing the transaction (<i>e.g.</i>, Terminal Unpredictable Number), bank information, a time of day, a date, a transaction amount, a count of past transactions, a sequence count (<i>e.g.</i>, transaction counter), a historical record of transactions, a merchant account, a user's location (<i>e.g.</i>, device location), an online address, a device-internal secret (<i>e.g.</i>, DAN), a device unique identifier, a payment authority key (<i>e.g.</i>, payment token key, CVV-key), a payment issuer authority secret (<i>e.g.</i>, payment token key, CVV-key), a method and direction of payment, deposit, transfer and receipt, a cryptocurrency server, a cryptocurrency type, a cryptocurrency private key, a cryptocurrency public key, a cryptocurrency address, a touch gesture, a biometrically sensed user information, a user's private information, a user key, a user email, password, passcode, a PIN, a user secret, and a user input. <i>See supra</i> limitation 18[h]. When you use Apple Pay in stores [. . .] After you authenticate your transaction, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code to the store's point of sale terminal along with additional information needed to complete the transaction. Again, neither Apple nor your device sends your actual payment 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 that it's unique and tied to your device. <i>See, e.g., Apple Pay security and privacy overview</i>, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554. <i>Note:</i> If you have Location Services turned on, the location of your iPhone at the time you make a payment may be sent to Apple and the card issuer to help prevent fraud. See Control the location information you share. <i>See, e.g., iPhone User Guide – iOS 18, Use Apple Pay for contactless payments on iPhone</i>, Apple, https://support.apple.com/guide/iphone/use-apple-pay-for-contactless-payments-iphbd4cf42b4/ios (last visited Dec. 30, 2024).

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products				
sensed user information, a user's private information, a user key, a user email, password, passcode, a PIN, a user secret, and a user input.	Using a payment cryptogram for dynamic security Payment transactions originating from the payment applets include a payment cryptogram along with a Device Account Number. This cryptogram, a one-time code, is computed using a transaction counter and a key. The transaction counter is incremented for each new transaction. The key is provisioned in the payment applet during personalization and is known by the payment network or the card issuer or both. Depending on the payment scheme, other data may also be used in the calculation, including: • A Terminal Unpredictable Number, for near-field-communication (NFC) transactions • An Apple Pay server anti-replay value, for transactions within apps • User verification results, such as Cardholder Verification Method (CVM) information These security codes are provided to the payment network and to the card issuer, which allows the issuer to verify each transaction. The length of these security codes may vary based on the type of transaction. See, e.g., <i>Apple Platform Security</i>, at 183 (Dec. 2024) available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; see also, e.g., <i>Apple Platform Security, Payment authorization with Apple Pay</i>, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/payment-authorization-with-apple-pay-secc1f57e189/web. 5. End-to-End EMV Payment Tokenization Flows This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3): • In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 12, 23 (June 2019) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf. <table border="1"> <thead> <tr> <th>Term</th><th>Definition</th></tr> </thead> <tbody> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token. Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </tbody> </table> See, e.g., EMVCo, <i>EMV® Payment Tokenisation Specification – Technical Framework v2.1</i> at 10 (Jun. 14, 2019).	Term	Definition	Token Cryptogram	A cryptogram, containing a transaction-unique value, typically generated using the Payment Token. Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.
Term	Definition				
Token Cryptogram	A cryptogram, containing a transaction-unique value, typically generated using the Payment Token. Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.				

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	When a Payment Card is added to Apple Pay When you add a new payment card (<i>i.e. a credit or a debit card</i>) to Apple Pay, here are the steps that happen behind the scenes. [. . .] 7. Apple Pay, uses its own Trusted Service Manager (TSM) and provisions the <i>Payment Token, Payment Token-Key</i> and <i>CVV-Key</i> and maybe other data onto the “Secure Element” <i>i.e. the secure hardware chip on the physical iPhone device.</i> This then is the “Payment Token” that Apple saves on its Secure Element (SE) and calls the <i>DAN (Device Account Number)</i>. When you Pay using Apple Pay with your iPhone Apple Pay uses <i>NFC</i> to send payment data to the contactless POS terminal when you Tap & Pay . Apple Pay uses the <i>EMVCo’s contactless suite of specifications</i> to pass the data from your iPhone to the contactless reader terminal. [. . .] 2. Once you authenticate yourself to the iPhone the Secure Element on the iPhone takes the following steps, (a) <i>generates a Dynamic Cryptogram,</i> - which is a combination of the <i>Payment Token, transaction amount, transaction counter etc.</i> along with the <i>Payment-Token-Key</i> (<i>i.e. the public key provided by the TSP</i>). (b) <i>generates a Dynamic CVV,</i> - using the <i>CVV-key</i> (<i>i.e. the public key provided by the Issuing Bank</i>).

Claim No.	Accused Products
	 The diagram illustrates the Apple Pay transaction process in eight steps: - Person authenticates using biometric on iPhone. - Secure Element on iPhone generates Dynamic Cryptogram, DAN, and Dynamic CVV. - iPhone passes DAN, Dynamic Cryptogram, Dynamic CVV to POS via NFC using EMVCo Specification. - Contactless POS notifies iPhone via NFC that the transaction was approved. - Transaction Authorized response is sent back to the POS. - POS passes DAN, Dynamic Cryptogram, Dynamic CVV to Acquirer Bank. - Merchant Bank passes DAN, Dynamic Cryptogram, Dynamic CVV to Payment Network (e.g., Visa, Mastercard etc). - Transaction Authorized response is sent back to the Merchant Bank. - Payment Network passes DAN, Dynamic Cryptogram to the Token Service Provider. - TSP returns the Real PAN to the Payment Network. - TSP decrypts the Dynamic Cryptogram, and looks up the real PAN for the Payment Token in the Token Vault. - Payment network passes the PAN, transaction info and Dynamic CVV to Issuer Bank. - Transaction Authorized response is sent back to the Payment Network. - Issuer Bank validates transaction by decrypting the Dynamic CVV and then checks customer credit limit and authorizes transaction. When you Pay using Apple Pay with your iPhone See, e.g., Prashant Ram, <i>How Apple Pay works under the hood?</i>, codeburst (Nov. 5, 2019), https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7.
23. The method of claim of 18, wherein the payment information comprises combining a plurality of static portions, and a plurality of dynamically generated limited-use portions, and wherein the static portion is a token account number with a limited-duration expiration date, to be used in place of issuer provided information.	An Apple Pay- and/or Apple Wallet-enabled computing device, such as a smartphone or smartwatch, on information and belief, exchanges payment information comprising combining a plurality of static portions (e.g., DAN and associated expiration date), and a plurality of dynamically generated limited-use portions (e.g., dynamic cryptogram, dynamic security code), and wherein the static portion is a token account number with a limited-duration expiration date, to be used in place of issuer provided information (e.g., PAN or associated expiration date or CVV). See <i>supra</i> limitation 1[n]. When you use Apple Pay in stores [.] After you authenticate your transaction, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code to the store’s point of sale terminal along with additional information needed to complete the transaction. Again, neither Apple nor your device sends your actual payment 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 that it’s unique and tied to your device.

Claim No.	Accused Products
	When you use Apple Pay within apps or on the web When you use an app or a website that uses Apple Pay in iOS, watchOS, or macOS, the app or website can check if you have Apple Pay enabled on that device. You can manage this option in Settings > Safari on your iOS device, and in the Privacy tab in Safari preferences on your Mac. To securely transmit your payment information when you pay in apps or on the web, Apple Pay receives your encrypted transaction and re-encrypts it with a developer-specific key before the transaction information is sent to the developer or payment processor. This key helps ensure that only the app or the website that you’re purchasing from can access your encrypted payment information. Websites must verify their domain every time they offer Apple Pay as a payment option. Like with in-store payments, Apple sends your Device Account Number to the app or website along with the transaction-specific dynamic security code. Neither Apple nor your device sends your actual payment card number to the app. See, e.g., <i>Apple Pay security and privacy overview</i>, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554. Using a payment cryptogram for dynamic security Payment transactions originating from the payment applets include a payment cryptogram along with a Device Account Number. This cryptogram, a one-time code, is computed using a transaction counter and a key. The transaction counter is incremented for each new transaction. The key is provisioned in the payment applet during personalization and is known by the payment network or the card issuer or both. Depending on the payment scheme, other data may also be used in the calculation, including: • A Terminal Unpredictable Number, for near-field-communication (NFC) transactions • An Apple Pay server anti-replay value, for transactions within apps • User verification results, such as Cardholder Verification Method (CVM) information These security codes are provided to the payment network and to the card issuer, which allows the issuer to verify each transaction. The length of these security codes may vary based on the type of transaction. See, e.g., <i>Apple Platform Security</i>, at 183 (Dec. 2024) available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; see also, e.g., <i>Apple Platform Security, Payment authorization with Apple Pay</i>, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/payment-authorization-with-apple-pay-secc1f57e189/web. When a Payment Card is added to Apple Pay When you add a new payment card (i.e. a credit or a debit card) to Apple Pay, here are the steps that happen behind the scenes. [...]

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	7. Apple Pay, uses its own Trusted Service Manager (TSM) and provisions the <i>Payment Token</i>, <i>Payment Token-Key</i> and <i>CVV-Key</i> and maybe other data onto the “Secure Element” i.e. the secure hardware chip on the physical iPhone device. This then is the “Payment Token” that Apple saves on its Secure Element (SE) and calls the <i>DAN (Device Account Number)</i>. When you Pay using Apple Pay with your iPhone Apple Pay uses <i>NFC</i> to send payment data to the contactless POS terminal when you Tap & Pay . Apple Pay uses the <i>EMVCo’s contactless suite of specifications</i> to pass the data from your iPhone to the contactless reader terminal. 2. Once you authenticate yourself to the iPhone the Secure Element on the iPhone takes the following steps, (a) <i>generates a Dynamic Cryptogram</i>, - which is a combination of the <i>Payment Token</i>, <i>transaction amount</i>, <i>transaction counter etc.</i> along with the <i>Payment-Token-Key</i> (i.e. the public key provided by the TSP). (b) <i>generates a Dynamic CVV</i>, - using the <i>CVV-key</i> (i.e. the public key provided by the Issuing Bank).

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 ("520 Patent")

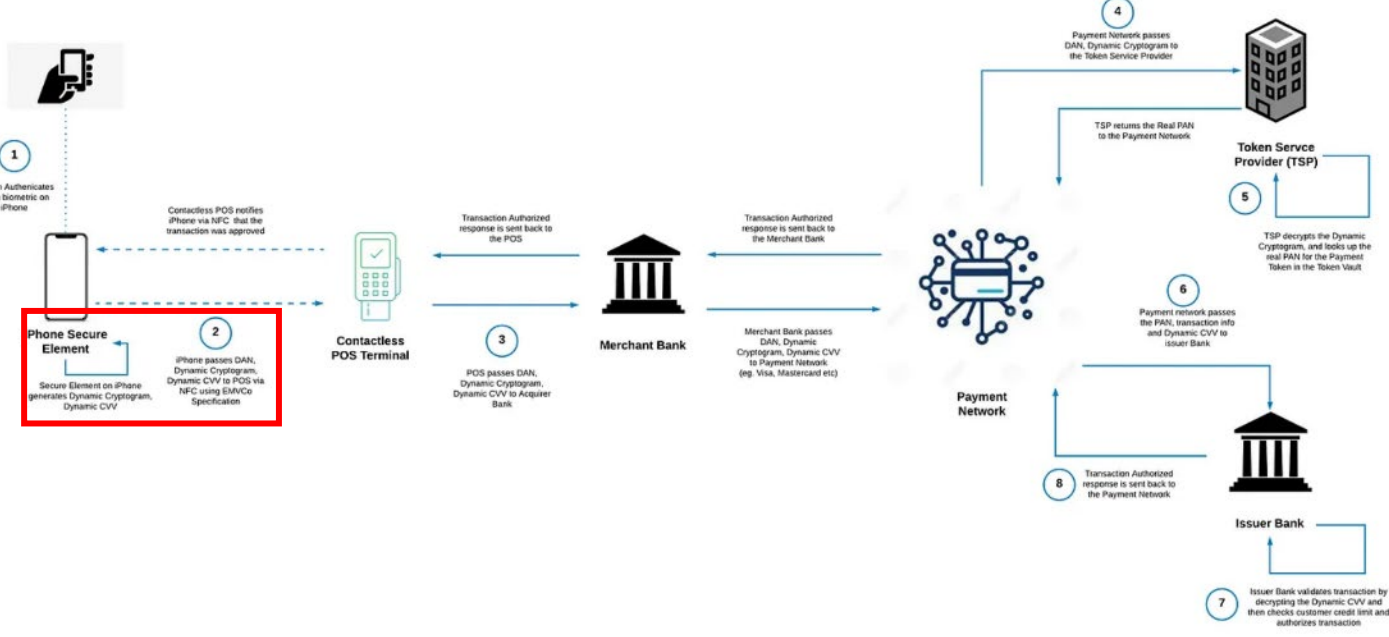
Claim No.	Accused Products
	 The diagram illustrates the Apple Pay transaction flow with the following steps: 1 Person Authenticates using biometric on iPhone. 2 iPhone passes DAN, Dynamic Cryptogram, Dynamic CVV to POS via NFC using EMVCo Specification. (This step is highlighted with a red box in the original image.) 3 POS passes DAN, Dynamic Cryptogram, Dynamic CVV to Acquirer Bank. 4 Payment network passes DAN, Dynamic Cryptogram to the Token Service Provider. 5 TSP returns the Real PAN to the Payment Network. TSP decrypts the Dynamic Cryptogram and looks up the real PAN for the Payment Token in the Token Vault. 6 Payment network passes the PAN, transaction info and Dynamic CVV to issuer Bank. 7 Issuer Bank validates transaction by decrypting the Dynamic CVV and then checks customer credit limit and authorizes transaction. 8 Transaction Authorized response is sent back to the Payment Network. Other components and flows shown include: Contactless POS Terminal, Merchant Bank, Payment Network, and Token Service Provider (TSP). When you Pay using Apple Pay with your iPhone See, e.g., Prashant Ram, <i>How Apple Pay works under the hood?</i>, codeburst (Nov. 5, 2019), https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7. 5. End-to-End EMV Payment Tokenization Flows This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3): - In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 19-21 (June 2019) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf ("Tokens, like PANs, have an expiration date.").

EXHIBIT A: Infringement Claim Chart for U.S. Patent No. 10,339,520 (“520 Patent”)

Claim No.	Accused Products
	5.1.3.2 Token Generation Token Generation is the process of creating a Payment Token and its associated Token Expiry Date and mapping it to a specific underlying PAN, for use by a specific Token Requestor and Token Domain(s), as identified the Token Requestor ID. The Token Service Provider SHALL facilitate the generation of a Payment Token and related data. This may be in response to a Token Request from a registered Token Requestor with a valid Token Requestor ID or an existing Payment Token may be mapped to an underlying PAN in response to a Token Request from a registered Token Requestor with a valid Token Requestor ID. See, e.g., EMVCo, <i>EMV® Payment Tokenisation Specification – Technical Framework v2.1</i> at 35–36 (Jun. 14, 2019). In general terms, the process for registering a card in a mobile wallet is as follows: [. . .] 5. If everything is correct, the TSP registers the PAN and links it to a new token in a secure database (<i>Token Vault</i>). Along with the TR Identifier, the token expiration date, and a number of additional security features called <i>Token Domain</i>, including restrictions on the use of the new token on certain channels, use by a particular merchant, limitation on the number of permitted uses, and verification of the cryptogram. 6. The TSP notifies the application of the newly generated token. 7. The application stores the generated token (<i>Device Account Number</i> (DAN) for Apple Pay or Digitized PAN (DPAN) for Samsung Pay) in a secure location (Secure Element (SE) or Host Card Emulation (HCE)). See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details (captured May 9, 2024).

APPENDIX – Accused Products

The Accused Products refers to all products manufactured, used, tested, imported, or sold by or on behalf of Defendant that embody the devices claimed by the ’520 Patent and all processes employed by Defendant that practice the methods claimed by the ’520 Patent, consisting of at least Defendant’s products that support Apple Pay (alone or with Apple Wallet), including the following Apple-branded smartphones, smartwatches, and tablets.¹

I. Accused Smartphones

The accused smartphones include Apple iPhone models with Face ID and iPhone models with TouchID, except iPhone 5s.²

Product	Model No.	Product	Model No.
iPhone 16 Pro Max	A3084	iPhone 12 mini	A2176
iPhone 16 Pro	A3083	iPhone 12	A2172
iPhone 16 Plus	A3082	iPhone SE (2nd generation)	A2275
iPhone 16	A3081	iPhone 11 Pro Max	A2161
iPhone 15 Pro Max	A2849	iPhone 11 Pro	A2160
iPhone 15 Pro	A2848	iPhone 11	A2111
iPhone 15 Plus	A2847	iPhone XR	A1984, A2105, A2107
iPhone 15	A2846	iPhone XS Max	A1921, A2101, A2103
iPhone 14 Pro Max	A2651	iPhone XS	A1920, A2097, A2099
iPhone 14 Pro	A2650	iPhone X*	A1865, A1901
iPhone 14 Plus	A2632	iPhone 8 Plus	A1864, A1897
iPhone 14	A2649	iPhone 8	A1863, A1905
iPhone SE (3rd generation)	A2595	iPhone 7 Plus	A1661, A1784
iPhone 13 Pro Max	A2484	iPhone 7	A1660, A1778
iPhone 13 Pro	A2483	iPhone SE (1st generation)*	A1723, A1662, A1724
iPhone 13 mini	A2481	iPhone 6s Plus*	A1634, A1687, A1699
iPhone 13	A2482	iPhone 6s*	A1633, A1688, A1700
iPhone 12 Pro Max	A2342	iPhone 6 Plus*	A1522, A1524, A1593
iPhone 12 Pro	A2341	iPhone 6*	A1549, A1586, A1589

*Accused to the extent that Apple has induced or contributed to third parties’ use of such devices to practice the accused methods during on or after November 4, 2018 (“the Relevant Time Period”).

¹ See, e.g., *Devices compatible with Apple Pay*, Apple (Nov. 22, 2024), <https://support.apple.com/en-us/102896>.

² See, e.g., *Identify your iPhone Model*, Apple (Sept. 19, 2024), <https://support.apple.com/en-us/108044>; *iPhone and iPad models that support Face ID*, Apple (Dec. 18, 2023), <https://support.apple.com/en-us/102854>; Benj Edwards, *Which iPhones Have Touch ID?*, How-To Geek (May 13, 2022), <https://www.howtogeek.com/802122/which-iphones-have-touch-id/>.

II. Accused Smartwatches

The accused smartwatches include Apple Watch Series 1 and later.³

Product	Model No.	Product	Model No.
Apple Watch Series 10 (GPS)	A2997, A2999	Apple Watch SE (GPS + Cellular) Aluminum	A2353, A2354
Apple Watch Series 10 (GPS + Cellular) Aluminum	A3001, A3003	Apple Watch Nike (GPS + Cellular)	A2353, A2354
Apple Watch Series 10 (GPS + Cellular) Titanium	A3001, A3003	Apple Watch Series 5 (GPS)	A2092, A2093
Apple Watch Hermès Series 10 (GPS + Cellular)	A3001, A3003	Apple Watch Nike (GPS)	A2092, A2093
Apple Watch Ultra 2 (GPS + Cellular)	A2986, A2987	Apple Watch Series 5 (GPS + Cellular) Aluminum	A2094, A2095
Apple Watch Hermès Ultra 2 (GPS + Cellular)	A2986, A2987	Apple Watch Nike (GPS + Cellular)	A2094, A2095
Apple Watch Series 9 (GPS)	A2978, A2980	Apple Watch Series 5 (GPS + Cellular) Stainless Steel	A2094, A2095
Apple Watch Series 9 (GPS + Cellular) Aluminum	A2982, A2984	Apple Watch Hermès (GPS + Cellular)	A2094, A2095
Apple Watch Series 9 (GPS + Cellular) Stainless Steel	A2982, A2984	Apple Watch Edition (GPS + Cellular) Titanium	A2094, A2095
Apple Watch Series 9 Hermès (GPS + Cellular)	A2982, A2984	Apple Watch Edition (GPS + Cellular) Ceramic	A2094, A2095
Apple Watch Ultra (GPS + Cellular)	A2622	Apple Watch Series 4 (GPS)	A1977, A1978
Apple Watch Series 8 (GPS)	A2770, A2771	Apple Watch Nike+ (GPS)	A1977, A1978
Apple Watch Series 8 (GPS + Cellular) Aluminum	A2772, A2774	Apple Watch Series 4 (GPS + Cellular) Aluminum	A1975, A1976
Apple Watch Series 8 (GPS + Cellular) Stainless Steel	A2772, A2774	Apple Watch Nike+ (GPS + Cellular)	A1975, A1976
Apple Watch Series 8 Hermès (GPS + Cellular)	A2772, A2774	Apple Watch Series 4 (GPS + Cellular) Stainless Steel	A1975, A1976
Apple Watch SE (2nd generation) (GPS)	A2722, A2723	Apple Watch Hermès (GPS + Cellular)	A1975, A1976
Apple Watch SE (2nd generation) (GPS + Cellular)	A2726, A2727	Apple Watch Series 3 (GPS)	A1858, A1859
Apple Watch Series 7 (GPS)	A2473, A2474	Apple Watch Nike+ (GPS)	A1858, A1859
Apple Watch Nike (GPS)	A2473, A2474	Apple Watch Series 3 (GPS + Cellular) Aluminum	A1860, A1861
Apple Watch Series 7 (GPS + Cellular) Aluminum	A2475, A2477	Apple Watch Nike+ (GPS + Cellular)	A1860, A1861
Apple Watch Nike (GPS + Cellular)	A2475, A2477	Apple Watch Series 3 (GPS + Cellular) Stainless Steel	A1860, A1861
Apple Watch Series 7 (GPS + Cellular) Stainless Steel	A2475, A2477	Apple Watch Hermès (GPS + Cellular)	A1860, A1861

³ See, e.g., *Identify your Apple Watch*, Apple (Oct. 3, 2024), <https://support.apple.com/en-us/108056>.

Product	Model No.	Product	Model No.
Apple Watch Hermès (GPS + Cellular)	A2475, A2477	Apple Watch Edition (GPS + Cellular)	A1860, A1861
Apple Watch Edition (GPS + Cellular) Titanium	A2475, A2477	Apple Watch Series 2 Aluminum*	A1757, A1758
Apple Watch Series 6 (GPS)	A2291, A2292	Apple Watch Nike+*	A1757, A1758
Apple Watch Nike (GPS)	A2291, A2292	Apple Watch Series 2 Stainless Steel*	A1757, A1758
Apple Watch Series 6 (GPS + Cellular) Aluminum	A2293, A2294	Apple Watch Hermès*	A1757, A1758
Apple Watch Nike (GPS + Cellular)	A2293, A2294	Apple Watch Edition*	A1816, A1817
Apple Watch Series 6 (GPS + Cellular) Stainless Steel	A2293, A2294	Apple Watch Series 1 Aluminum*	A1802, A1803
Apple Watch Hermès (GPS + Cellular)	A2293, A2294	Apple Watch (1st generation)*	A1553, A1554
Apple Watch Edition (GPS + Cellular) Titanium	A2293, A2294	Apple Watch Sport*	A1553, A1554
Apple Watch SE (GPS)	A2351, A2352	Apple Watch Hermès*	A1553, A1554
Apple Watch Nike (GPS)	A2351, A2352	Apple Watch Edition*	A1553, A1554

*Accused to the extent that Apple has induced or contributed to third parties’ use of such devices to practice the accused methods during the Relevant Time Period.

III. Accused Tablets

The accused tablets include iPad Pro, iPad Air, iPad, and iPad mini models with Touch ID or Face ID.⁴

Product	Model No.	Product	Model No.
iPad Pro 13-inch (M4)	A2925, A2926	iPad Air (5th generation)	A2588, A2589, A2591
iPad Pro 11-inch (M4)	A2836, A2837	iPad Air (4th generation)	A2316, A2324, A2325, A2072
iPad Pro 12.9-inch (6th generation)	A2436, A2437, A2764	iPad Air (3rd generation)	A2152, A2123, A2153
iPad Pro 11-inch (4th generation)	A2759, A2761, A2435	iPad Air 2*	A1566, A1567
iPad Pro 12.9-inch (5th generation)	A2378, A2461, A2379	iPad Air*	A1474, A1475, A1476
iPad Pro 11-inch (3rd generation)	A2377, A2459, A2301	iPad mini (A17 Pro)	A2993, A2995
iPad Pro 12.9-inch (4th generation)	A2229, A2069, A2232	iPad mini (6th generation)	A2567, A2568
iPad Pro 11-inch (2nd generation)	A2228, A2068	iPad mini (5th generation)	A2133, A2124, A2126

⁴ See, e.g., *Identify your iPad Model*, Apple (Oct. 23, 2024), <https://support.apple.com/en-us/108043>; *iPhone and iPad models that support Face ID*, Apple (Dec. 18, 2023), <https://support.apple.com/en-us/102854>.

Product	Model No.	Product	Model No.
iPad Pro 12.9-inch (3rd generation)	A1876, A2014, A1895	iPad mini 4	A1538, A1550
iPad Pro 11-inch (1st generation)	A1980, A2013, A1934	iPad mini 3*	A1599, A1600
iPad Pro 12.9-inch (2nd generation)	A1670, A1671	iPad (10th generation)	A2696, A2757
iPad Pro (10.5-inch)	A1701, A1709	iPad (9th generation)	A2602, A2604, A2603
iPad Pro (9.7-inch)*	A1673, A1674, A1675	iPad (8th generation)	A2270, A2428, A2429, A2430
iPad Pro (12.9-inch) (1st generation)*	A1584, A1652	iPad (7th generation)	A2197, A2200, A2198
iPad Air 13-inch (M2)	A2898, A2899	iPad (6th generation)	A1893, A1954
iPad Air 11-inch (M2)	A2902, A2903	iPad (5th generation)*	A1822, A1823

*Accused to the extent that Apple has induced or contributed to third parties’ use of such devices to practice the accused methods during the Relevant Time Period.