Exhibit B to CardWare's Preliminary Infringement Contentions
Infringement of U.S. Patent No. 10,628,820

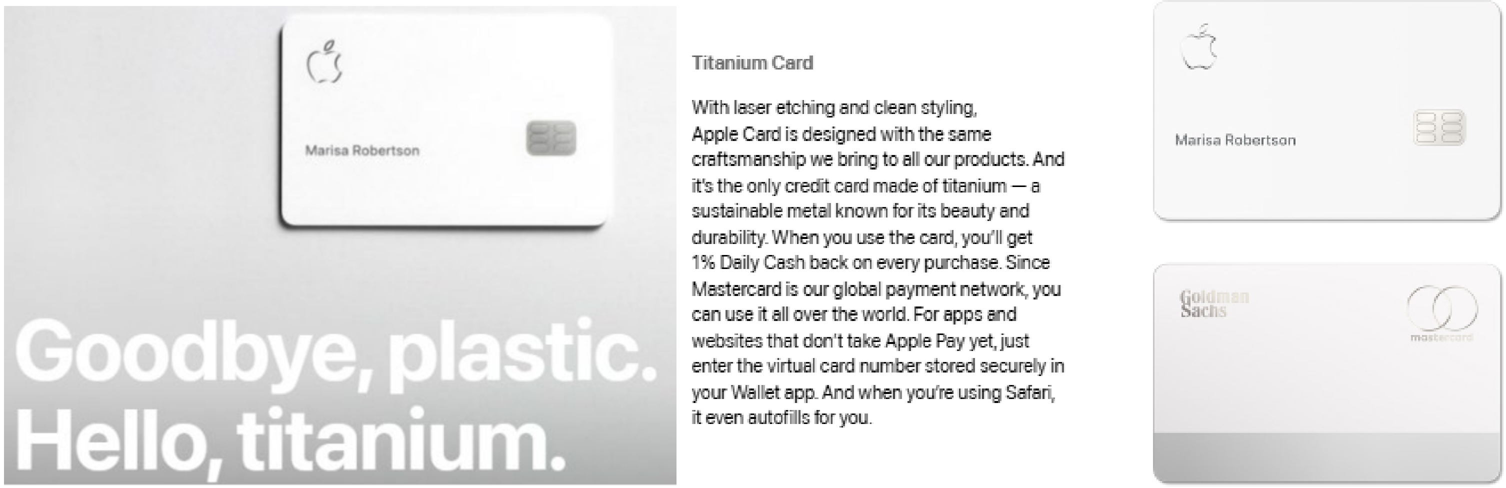
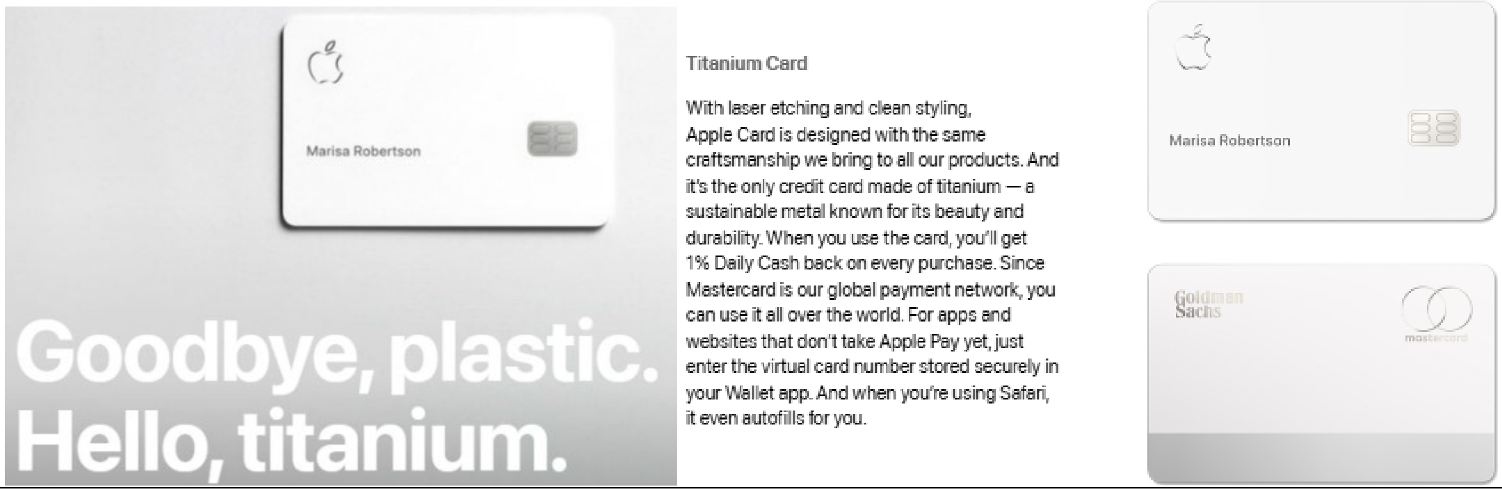
This claim chart is based on publicly available literature. Plaintiff CardWare Inc. ("CardWare") reserves the right to supplement and/or amend its positions based on discovery from Apple Inc. ("Apple" or "Defendant"), including technical documentation such as schematics and datasheets, and source code.

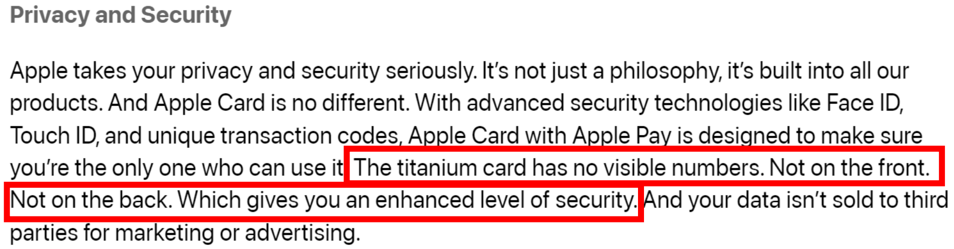
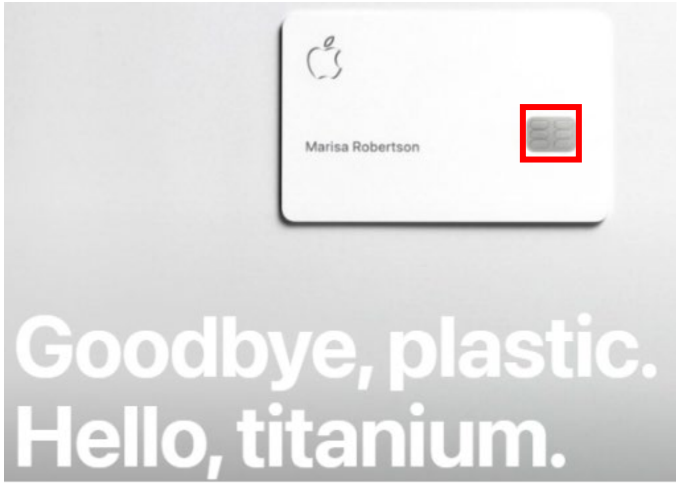
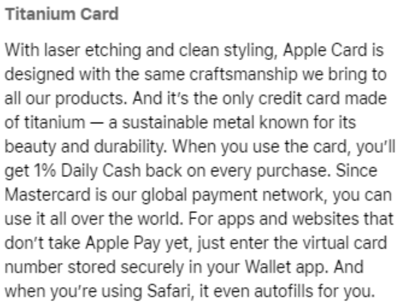
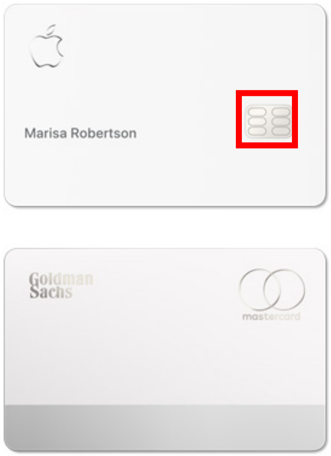
Apple infringed and continues to infringe U.S. Patent No. 10,628,820 (the "'820 patent") by making, using, selling or offering for sale, and/or importing into the United States devices and/or payment systems covered by one or more claims of the '820 patent. CardWare's allegations include all such devices, unless otherwise noted or prohibited by license ("Accused Products"). *See infra* Appendix. Apple has also infringed by contributing to and/or inducing infringement by others, for the reasons set forth herein.

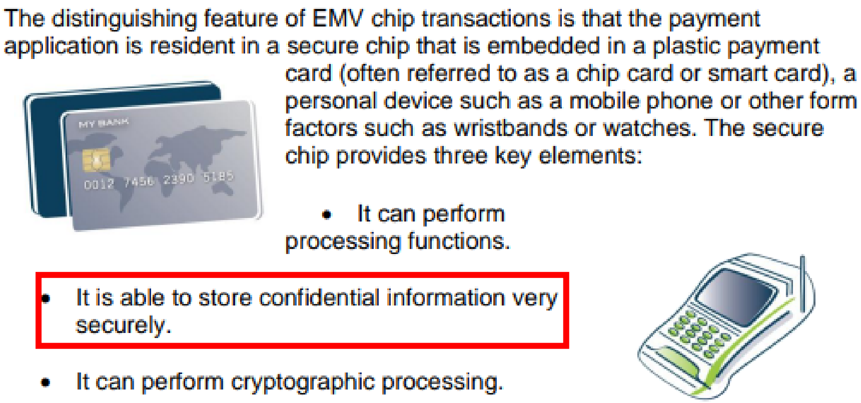
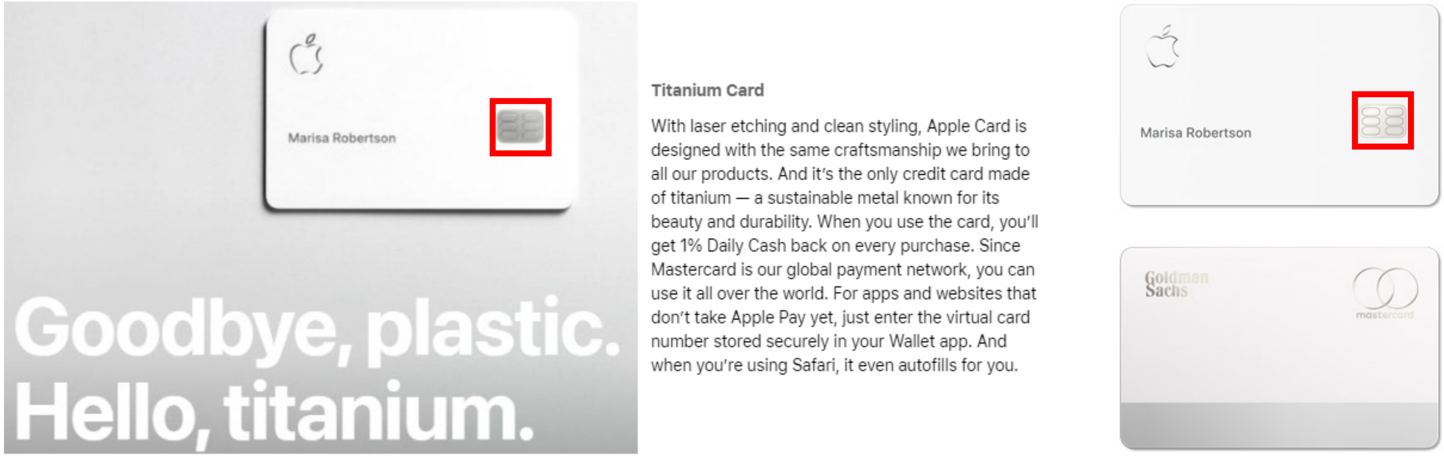
To the extent certain acts or steps constituting part of the infringement are performed by another entity besides Apple (*e.g.*, a third party payment processor or token service provider), those acts may be attributed to Apple because Apple and the other entity, or entities, are acting in a joint enterprise 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.

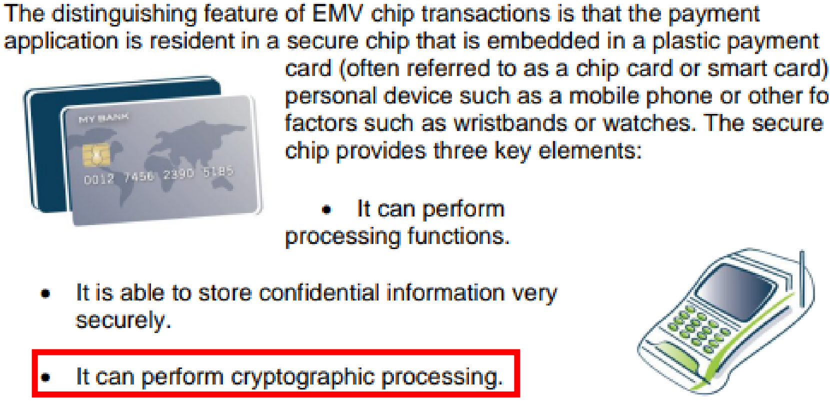
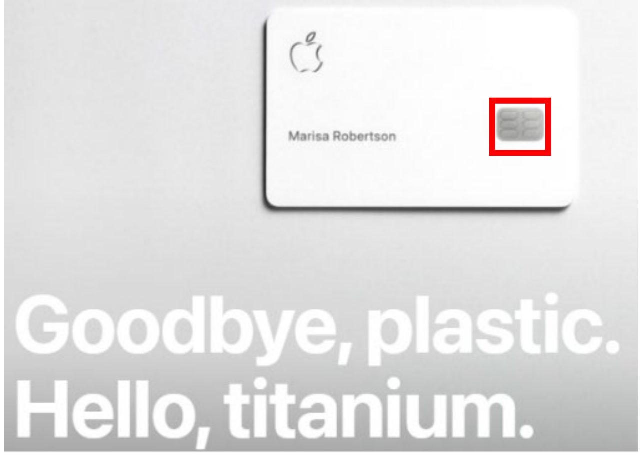
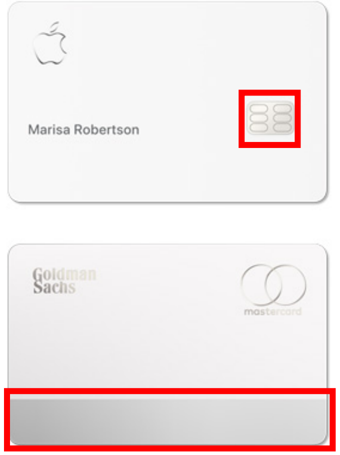
Theories exemplifying how the Accused Products infringed and continue to infringe the asserted claims of the '820 patent are detailed herein. The products included are representative; on information and belief, all Accused Products function in substantially the same manner as one or more of the examples 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.

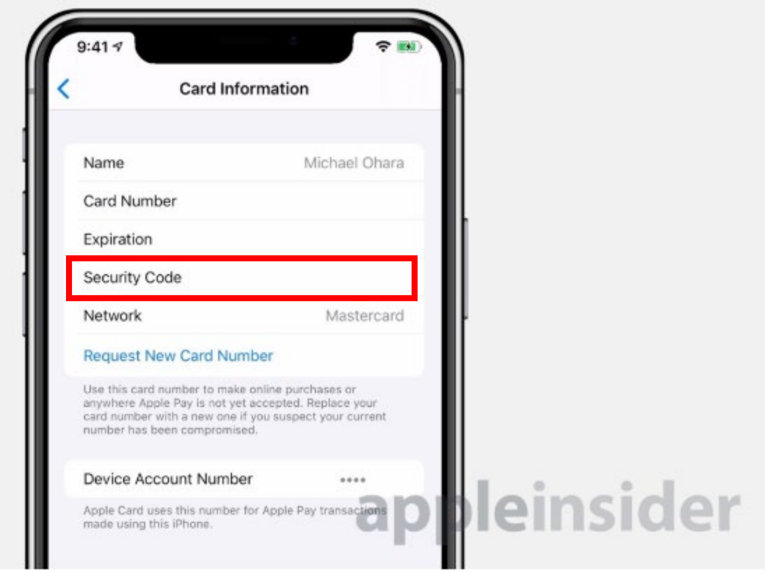
I. Claim 1 and Dependent Claims 2, 4, and 10

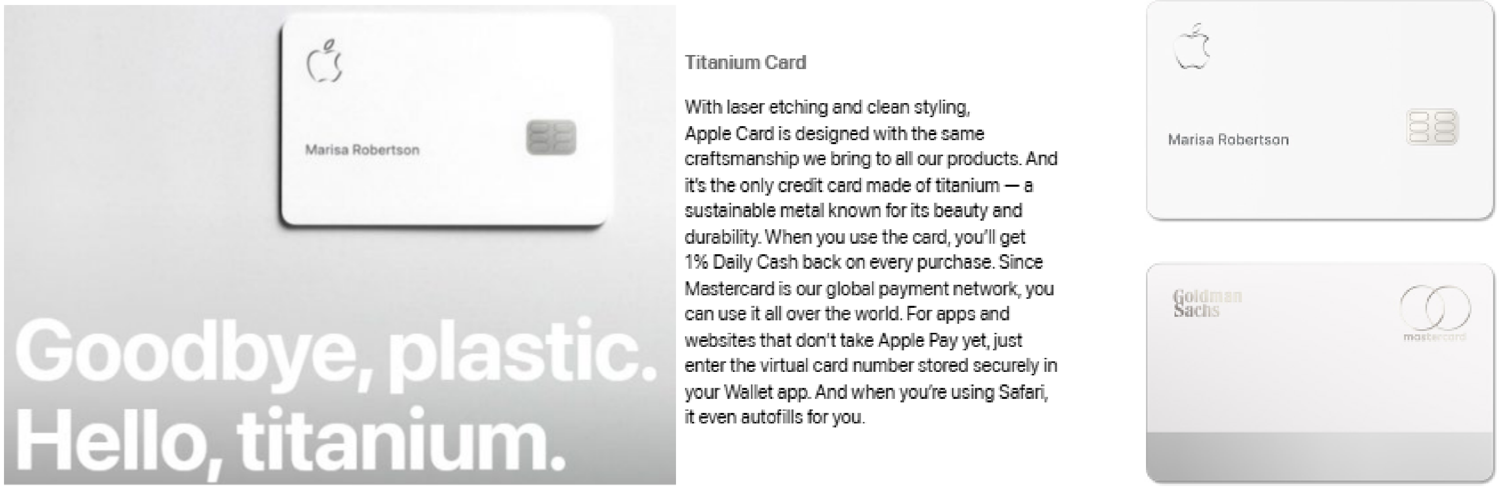
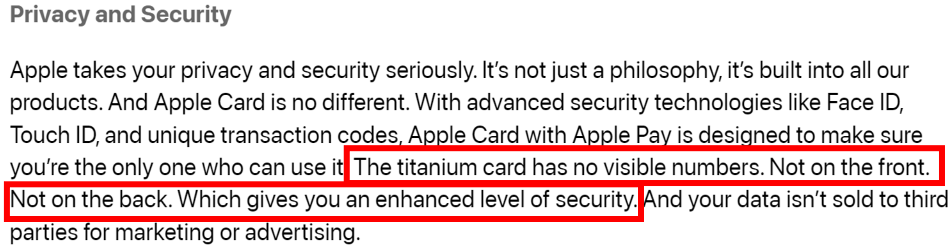
Claim Language	Accused Products
1[pre] A payment device comprising:	To the extent the preamble is limiting, an Apple Card is a payment device.  Goodbye, plastic. Hello, titanium. Marisa Robertson Goldman Sachs mastercard Titanium Card With laser etching and clean styling, Apple Card is designed with the same craftsmanship we bring to all our products. And it's the only credit card made of titanium — a sustainable metal known for its beauty and durability. When you use the card, you'll get 1% Daily Cash back on every purchase. Since Mastercard is our global payment network, you can use it all over the world. For apps and websites that don't take Apple Pay yet, just enter the virtual card number stored securely in your Wallet app. And when you're using Safari, it even autofills for you. *See, e.g.*, *Apple Card*, Apple, https://www.apple.com/apple-card/ (last visited Dec. 30, 2024); *How to request or replace a titanium Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102517.
1[a] a thin shaped body having no fixed payment numbers disposed thereon;	An Apple Card is a thin shaped body having no fixed payment devices disposed thereon.  Goodbye, plastic. Hello, titanium. Marisa Robertson Goldman Sachs mastercard Titanium Card With laser etching and clean styling, Apple Card is designed with the same craftsmanship we bring to all our products. And it's the only credit card made of titanium — a sustainable metal known for its beauty and durability. When you use the card, you'll get 1% Daily Cash back on every purchase. Since Mastercard is our global payment network, you can use it all over the world. For apps and websites that don't take Apple Pay yet, just enter the virtual card number stored securely in your Wallet app. And when you're using Safari, it even autofills for you.

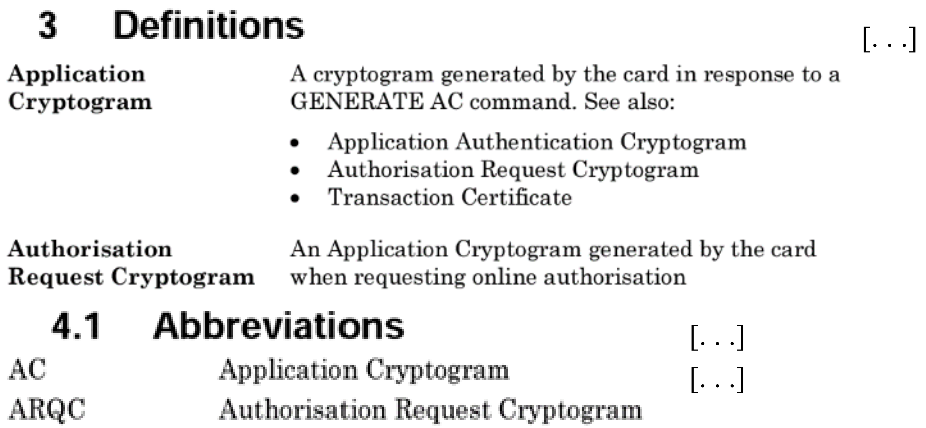
Claim Language	Accused Products
	 **Privacy and Security** Apple takes your privacy and security seriously. It's not just a philosophy, it's built into all our products. And Apple Card is no different. With advanced security technologies like Face ID, Touch ID, and unique transaction codes, Apple Card with Apple Pay is designed to make sure you're the only one who can use it. The titanium card has no visible numbers. Not on the front. Not on the back. Which gives you an enhanced level of security. And your data isn't sold to third parties for marketing or advertising. *See, e.g.*, *Apple Card*, Apple, https://www.apple.com/apple-card/ (last visited Dec. 30, 2024); *How to request or replace a titanium Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102517.
1[b] a memory;	The Apple Card includes a memory (*e.g.*, memory of the EMV chip).   **Titanium Card** With laser etching and clean styling, Apple Card is designed with the same craftsmanship we bring to all our products. And it's the only credit card made of titanium — a sustainable metal known for its beauty and durability. When you use the card, you'll get 1% Daily Cash back on every purchase. Since Mastercard is our global payment network, you can use it all over the world. For apps and websites that don't take Apple Pay yet, just enter the virtual card number stored securely in your Wallet app. And when you're using Safari, it even autofills for you.  *See, e.g.*, *Apple Card*, Apple, https://www.apple.com/apple-card/ (last visited Dec. 30, 2024); *How to request or replace a titanium Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102517; Joe Wituschek, *Apple Card: Everything you need to know!*; iMore (last updated Jan. 21, 2022), https://www.imore.com/apple-goldman-sachs-credit-card ("The front of the card features the cardholder's name, the Apple logo, and the EMV chip that has been redesigned by Apple."); Arun Venkatesan, *The design of Apple's credit card*, arun.is (Mar. 28, 2019), https://arun.is/blog/apple-card/ ("Apple's video shows a card blank being cut from a single sheet of titanium. Then, a CNC mill cuts out a space for the EMV chip to be inserted in a later step.").

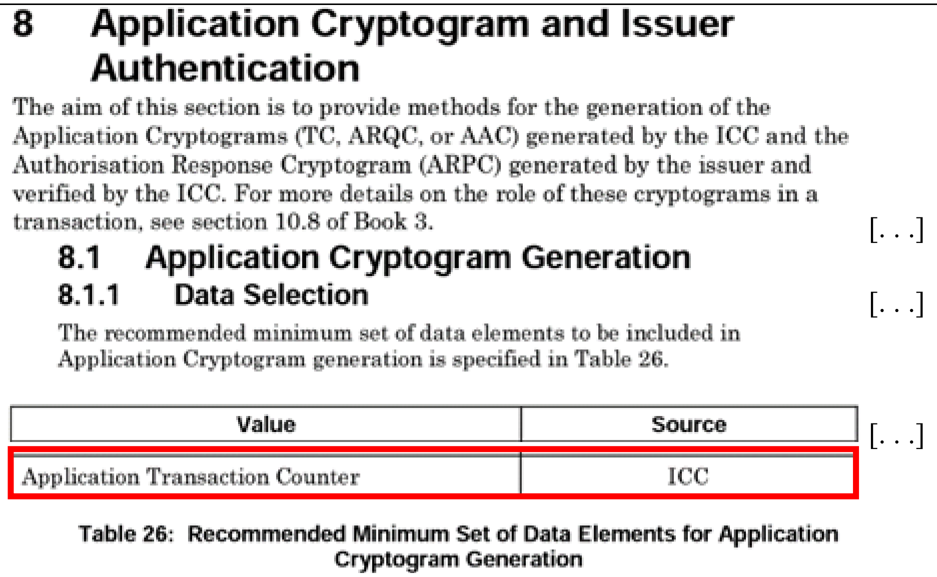
Claim Language	**Accused Products**
	 MY BANK 0012 7456 2390 5185 The distinguishing feature of EMV chip transactions is that the payment application is resident in a secure chip that is embedded in a plastic payment card (often referred to as a chip card or smart card), a personal device such as a mobile phone or other form factors such as wristbands or watches. The secure chip provides three key elements: • It can perform processing functions. • It is able to store confidential information very securely. • It can perform cryptographic processing. *See, e.g.*, *A Guide to EMV Chip Technology*, Version 2.0 at 5 (Nov. 2014) *available at* https://usermanual.wiki/Document/AGuidetoEMVChipTechnologyv2020141120122132753.1666646776.pdf.
1[c] a cryptographic processor coupled to the memory; and	The Apple Card includes a cryptographic processor (*e.g.*, processor of the EMV chip) coupled to the memory (*e.g.*, as identified above).  Marisa Robertson Goodbye, plastic. Hello, titanium. Marisa Robertson Goldman Sachs mastercard **Titanium Card** With laser etching and clean styling, Apple Card is designed with the same craftsmanship we bring to all our products. And it's the only credit card made of titanium — a sustainable metal known for its beauty and durability. When you use the card, you'll get 1% Daily Cash back on every purchase. Since Mastercard is our global payment network, you can use it all over the world. For apps and websites that don't take Apple Pay yet, just enter the virtual card number stored securely in your Wallet app. And when you're using Safari, it even autofills for you. *See, e.g.*, *Apple Card*, Apple, https://www.apple.com/apple-card/ (last visited Dec. 30, 2024); *How to request or replace a titanium Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102517; Joe Wituschek, *Apple Card: Everything you need to know!*; iMore (last updated Jan. 21, 2022), https://www.imore.com/apple-goldman-sachs-credit-card ("The front of the card features the cardholder's name, the Apple logo, and the EMV chip that has been redesigned by Apple."); Arun Venkatesan, *The design of Apple's credit card*, arun.is (Mar. 28, 2019), https://arun.is/blog/apple-card/ ("Apple's video shows a card blank being cut from a single sheet of titanium. Then, a CNC mill cuts out a space for the EMV chip to be inserted in a later step.").

Claim Language	**Accused Products**
	 MY BANK 0012 7456 2390 5185 The distinguishing feature of EMV chip transactions is that the payment application is resident in a secure chip that is embedded in a plastic payment card (often referred to as a chip card or smart card), a personal device such as a mobile phone or other form factors such as wristbands or watches. The secure chip provides three key elements: • It can perform processing functions. • It is able to store confidential information very securely. • It can perform cryptographic processing. *See, e.g.*, *A Guide to EMV Chip Technology*, Version 2.0 at 5 (Nov. 2014) *available at* https://usermanual.wiki/Document/AGuidetoEMVChipTechnologyv20201411201221327 53.1666646776.pdf.
1[d] a reader interface, including at least one interface selected from a set comprising: a magnetic-stripe, a smart card reader interface, a mag-stripe inductor interface, an RF interface, an NFC interface, and a wireless interface, and	The Apple Card includes a reader interface, including at least one interface selected from a set comprising: a magnetic-stripe (*e.g.*, on the back and bottom of the Apple Card), a smart card reader interface (*e.g.*, EMV chip on the front of the Apple Card), a mag-stripe inductor interface, an RF interface, an NFC interface, and a wireless interface.  Titanium Card With laser etching and clean styling, Apple Card is designed with the same craftsmanship we bring to all our products. And it's the only credit card made of titanium — a sustainable metal known for its beauty and durability. When you use the card, you'll get 1% Daily Cash back on every purchase. Since Mastercard is our global payment network, you can use it all over the world. For apps and websites that don't take Apple Pay yet, just enter the virtual card number stored securely in your Wallet app. And when you're using Safari, it even autofills for you.  *See, e.g.*, *Apple Card*, Apple, https://www.apple.com/apple-card/ (last visited Dec. 30, 2024); *How to request or replace a titanium Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102517; Joe Wituschek, *Apple Card: Everything you need to know!*; iMore (last updated Jan. 21, 2022), https://www.imore.com/apple-goldman-sachs-credit-card ("The front of the card features the cardholder's name, the Apple logo, and the EMV chip that has been redesigned by Apple. The back of the card displays the Goldman Sachs and Mastercard logos, as well as the magnetic stripe, which runs to the bottom of the card.").

Claim Language	**Accused Products**
1[e] wherein payment information for a transaction is operable to be conveyed via the reader interface and comprises limited-use payment information, and wherein further the limited-use payment information is to be used in place of card issuer payment information for payment transactions by said device at payment card reader facilities.	The Apple Card conveys payment information for a transaction via the reader interface (*e.g.*, the magnetic stripe and the EMV chip), the payment information for a transaction comprising limited-use payment information (*e.g.*, Card Validation Value 1 ("CVV1") limited to magnetic stripe facilities or Card Validation Value 3 ("CVV3") limited to smart chip readers), and wherein further the limited-use payment information is to be used in place of card issuer payment information (*e.g.*, the CVV1 and CVV3 are used, on information and belief, in place of the Apple Card security code stored on an accompanying iPhone, which is a Card Validation Value 2 ("CVV2")) for payment transactions by said device at payment card reader facilities (*e.g.*, at magnetic stripe readers and smart chip readers). *See* limitation 1[d].  9:41 Card Information Name Michael Ohara Card Number Expiration Security Code Network Mastercard Request New Card Number Use this card number to make online purchases or anywhere Apple Pay is not yet accepted. Replace your card number with a new one if you suspect your current number has been compromised. Device Account Number •••• Apple Card uses this number for Apple Pay transactions made using this iPhone. *See, e.g.*, Andrew O'Hara, *Tips and tricks for mastering Apple Card*, AppleInsider (Aug. 20, 2019), https://appleinsider.com/articles/19/08/20/tips-and-tricks-for-mastering-apple-card ("If you want to use your Apple Card online, and the retailer doesn't support Apple Pay or autofill in Safari, you have to manually enter in your card number. Those details can be readily found within the Wallet app."); Jason Fernando, *Validation Code: What it is, How it Works, Example*, Investopedia (last updated Mar. 15, 2021), https://www.investopedia.com/terms/v/validation-code.asp ("A validation code—also known as a CVV, CV2, or CVV2 code—is a series of three or four numbers located on the front or back of a credit card. It is intended to provide an additional layer of security for credit card transactions that take place online or over the phone."). The magnetic stripe on the bottom of the Apple Card conveys limited-use payment information, including the Primary Account Number ("PAN"), Expiration ("EXP"), Cardholder Name ("CHN"), and CVV1 according to the ISO7812 standard. This information is used in place of the CVV2 for transactions at magnetic stripe readers. *See, e.g.*, ISO/IEC7812-1:2017 *available at* https://www.iso.org/standard/70484.html.

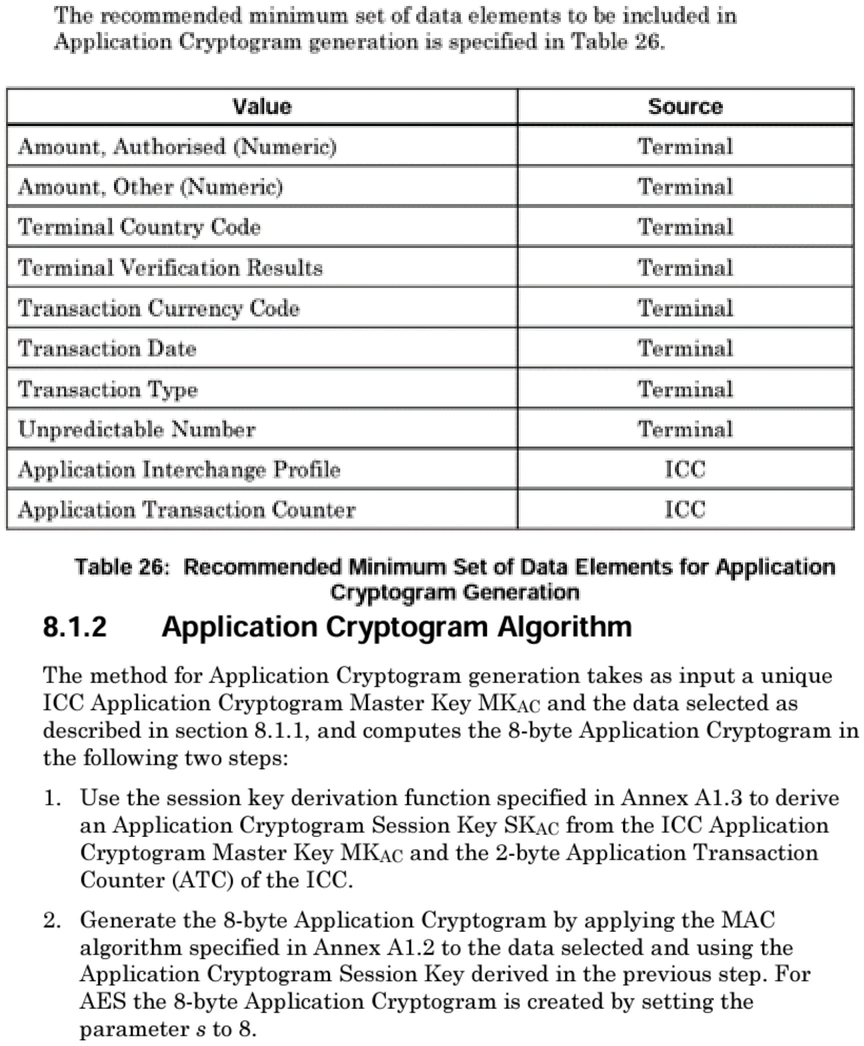
Claim Language	**Accused Products**
	The smart card reader interface (EMV chip) on the front of the Apple Card conveys limited-use payment information, including the PAN, EXP, CHN, and the single-use CVV3 according to the EMV and ISO7816 standards, which is used in place of the CVV2 for transactions at smart card readers. *See, e.g.*, ISO/IEC 7816-8:2021 *available at* https://www.iso.org/standard/79893.html; ISO/IEC 7816-8:2019 *available at* https://www.iso.org/standard/75844.html; *A Guide to EMV Chip Technology*, Version 2.0 at 5 (Nov. 2014) *available at* https://usermanual.wiki/Document/AGuidetoEMVChipTechnologyv2020141120122132753.1666646776.pdf.
2. The device of claim 1, wherein the body comprises fixed payment information disposed thereon and wherein the fixed payment information includes only: a card-holder name; a payment issuing logo; and a card payment network logo, and wherein further, the body is free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon.	The Apple Card comprises fixed payment information disposed thereon and wherein the fixed payment information includes only: a card-holder name (*e.g.*, "Marisa Robertson" below); a payment issuing logo (*e.g.*, "Goldman Sachs"); and a card payment network logo (*e.g.*, "MasterCard" below), and wherein further, the body is free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon.  Marisa Robertson Goodbye, plastic. Hello, titanium. Marisa Robertson Goldman Sachs mastercard **Titanium Card** With laser etching and clean styling, Apple Card is designed with the same craftsmanship we bring to all our products. And it's the only credit card made of titanium — a sustainable metal known for its beauty and durability. When you use the card, you'll get 1% Daily Cash back on every purchase. Since Mastercard is our global payment network, you can use it all over the world. For apps and websites that don't take Apple Pay yet, just enter the virtual card number stored securely in your Wallet app. And when you're using Safari, it even autofills for you.  **Privacy and Security** Apple takes your privacy and security seriously. It's not just a philosophy, it's built into all our products. And Apple Card is no different. With advanced security technologies like Face ID, Touch ID, and unique transaction codes, Apple Card with Apple Pay is designed to make sure you're the only one who can use it. The titanium card has no visible numbers. Not on the front. Not on the back. Which gives you an enhanced level of security. And your data isn't sold to third parties for marketing or advertising. *See, e.g.*, *Apple Card*, Apple, https://www.apple.com/apple-card/ (last visited Dec. 30, 2024); *How to request or replace a titanium Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102517.

Claim Language	Accused Products
4. The device of claim 1, wherein said limited-use payment information is provided by a card issuing authority for use by the payment device and wherein the card processing authority rejects as invalid, any use of said limited-use payment information obtained via any means other than: a payment card reader reading said limited-use payment information from the reader interface.	The Apple Card conveys limited-use payment information (*e.g.*, CVV1, CVV3) that is provided by a card issuing authority for use by the payment device and wherein the card processing authority rejects as invalid, any use of said limited-use payment information obtained via any means other than: a payment card reader (*e.g.*, magnetic stripe reader or smart card reader) reading said limited-use payment information from the reader interface (*e.g.*, magnetic stripe, EMV chip). *See supra* limitations 1[d] and 1[e]. The CVV1 and CVV3 are only useable with particular card reader interfaces. Thus, a card processing authority will reject transactions using the limited-use payment information if it is not received from the correct card reader interface (*i.e.*, if a CVV1 is attempted to be used in place of a CVV2 during a card-not-present transaction).
10[a] The device of claim 1, wherein the processor cryptographically dynamically generates a one-time limited-use number based on combination of a card device transaction sequence count, and	The Apple Card comprises a processor (*e.g.*, the EMV chip) that cryptographically dynamically generates a one-time limited-use number (*e.g.*, CVV3) based on the combination of a card device transaction sequence count (*e.g.*, Application Transaction Counter) and one of the following pieces of information. *See supra* limitation 1[c], 1[e].  **3 Definitions** [. . .] **Application Cryptogram** A cryptogram generated by the card in response to a GENERATE AC command. See also: • Application Authentication Cryptogram • Authorisation Request Cryptogram • Transaction Certificate **Authorisation Request Cryptogram** An Application Cryptogram generated by the card when requesting online authorisation **4.1 Abbreviations** [. . .] AC Application Cryptogram [. . .] ARQC Authorisation Request Cryptogram

<table>
<tr><th>Claim Language</th><th>Accused Products</th></tr>
<tr><td></td><td>

<h2>8 Application Cryptogram and Issuer Authentication</h2>
<p>The aim of this section is to provide methods for the generation of the Application Cryptograms (TC, ARQC, or AAC) generated by the ICC and the Authorisation Response Cryptogram (ARPC) generated by the issuer and verified by the ICC. For more details on the role of these cryptograms in a transaction, see section 10.8 of Book 3.</p>
<p>[. . .]</p>
<h3>8.1 Application Cryptogram Generation</h3>
<h3>8.1.1 Data Selection</h3>
<p>[. . .]</p>
<p>The recommended minimum set of data elements to be included in Application Cryptogram generation is specified in Table 26.</p>
<table>
<tr><th>Value</th><th>Source</th></tr>
<tr><td>Application Transaction Counter</td><td>ICC</td></tr>
</table>
<p>[. . .]</p>
<p><b>Table 26: Recommended Minimum Set of Data Elements for Application Cryptogram Generation</b></p>
<p><i>See, e.g.</i>, EMVCo, <i>EMV Integrated Circuit Card Specifications for Payment Systems, Book 2 – Security and Key Management v4.3</i> at 11, 21, 87–88 (Nov. 2011).</p>
</td></tr>
<tr><td>10[b] at least one of a set of information including: a user information; a user card account number; a device account number; device secret keys; card issuer keys; a time; a merchant; a location; an online address; a payment information; a card reader information; an account information; an amount; a transaction information; and a cryptographic combination of at least two of the above set of information, and</td><td>
<p>The Apple Card comprises a processor (<i>e.g.</i>, EMV chip) that cryptographically dynamically generates a one-time limited-use number (<i>e.g.</i>, the CVV3) based on at least one of a set of information include a user information; a user card account number; a device account number; device secret keys; card issuer keys; a time; a merchant; a location; an online address; a payment information; a card reader information (<i>e.g.</i>, Terminal Country Code); an account information (<i>e.g.</i>, cryptographic keys); an amount <i>(e.g.</i>, Amount, Authorized or Amount, Other); a transaction information (<i>e.g.</i>, Transaction Date, Transaction Type); and a cryptographic combination of at least two of the above set of information.</p>
<p><i>See supra</i> limitation 1[c], 1[e], 10[a].</p>

<h3>8.1 Application Cryptogram Generation</h3>
<h3>8.1.1 Data Selection</h3>
<p>[. . .]</p>
</td></tr>
</table>

Claim Language	**Accused Products**



The recommended minimum set of data elements to be included in Application Cryptogram generation is specified in Table 26.

Value	Source
Amount, Authorised (Numeric)	Terminal
Amount, Other (Numeric)	Terminal
Terminal Country Code	Terminal
Terminal Verification Results	Terminal
Transaction Currency Code	Terminal
Transaction Date	Terminal
Transaction Type	Terminal
Unpredictable Number	Terminal
Application Interchange Profile	ICC
Application Transaction Counter	ICC

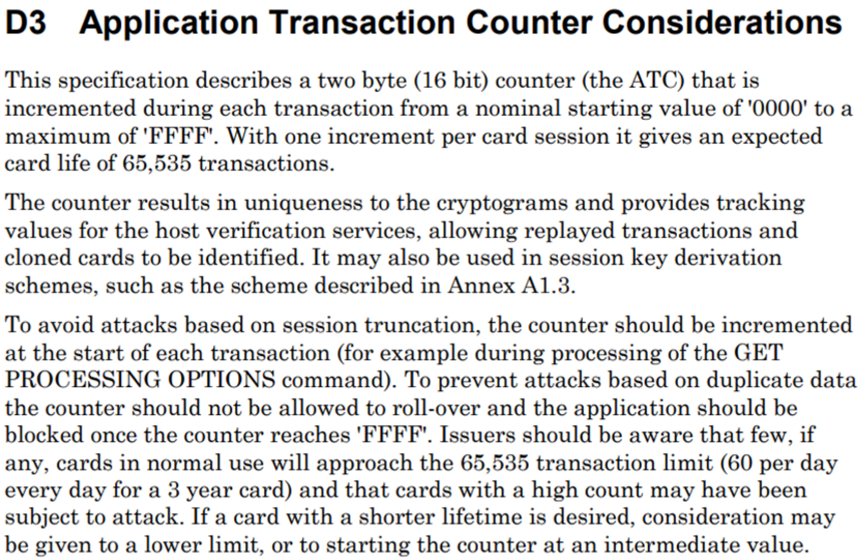
Table 26: Recommended Minimum Set of Data Elements for Application Cryptogram Generation

8.1.2 Application Cryptogram Algorithm

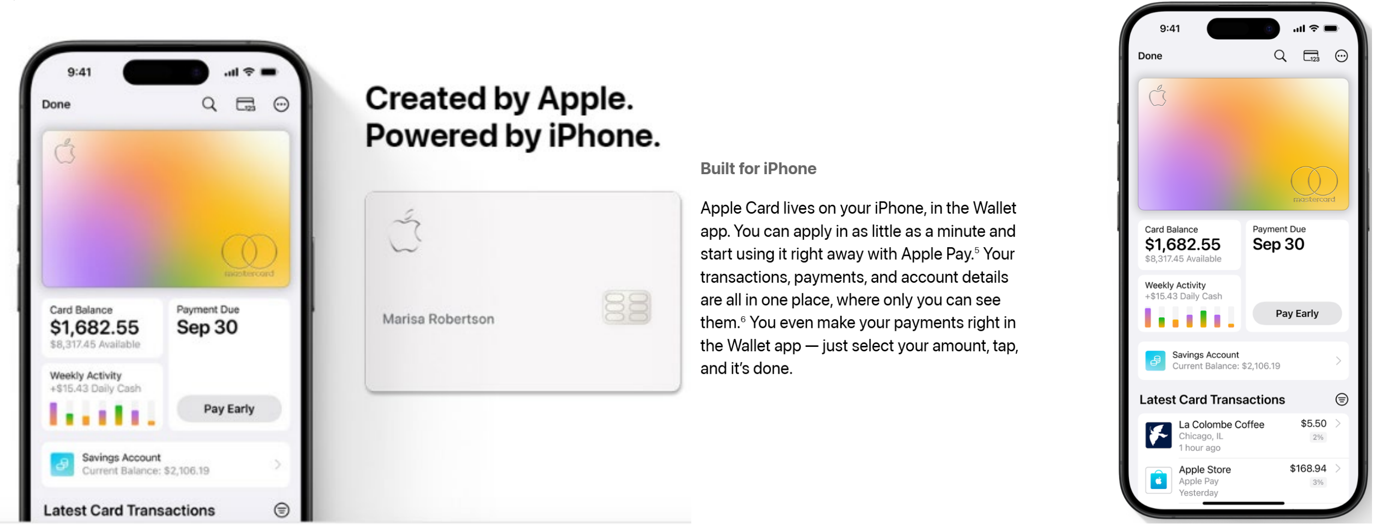
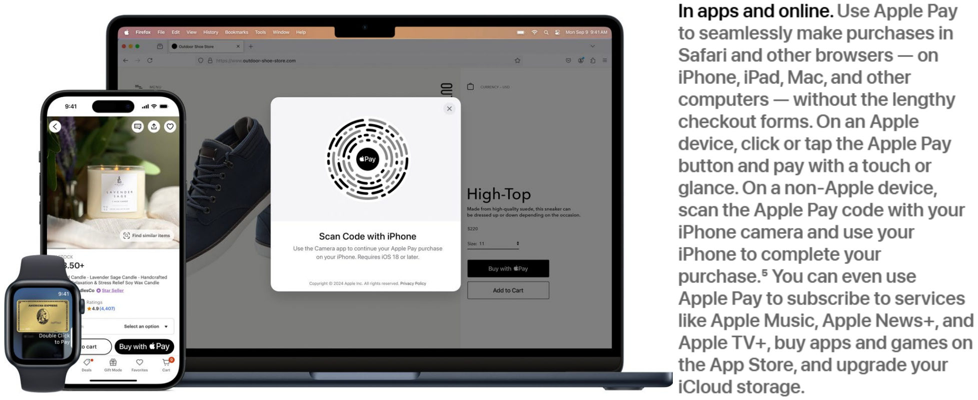
The method for Application Cryptogram generation takes as input a unique ICC Application Cryptogram Master Key MK_{AC} and the data selected as described in section 8.1.1, and computes the 8-byte Application Cryptogram in the following two steps:

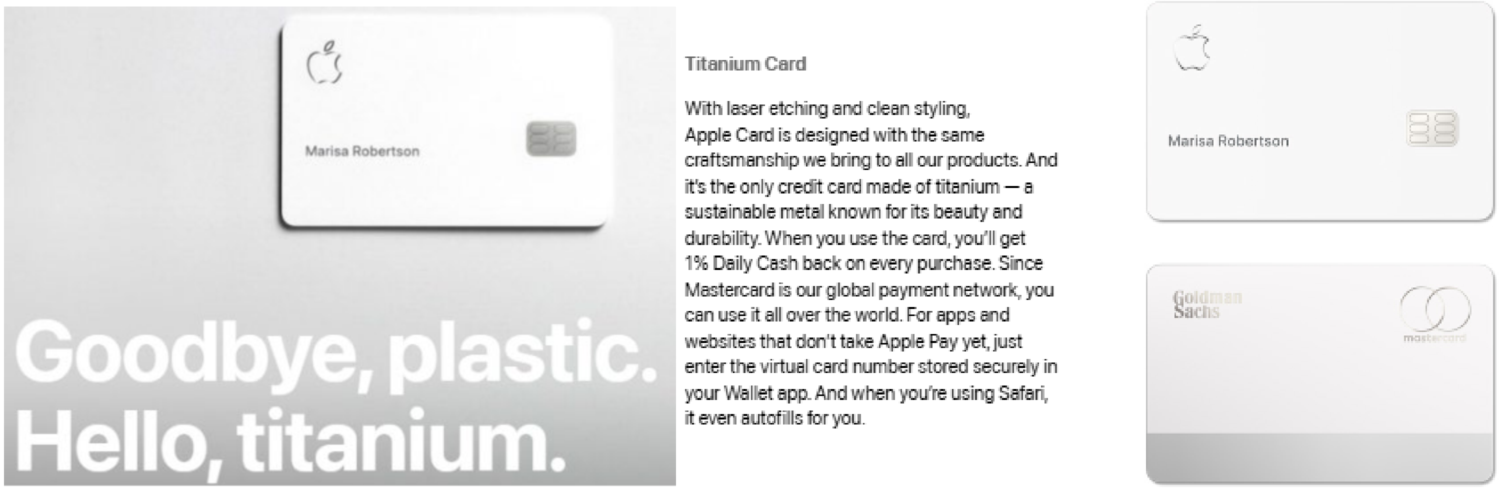
1. Use the session key derivation function specified in Annex A1.3 to derive an Application Cryptogram Session Key SK_{AC} from the ICC Application Cryptogram Master Key MK_{AC} and the 2-byte Application Transaction Counter (ATC) of the ICC.
2. Generate the 8-byte Application Cryptogram by applying the MAC algorithm specified in Annex A1.2 to the data selected and using the Application Cryptogram Session Key derived in the previous step. For AES the 8-byte Application Cryptogram is created by setting the parameter s to 8.

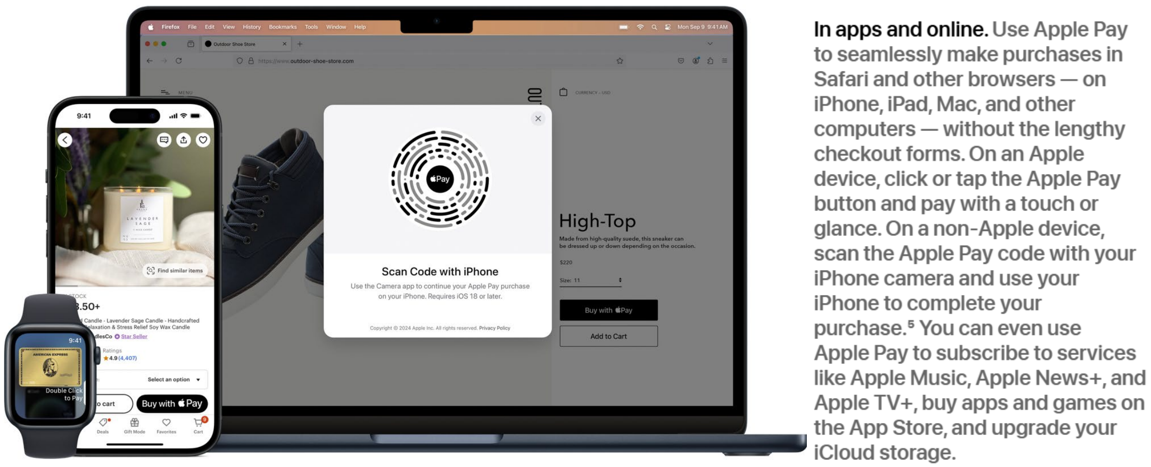
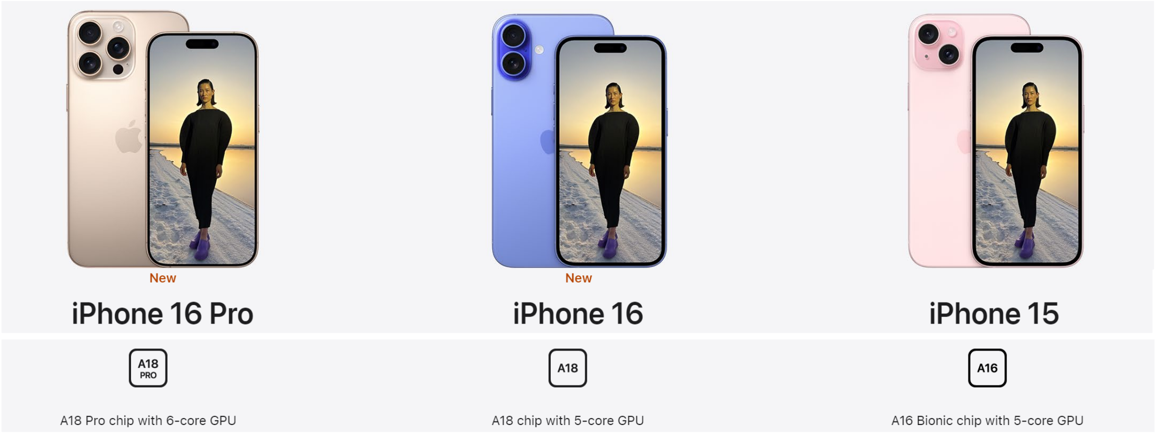
See, e.g., EMVCo, *EMV Integrated Circuit Card Specifications for Payment Systems, Book 2 – Security and Key Management v4.3* at 11, 21, 87–89 (Nov. 2011).

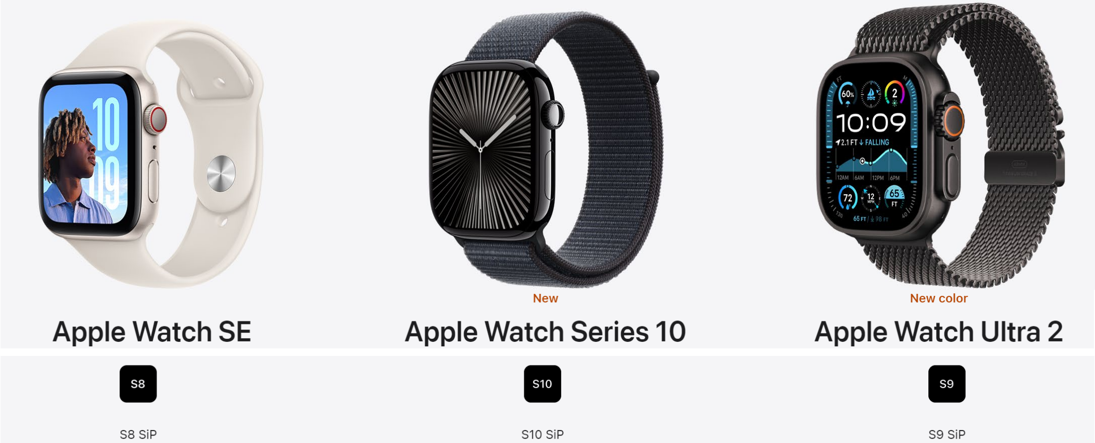
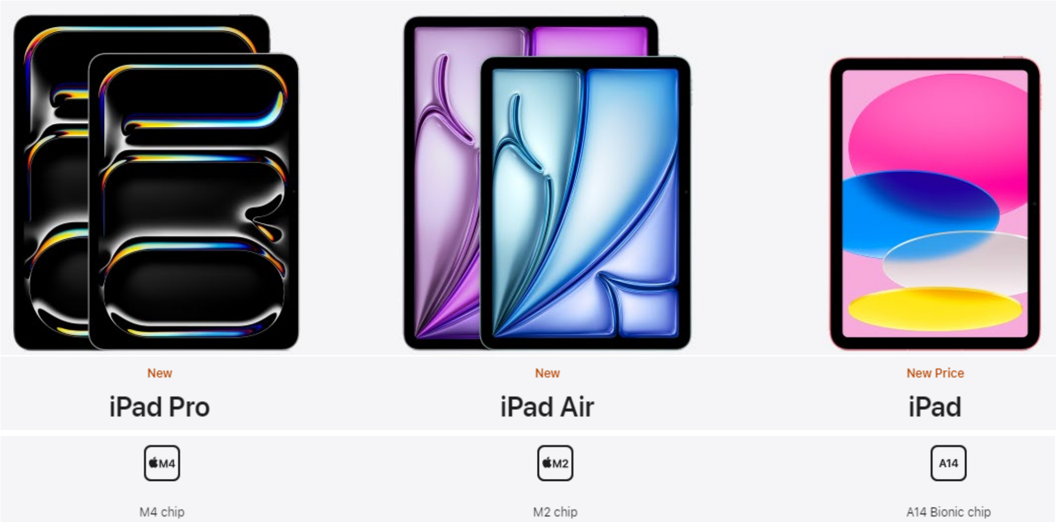
Claim Language	Accused Products
10[c] wherein the processor increments the card device transaction sequence count on each transaction.	The Apple Card comprises a processor (*e.g.*, EMV chip) that increments the card device transaction sequence count (*e.g.*, Application Transaction Counter) on each transaction.  **D3 Application Transaction Counter Considerations** This specification describes a two byte (16 bit) counter (the ATC) that is incremented during each transaction from a nominal starting value of '0000' to a maximum of 'FFFF'. With one increment per card session it gives an expected card life of 65,535 transactions. The counter results in uniqueness to the cryptograms and provides tracking values for the host verification services, allowing replayed transactions and cloned cards to be identified. It may also be used in session key derivation schemes, such as the scheme described in Annex A1.3. To avoid attacks based on session truncation, the counter should be incremented at the start of each transaction (for example during processing of the GET PROCESSING OPTIONS command). To prevent attacks based on duplicate data the counter should not be allowed to roll-over and the application should be blocked once the counter reaches 'FFFF'. Issuers should be aware that few, if any, cards in normal use will approach the 65,535 transaction limit (60 per day every day for a 3 year card) and that cards with a high count may have been subject to attack. If a card with a shorter lifetime is desired, consideration may be given to a lower limit, or to starting the counter at an intermediate value. *See, e.g.*, EMVCo*, Integrated Circuit Card Specifications for Payment Systems: Book 2: Security and Key Management v.4.3* at 147 (Nov. 2011).

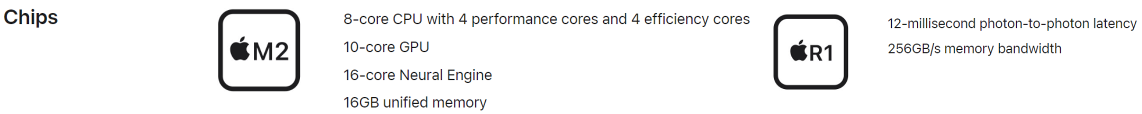
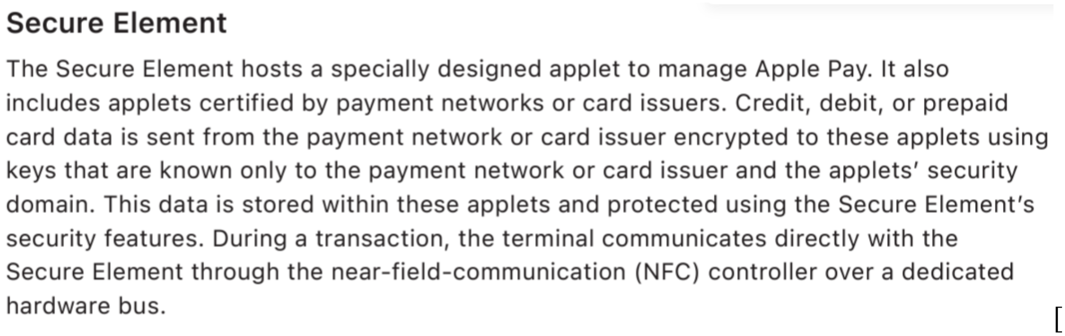
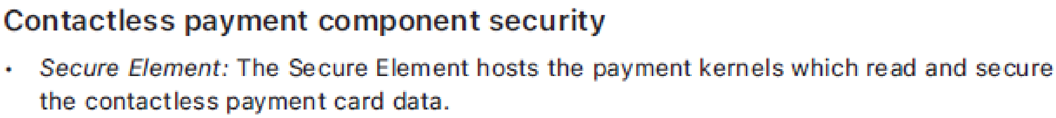
II. Claim 11 and Dependent Claims 12–14

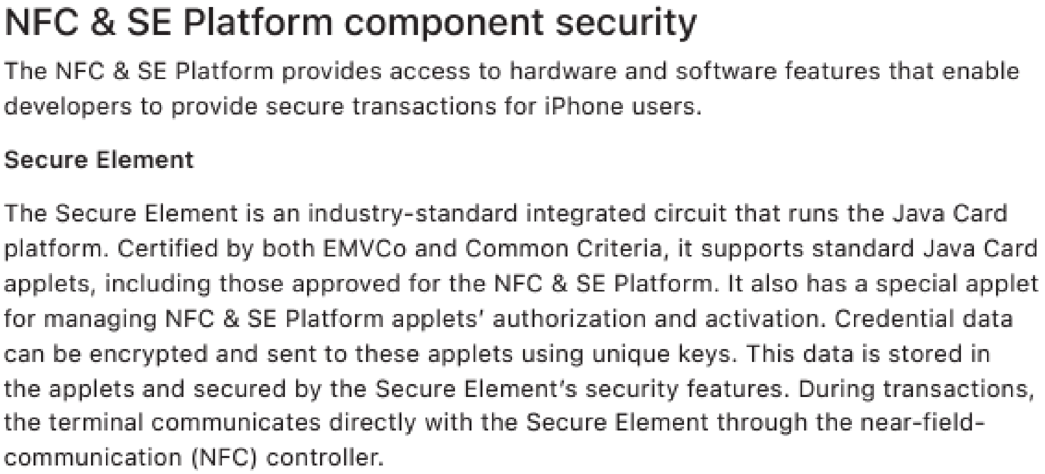
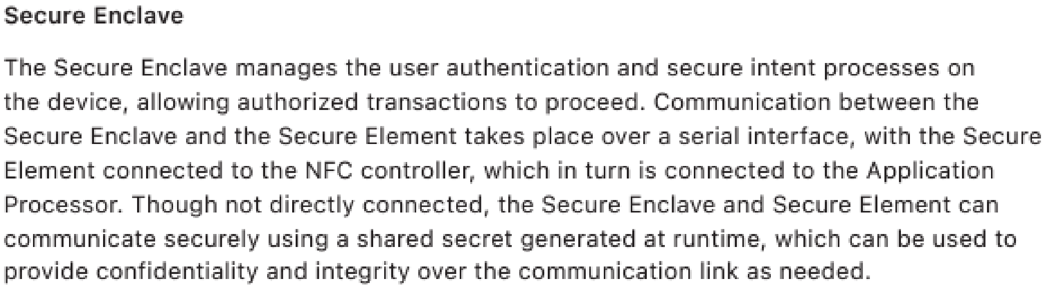
Claim Language	Accused Products
11[Pre]: An online payment system, the system comprising:	To the extent the preamble is limiting, the combination of an Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—with an Apple Card is an online payment system.  **Created by Apple. Powered by iPhone.** Built for iPhone Apple Card lives on your iPhone, in the Wallet app. You can apply in as little as a minute and start using it right away with Apple Pay.[5] Your transactions, payments, and account details are all in one place, where only you can see them.[6] You even make your payments right in the Wallet app — just select your amount, tap, and it's done. 9:41 Done Card Balance $1,682.55 $8,317.45 Available Payment Due Sep 30 Weekly Activity +$15.43 Daily Cash Pay Early Savings Account Current Balance: $2,106.19 Latest Card Transactions Marisa Robertson La Colombe Coffee Chicago, IL 1 hour ago $5.50 2% Apple Store Apple Pay Yesterday $168.94 3% *See, e.g.*, *Apple Card*, Apple, https://www.apple.com/apple-card/ (last visited Dec. 30, 2024).  **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.*, *Apple Pay*, Apple, https://www.apple.com/apple-pay/ (last visited Dec. 30, 2024); *Devices compatible with Apple Pay*, Apple (Nov. 22, 2024), https://support.apple.com/en-us/102896; Abby Ferguson, *How to set up Apple Pay*, 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.").

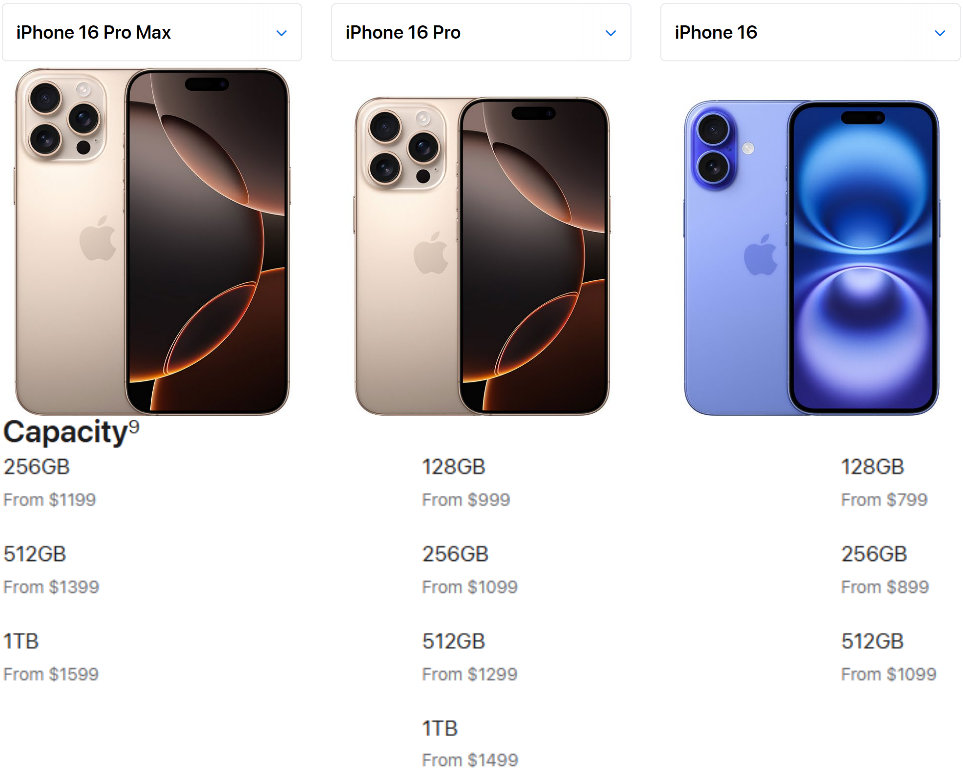
Claim Language	**Accused Products**
11[a]: a thin payment device comprising no fixed payment numbers visible thereon; and	The Apple Card is a thin shaped body having no fixed payment numbers disposed thereon.  Marisa Robertson Goodbye, plastic. Hello, titanium. Marisa Robertson Goldman Sachs mastercard Titanium Card With laser etching and clean styling, Apple Card is designed with the same craftsmanship we bring to all our products. And it's the only credit card made of titanium — a sustainable metal known for its beauty and durability. When you use the card, you'll get 1% Daily Cash back on every purchase. Since Mastercard is our global payment network, you can use it all over the world. For apps and websites that don't take Apple Pay yet, just enter the virtual card number stored securely in your Wallet app. And when you're using Safari, it even autofills for you. Privacy and Security Apple takes your privacy and security seriously. It's not just a philosophy, it's built into all our products. And Apple Card is no different. With advanced security technologies like Face ID, Touch ID, and unique transaction codes, Apple Card with Apple Pay is designed to make sure you're the only one who can use it. The titanium card has no visible numbers. Not on the front. Not on the back. Which gives you an enhanced level of security. And your data isn't sold to third parties for marketing or advertising. *See, e.g.*, *Apple Card*, Apple, https://www.apple.com/apple-card/ (last visited Dec. 30, 2024); *How to request or replace a titanium Apple Card*, Apple Support (Dec. 17, 2024), https://support.apple.com/en-us/102517.

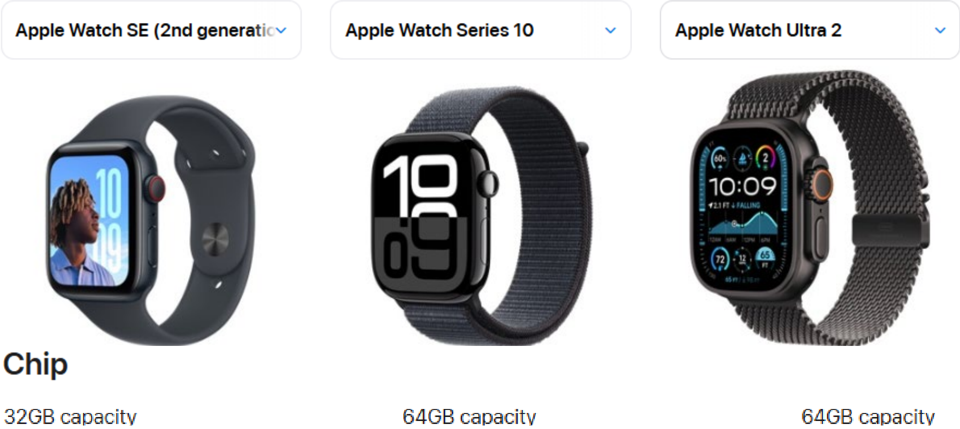
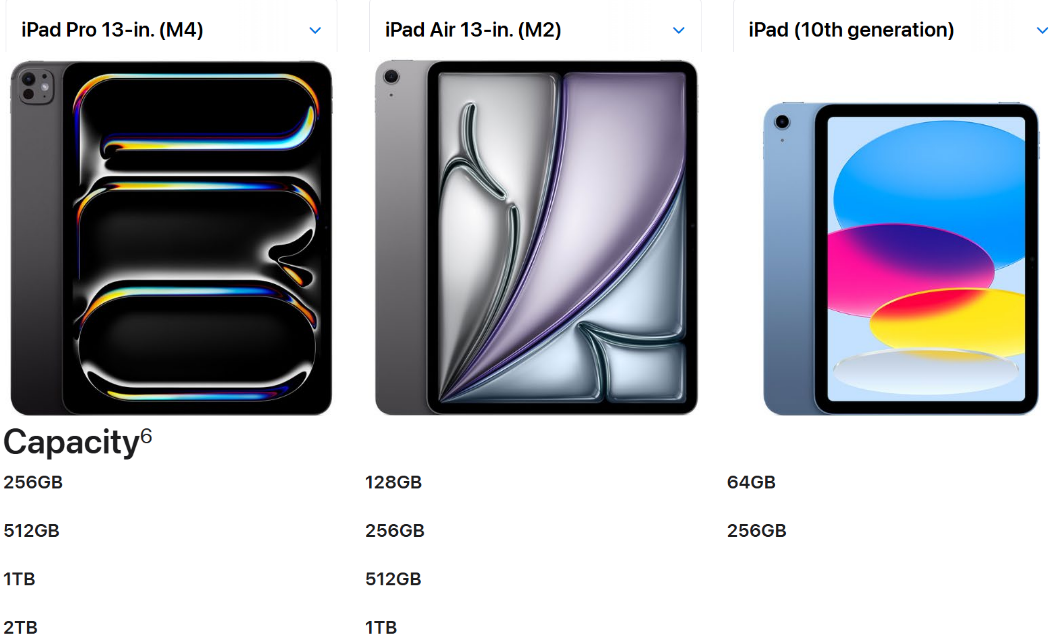
Claim Language	Accused Products
11[b]: a personal computing device, wherein the personal computing device comprises:	Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—is a personal computing device.  Scan Code with iPhone High-Top Buy with Pay Add to Cart **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.*, *Apple Pay*, Apple, https://www.apple.com/apple-pay/ (last visited Dec. 27, 2024); *Devices compatible with Apple Pay*, Apple (Nov. 22, 2024), https://support.apple.com/en-us/102896; Abby Ferguson, *How to set up Apple Pay*, 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.").
11[c]: a processor;	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—includes a processor (*e.g.*, system processor, processor of secure element, processor of secure enclave, or combination of the same).  New iPhone 16 Pro A18 PRO A18 Pro chip with 6-core GPU New iPhone 16 A18 A18 chip with 5-core GPU iPhone 15 A16 A16 Bionic chip with 5-core GPU [. . .] *See, e.g.*, *iPhone*, Apple, https://www.apple.com/iphone/ (last visited Dec. 27, 2024).

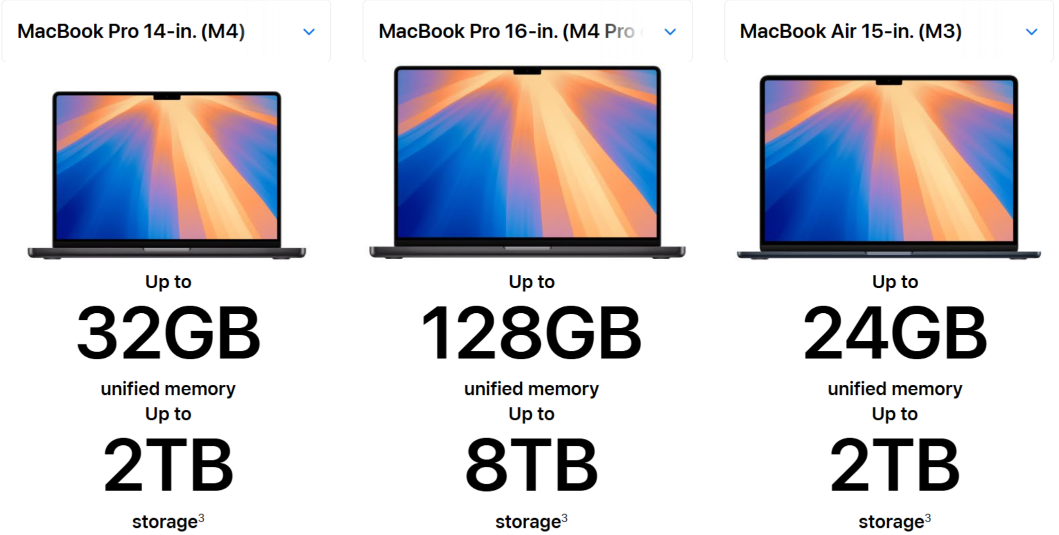
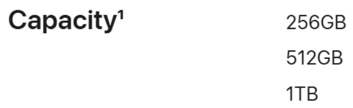
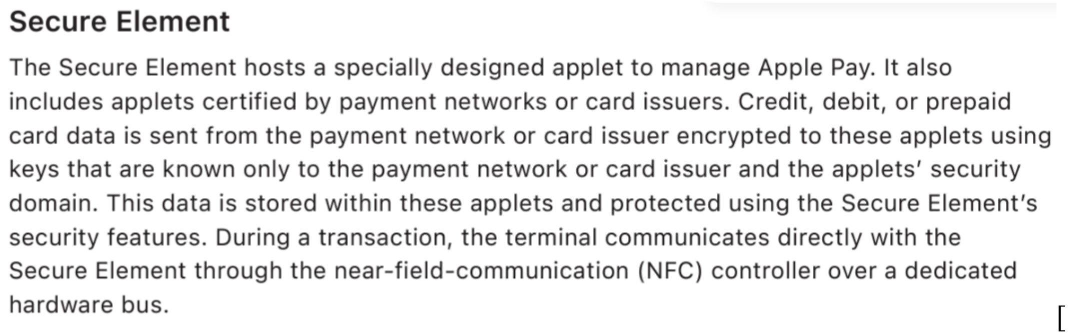
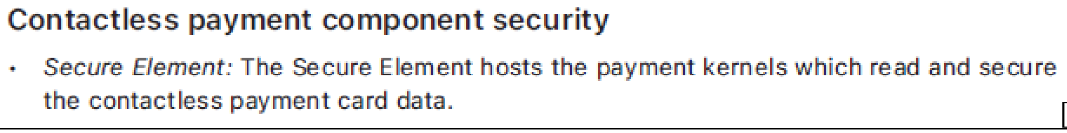
Claim Language	**Accused Products**
	 Apple Watch SE New Apple Watch Series 10 New color Apple Watch Ultra 2 S8 S8 SiP S10 S10 SiP S9 S9 SiP[. . .] *See, e.g.*, *Watch*, Apple, https://www.apple.com/watch/ (last visited Dec. 27, 2024).  New iPad Pro New iPad Air New Price iPad M4 M4 chip M2 M2 chip A14 A14 Bionic chip[. . .] *See, e.g.*, *iPad*, Apple, https://www.apple.com/ipad/ (last visited Dec. 30, 2024).

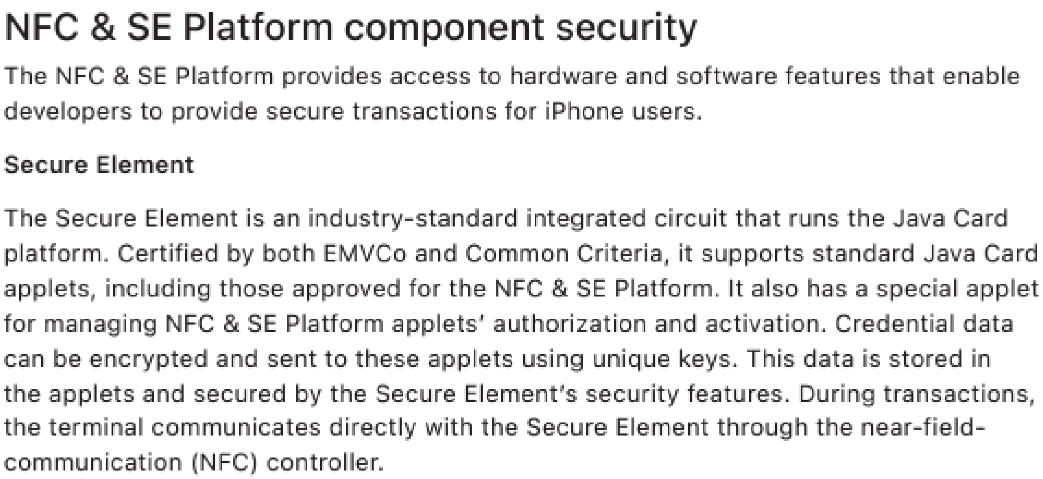
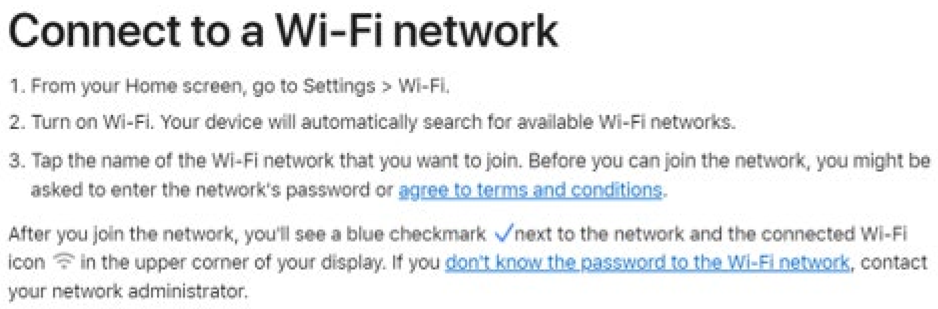
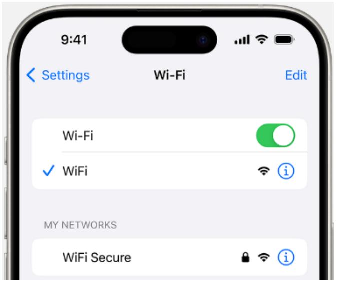
Claim Language	Accused Products
	  MacBook Pro 14″ and 16″ M4, M4 Pro, or M4 Max chip MacBook Air 13″ and 15″ M2 or M3 chip *See, e.g.*, *Mac*, Apple, https://www.apple.com/mac/ (last visited Dec. 30, 2024).  Chips M2 8-core CPU with 4 performance cores and 4 efficiency cores 10-core GPU 16-core Neural Engine 16GB unified memory R1 12-millisecond photon-to-photon latency 256GB/s memory bandwidth *See, e.g.*, *Apple Vision Pro – Tech Specs*, Apple, https://www.apple.com/apple-vision-pro/specs/ (last visited Dec. 30, 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** • *Secure Element:* The Secure Element hosts the payment kernels which read and secure the contactless payment card data. [. . .]

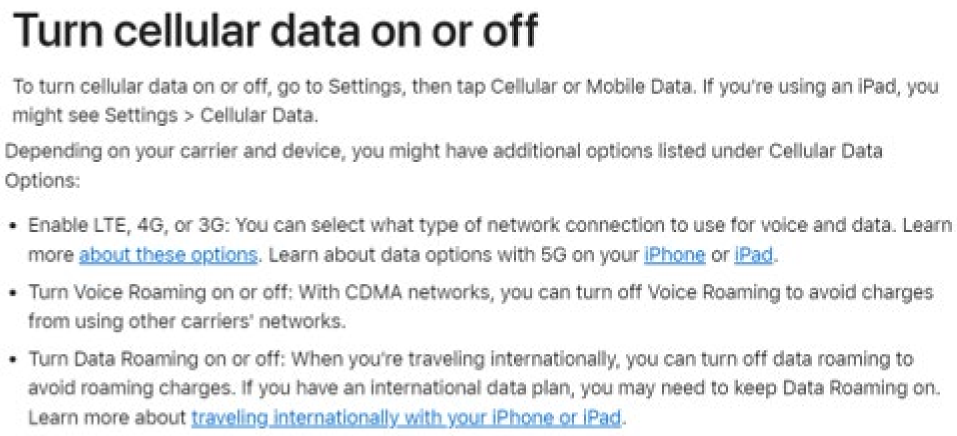
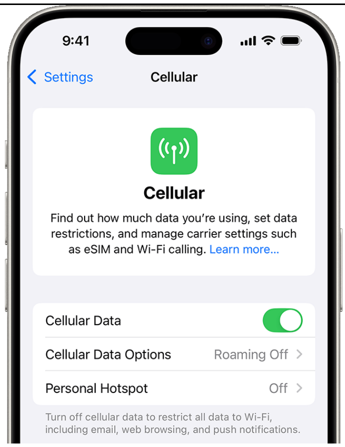
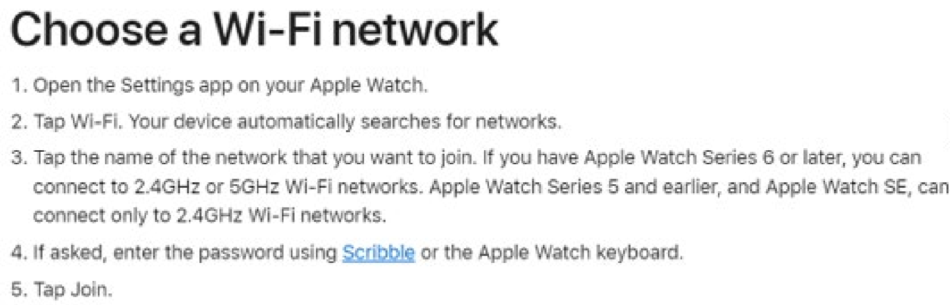
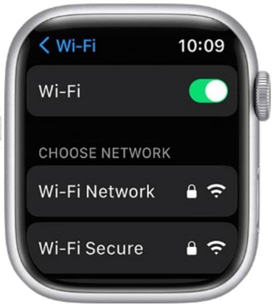
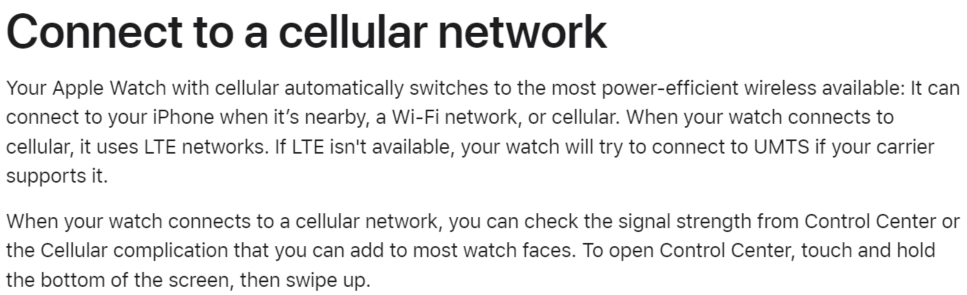
Claim Language	Accused Products
	 **NFC & SE Platform component security** The NFC & SE Platform provides access to hardware and software features that enable developers to provide secure transactions for iPhone users. **Secure Element** The Secure Element is an industry-standard integrated circuit that 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. *See, e.g.*, *Apple Platform Security*, at 178, 196, 260-261 (Dec. 2024), *available at* https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; *see also, e.g.*, Apple Platform Security, *How Apple Pay keeps users' purchases protected*, (Dec. 19, 2024), https://support.apple.com/guide/security/how-apple-pay-keeps-users-purchases-protected-seccb53a35f0/web; Apple Platform Security, *Tap to Pay on iPhone security* (Dec. 19, 2024), https://support.apple.com/guide/security/tap-to-pay-on-iphone-sec72cb155f4/web; Apple Platform Security, *NFC & SE Platform Security* (Dec. 19, 2024), https://support.apple.com/en-mn/guide/security/secda20f3f41/web.

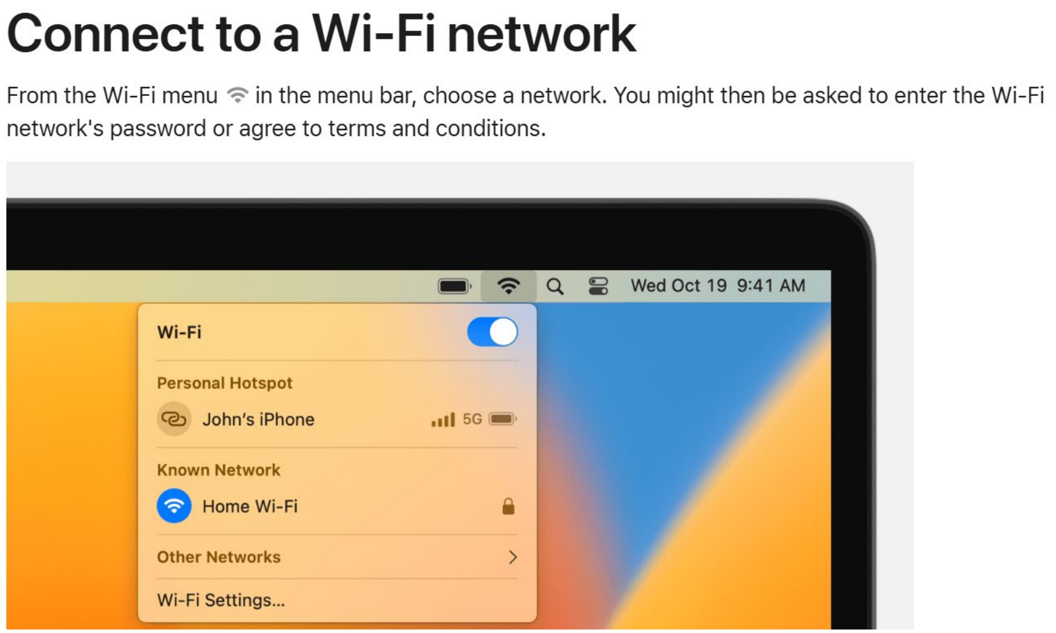
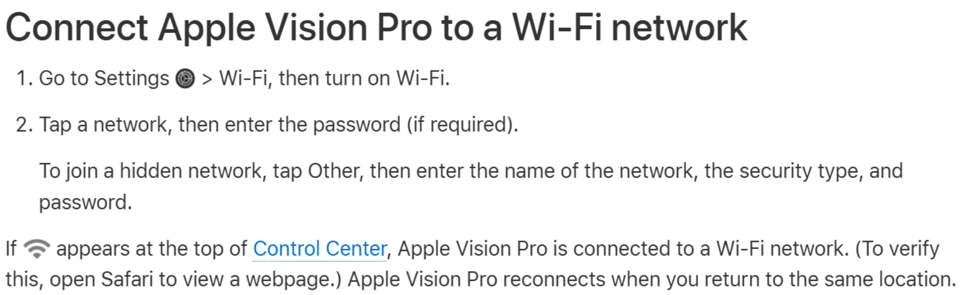
Claim Language	**Accused Products**
11[d]: a memory;	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—includes a memory (*e.g.*, system memory, memory of secure element, memory of secure enclave, memory of eSIM/SIM, or combination of the same).  Capacity[9] iPhone 16 Pro Max: 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, e.g.*, *Compare iPhone Models*, Apple, https://www.apple.com/iphone/compare/ (last visited Dec. 29, 2024); *What's the difference between device storage and iCloud storage?*, Apple (Sept. 16, 2024), https://support.apple.com/en-us/102670.

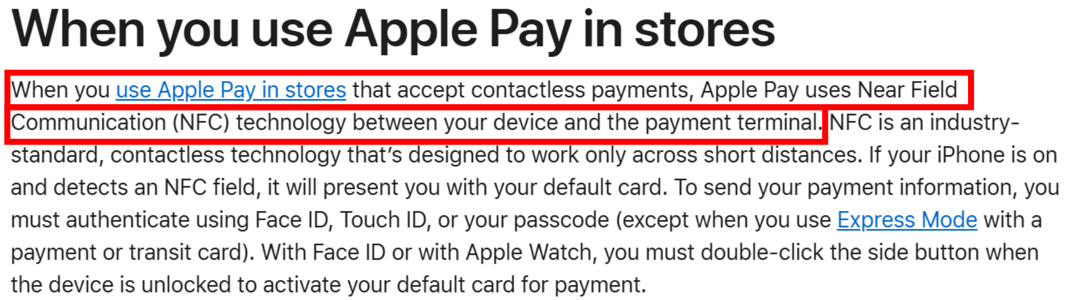
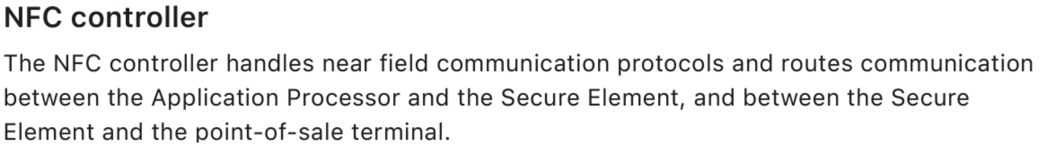
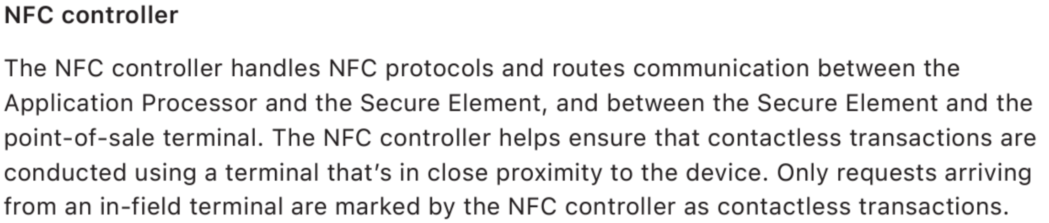
Claim Language	Accused Products
	 Apple Watch SE (2nd generatic Apple Watch Series 10 Apple Watch Ultra 2 Chip 32GB capacity 64GB capacity 64GB capacity [. . .] *See, e.g.*, *Compare Apple Watch models*, Apple https://www.apple.com/watch/compare/ (last visited Dec. 29, 2024); *If your Apple Watch storage 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.  iPad Pro 13-in. (M4) iPad Air 13-in. (M2) iPad (10th generation) Capacity[6] iPad Pro 13-in. (M4): 256GB, 512GB, 1TB, 2TB iPad Air 13-in. (M2): 128GB, 256GB, 512GB, 1TB iPad (10th generation): 64GB, 256GB [. . .] *See, e.g.*, *Compare iPad models*, Apple, https://www.apple.com/ipad/compare/ (last visited Dec. 30, 2024); *What's the difference between device storage and iCloud storage?*, Apple (Sept. 16, 2024), https://support.apple.com/en-us/102670; Allison Johnson, *The new iPads are ditching physical SIM cards*, The Verge (May 7, 2024), https://www.theverge.com/2024/5/7/24151262/apple-ipad-pro-air-esim-only ("First the iPhone, now the iPad — Apple is all in on an eSIM future, it seems.").

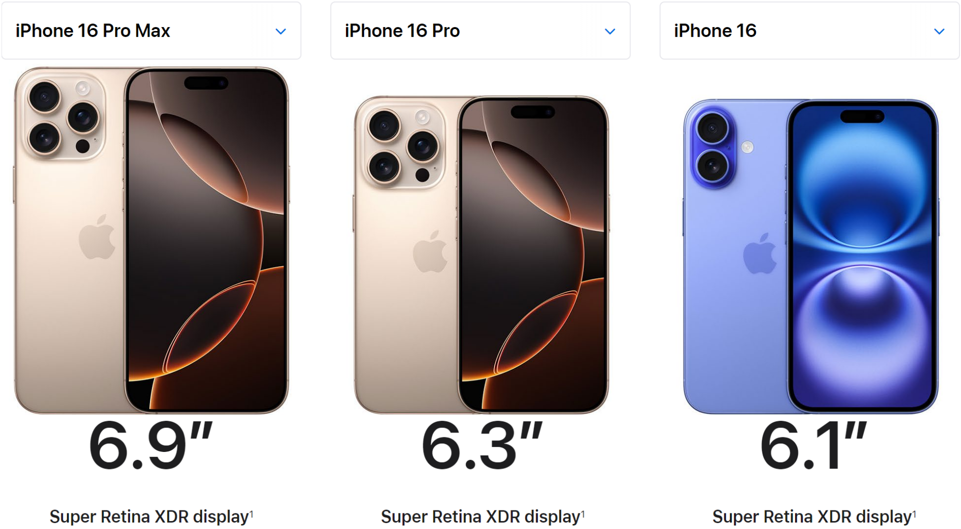
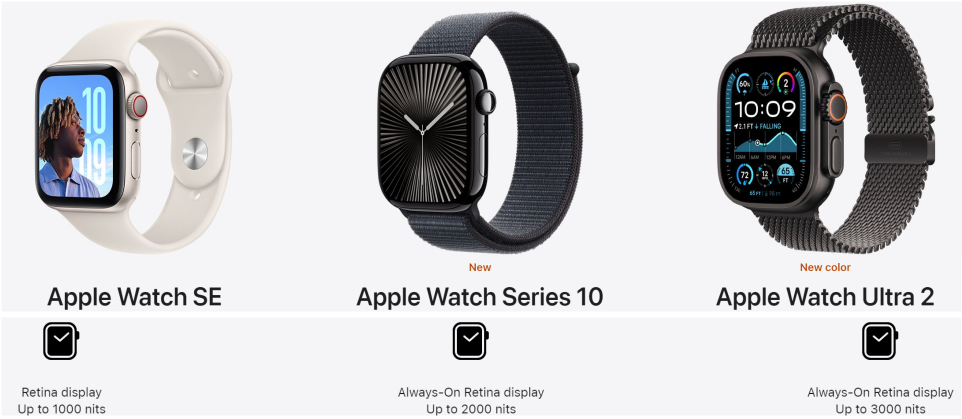
Claim Language	Accused Products
	 MacBook Pro 14-in. (M4) Up to **32GB** unified memory Up to **2TB** storage[3] MacBook Pro 16-in. (M4 Pro Up to **128GB** unified memory Up to **8TB** storage[3] MacBook Air 15-in. (M3) Up to **24GB** unified memory Up to **2TB** storage[3] *See, e.g.*, *Compare Mac models*, Apple, https://www.apple.com/mac/compare/ (last visited Dec. 30, 2024).  **Capacity[1]** 256GB 512GB 1TB *See, e.g.*, *Apple Vision Pro – Tech Specs*, Apple, https://www.apple.com/apple-vision-pro/specs/ (last visited Dec. 30, 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** - *Secure Element:* The Secure Element hosts the payment kernels which read and secure the contactless payment card data. [. . .]

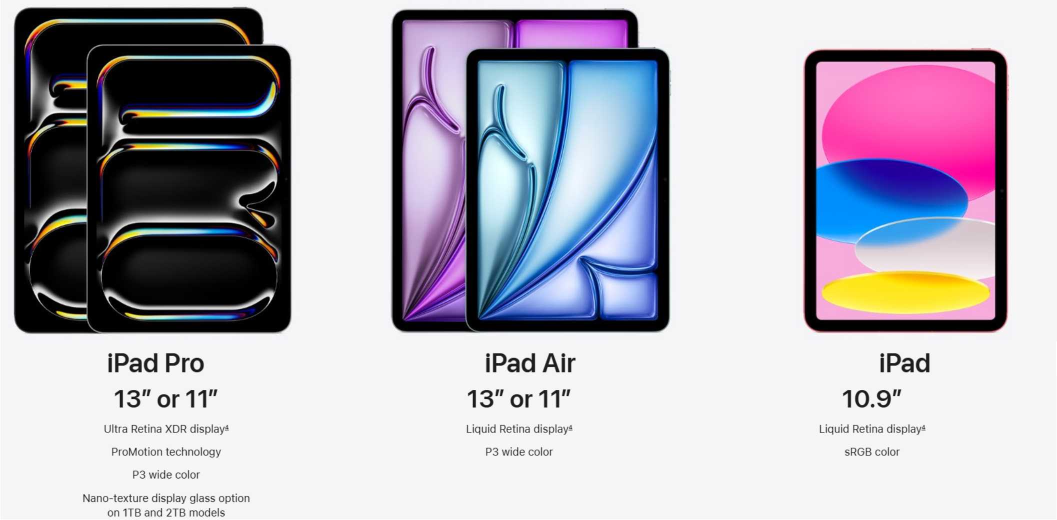
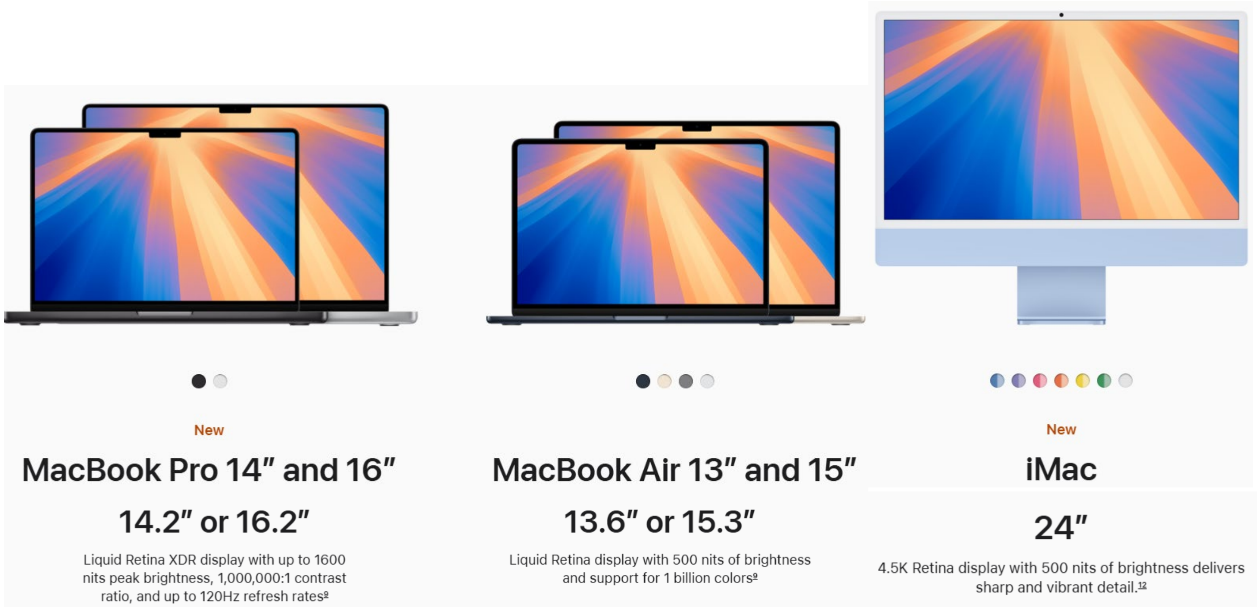
Claim Language	Accused Products
	 **NFC & SE Platform component security** The NFC & SE Platform provides access to hardware and software features that enable developers to provide secure transactions for iPhone users. **Secure Element** The Secure Element is an industry-standard integrated circuit that 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. *See, e.g.*, *Apple Platform Security*, at 178, 196, 260-261 (Dec. 2024), *available at* https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; *see also, e.g.*, Apple Platform Security, *How Apple Pay keeps users' purchases protected*, (Dec. 19, 2024), https://support.apple.com/guide/security/how-apple-pay-keeps-users-purchases-protected-seccb53a35f0/web; Apple Platform Security, *Tap to Pay on iPhone security* (Dec. 19, 2024), https://support.apple.com/guide/security/tap-to-pay-on-iphone-sec72cb155f4/web; Apple Platform Security, *NFC & SE Platform Security* (Dec. 19, 2024), https://support.apple.com/en-mn/guide/security/secda20f3f41/web.
11[e]: a wireless interface;	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—includes a wireless interface (*e.g.*, Wi-Fi, cellular, or NFC interfaces).  **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. [. . .]  9:41 Settings Wi-Fi Edit Wi-Fi ✓ WiFi MY NETWORKS WiFi Secure *See, e.g.*, *Connect to Wi-Fi on your iPhone, iPad, or iPod touch*, Apple (Jun. 28, 2024), https://support.apple.com/en-us/111107.

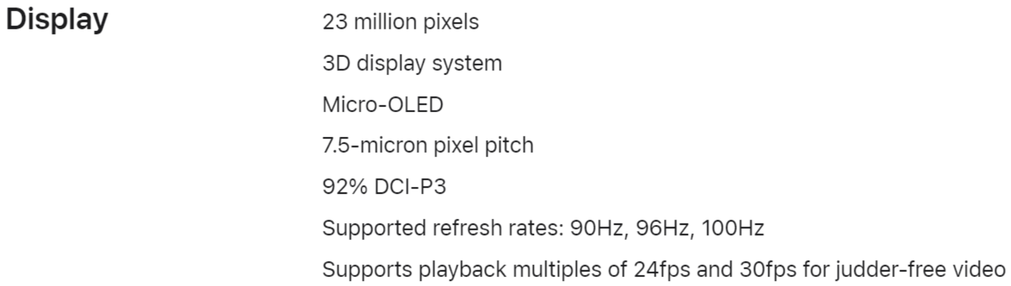
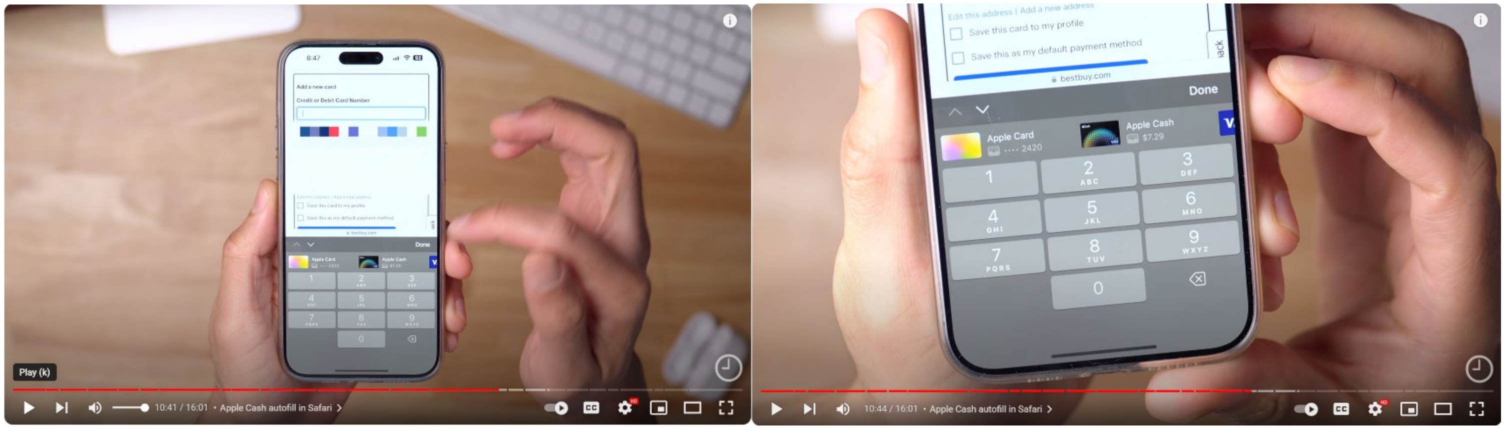
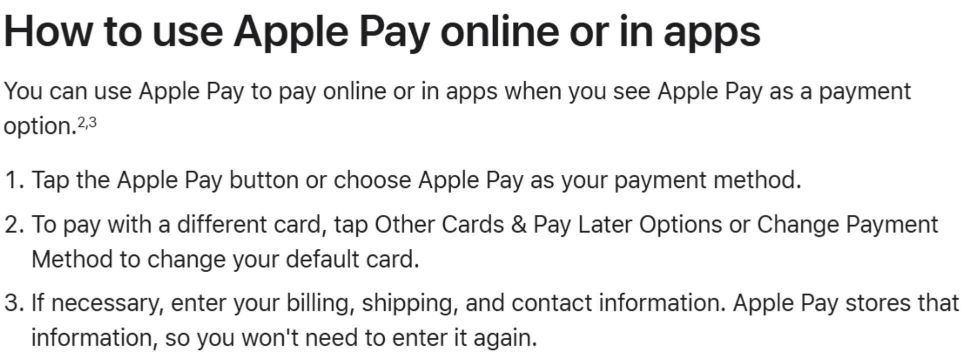
Claim Language	**Accused Products**
	 **Turn cellular data on or off** To turn cellular data on or off, go to Settings, then tap Cellular or Mobile Data. If you're using an iPad, you might see Settings > Cellular Data. Depending on your carrier and device, you might have additional options listed under 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. [. . .]  9:41 Settings Cellular Cellular Find out how much data you're using, set data restrictions, and manage carrier settings such as eSIM and Wi-Fi calling. Learn more... Cellular Data ● Cellular Data Options Roaming Off Personal Hotspot Off Turn off cellular data to restrict all data to Wi-Fi, including email, web browsing, and push notifications. *See, e.g.*, *Use cellular data on your iPhone or iPad*, 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. [. . .]  Wi-Fi 10:09 Wi-Fi ● CHOOSE NETWORK Wi-Fi Network Wi-Fi Secure *See, e.g.*, *Connect your Apple Watch to Wi-Fi*, 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.*, *Set up cellular on Apple Watch*, Apple (Jul. 10, 2024), https://support.apple.com/en-us/119601.

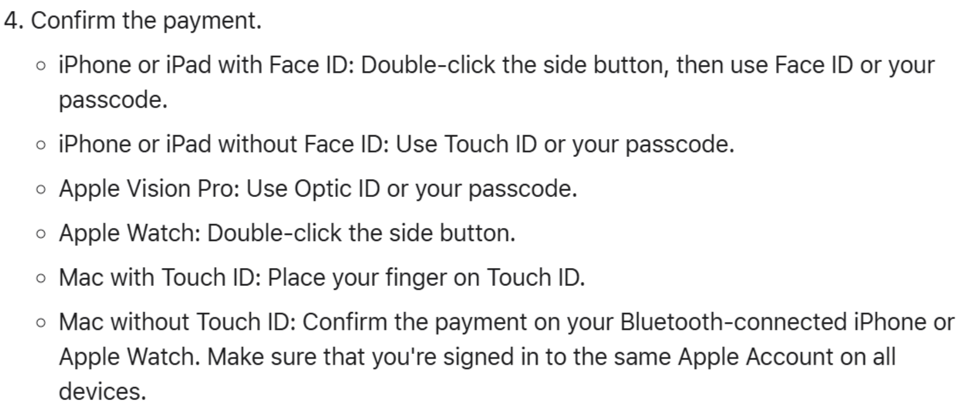
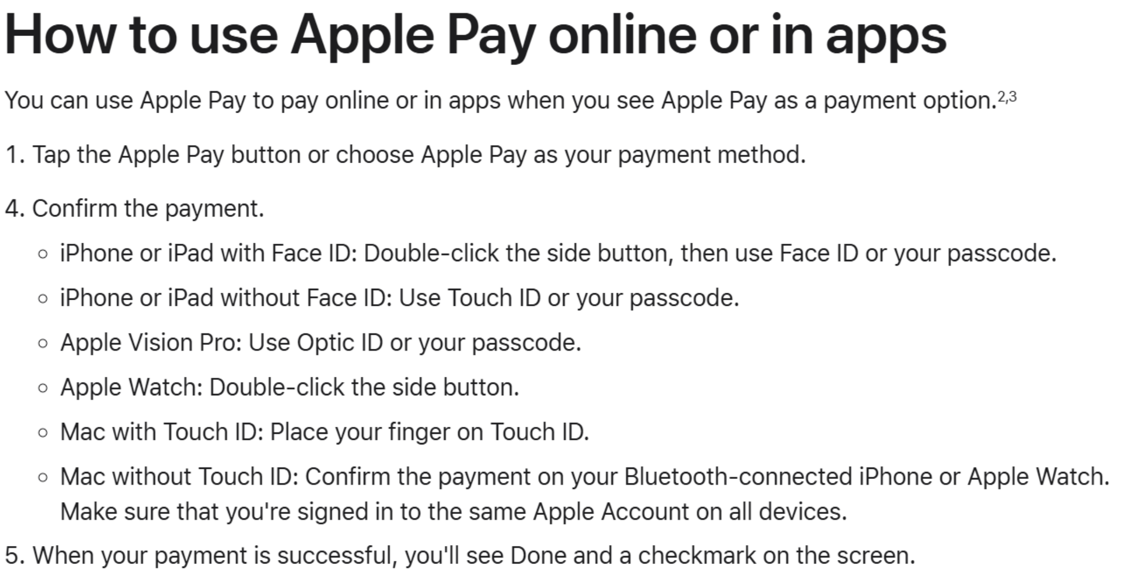
Claim Language	Accused Products
	 **Connect to a Wi-Fi network** From the Wi-Fi menu in the menu bar, choose a network. You might then be asked to enter the Wi-Fi network's password or agree to terms and conditions. Wed Oct 19 9:41 AM Wi-Fi Personal Hotspot John's iPhone 5G Known Network Home Wi-Fi Other Networks Wi-Fi Settings... *See, e.g.*, *Connect to the internet with your Mac*, Apple (Jun. 27, 2024), https://support.apple.com/en-us/101589.  **Connect Apple Vision Pro to a Wi-Fi network** 1. Go to Settings > Wi-Fi, then turn on Wi-Fi. 2. Tap a network, then enter the password (if required). To join a hidden network, tap Other, then enter the name of the network, the security type, and password. If appears at the top of Control Center, Apple Vision Pro is connected to a Wi-Fi network. (To verify this, open Safari to view a webpage.) Apple Vision Pro reconnects when you return to the same location. *See, e.g.*, Apple Vision Pro User Guide, *Connect Apple Vision Pro to the internet*, Apple, https://support.apple.com/guide/apple-vision-pro/connect-apple-vision-pro-to-the-internet-tan75f632320/visionos (last visited Dec. 30, 2024).

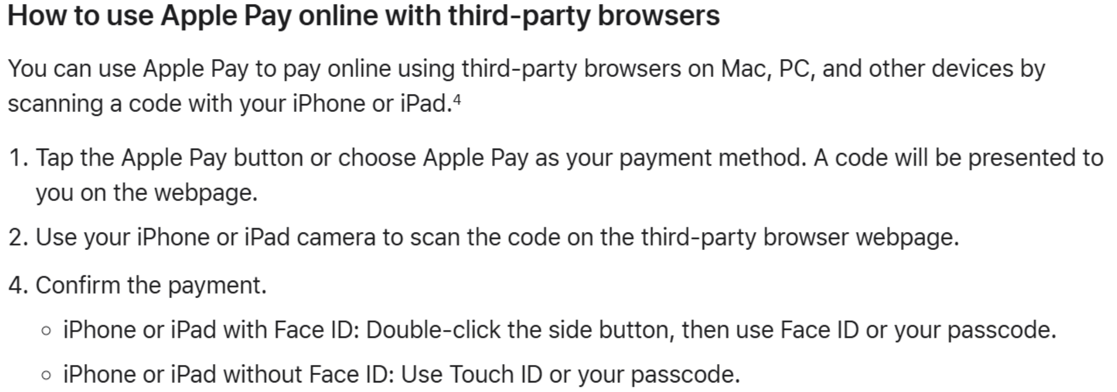
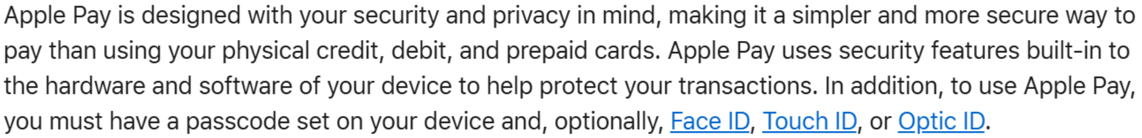
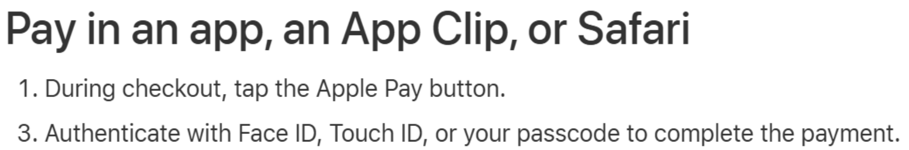
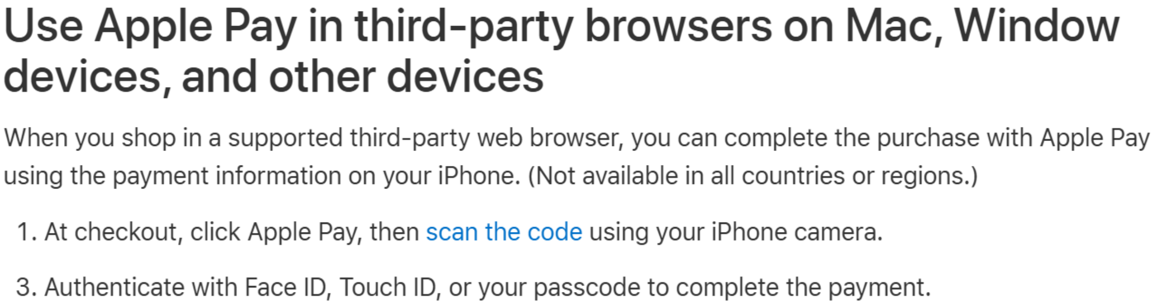
Claim Language	Accused Products
	 **When you use Apple Pay in stores** When you use Apple Pay in stores that accept contactless payments, Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard, contactless technology that's designed 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. *See, e.g.*, *Apple Pay security and privacy overview*, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554.  **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. [. . .]  **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. *See, e.g.*, *Apple Platform Security*, at 177, 196, 260 (Dec. 2024) *available at* https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; *see also, e.g.*, *Apple Pay component security*, Apple (May 13, 2022), https://support.apple.com/guide/security/apple-pay-component-security-sec2561eb018/web; Apple Platform Security, *NFC & SE Platform Security*, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/nfc-se-platform-security-secda20f3f41/web.

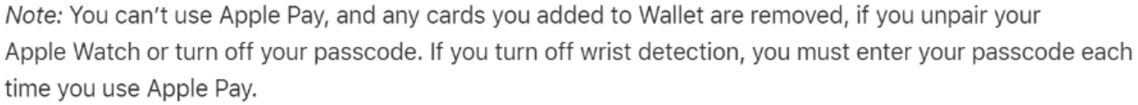
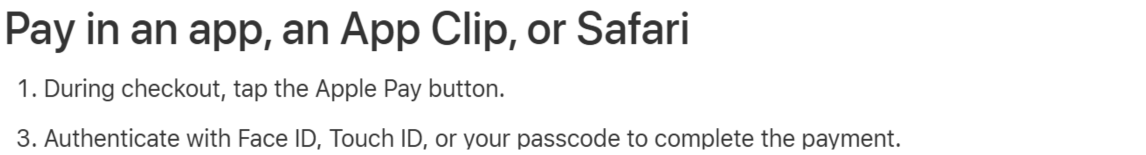
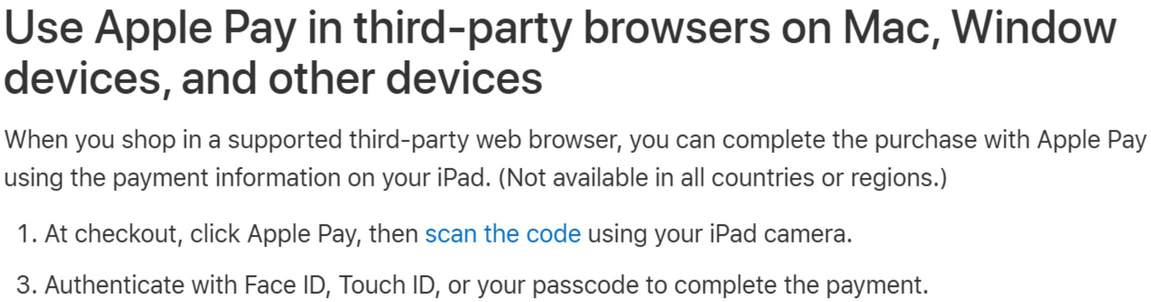
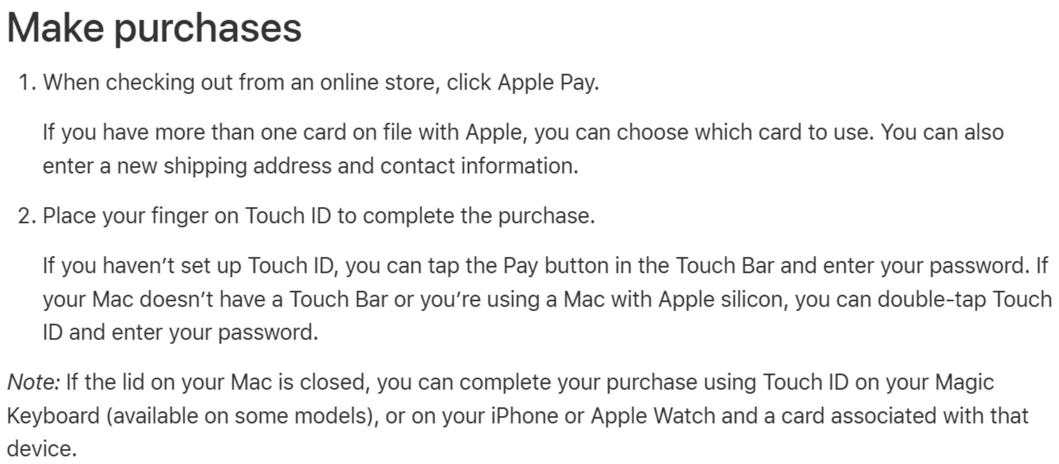
Claim Language	**Accused Products**
11[f]: a display operable to provide a visual user-interface operable for performing online transactions; and	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—includes a display operable to provide a visual user-interface for performing online transactions.  iPhone 16 Pro Max 6.9″ Super Retina XDR display[1] iPhone 16 Pro 6.3″ Super Retina XDR display[1] iPhone 16 6.1″ Super Retina XDR display[1] *See, e.g.*, *Compare iPhone Models*, Apple, https://www.apple.com/iphone/compare/ (last visited Dec. 29, 2024).  Apple Watch SE Retina display Up to 1000 nits New Apple Watch Series 10 Always-On Retina display Up to 2000 nits New color Apple Watch Ultra 2 Always-On Retina display Up to 3000 nits [. . .] *See, e.g.*, *Watch*, Apple, https://www.apple.com/watch/ (last visited Dec. 29, 2024).

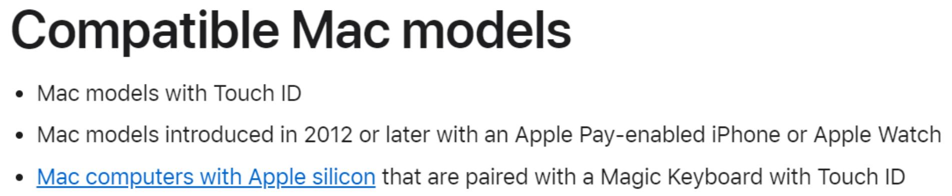
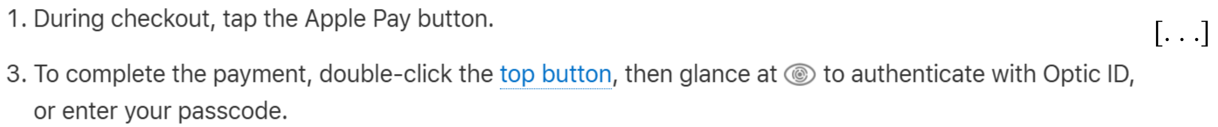
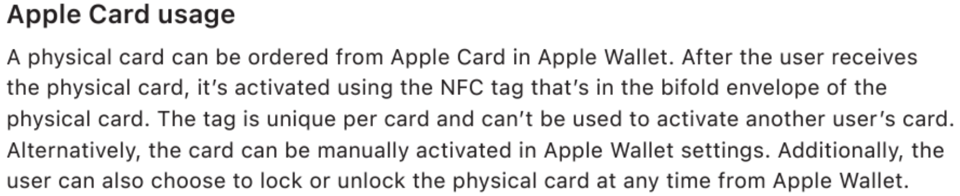
Claim Language	Accused Products
	 iPad Pro 13″ or 11″ Ultra Retina XDR display[4] ProMotion technology P3 wide color Nano-texture display glass option on 1TB and 2TB models iPad Air 13″ or 11″ Liquid Retina display[4] P3 wide color iPad 10.9″ Liquid Retina display[4] sRGB color *See, e.g.*, *iPad*, Apple, https://www.apple.com/ipad/ (last visited Dec. 30, 2024).  New MacBook Pro 14″ and 16″ 14.2″ or 16.2″ Liquid Retina XDR display with up to 1600 nits peak brightness, 1,000,000:1 contrast ratio, and up to 120Hz refresh rates[9] MacBook Air 13″ and 15″ 13.6″ or 15.3″ Liquid Retina display with 500 nits of brightness and support for 1 billion colors[9] New iMac 24″ 4.5K Retina display with 500 nits of brightness delivers sharp and vibrant detail.[12] *See, e.g.*, *Mac*, Apple, https://www.apple.com/mac/ (last visited Dec. 30, 2024). To the extent that Mac desktop models paired with a display do 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.*, providing a display that is functionally coupled to the device).

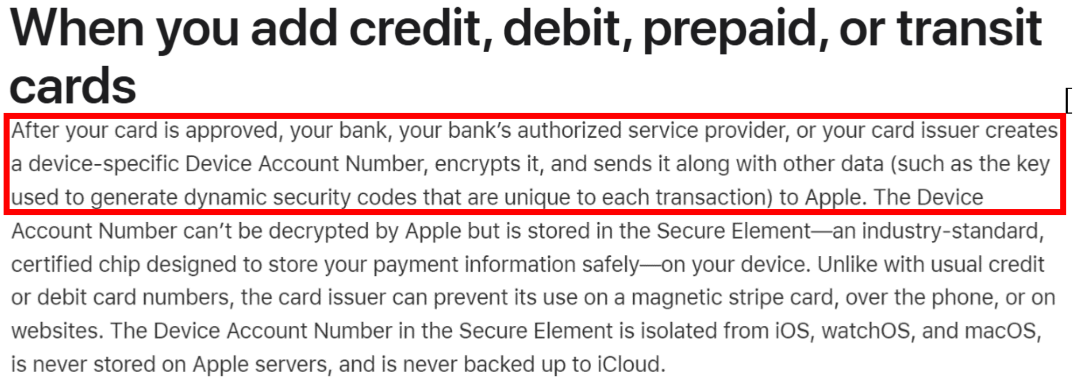
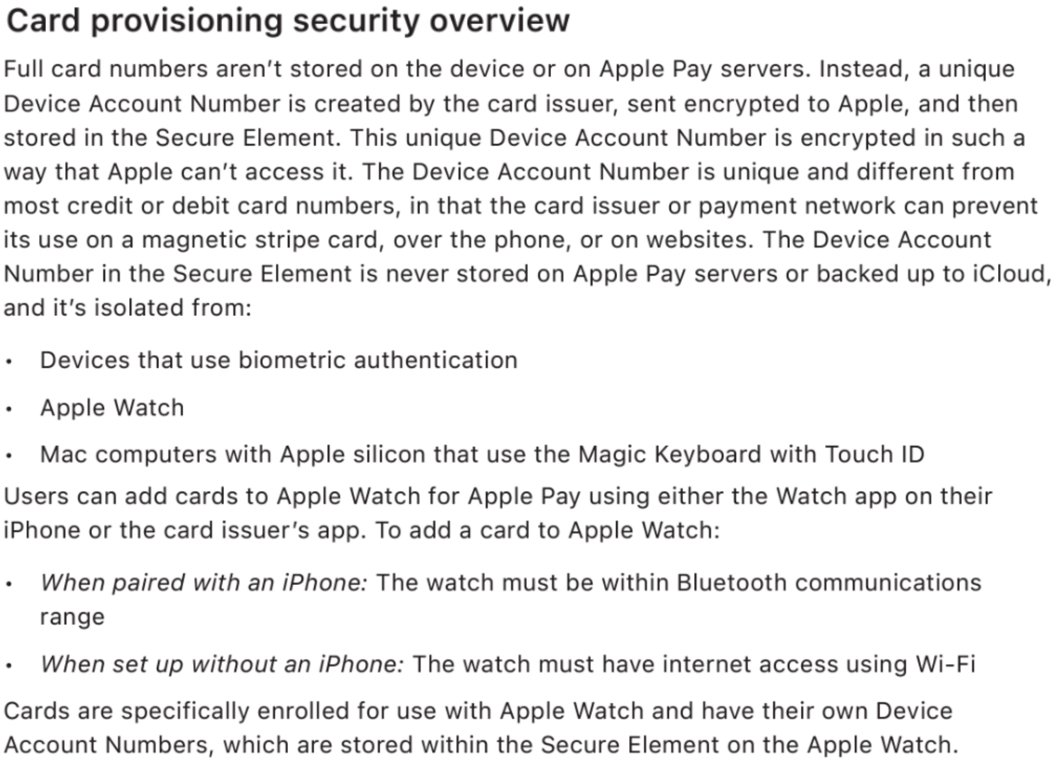
Claim Language	Accused Products
	 **Display** 23 million pixels 3D display system Micro-OLED 7.5-micron pixel pitch 92% DCI-P3 Supported refresh rates: 90Hz, 96Hz, 100Hz Supports playback multiples of 24fps and 30fps for judder-free video *See, e.g.*, *Apple Vision Pro – Tech Specs*, Apple, https://www.apple.com/apple-vision-pro/specs/ (last visited Dec. 30, 2024).  Add a new card Credit or Debit Card Number Save this card to my profile Save this as my default payment method bestbuy.com Done Apple Card •••• 2420 Apple Cash $7.29 Play (k) 10:41 / 16:01 • Apple Cash autofill in Safari 10:44 / 16:01 • Apple Cash autofill in Safari *See, e.g.*, 9to5Mac, *iOS 17.4 – 30+ New Changes and Features*, YouTube (Feb. 28, 2024), https://www.youtube.com/watch?v=wT5osIMpyuQ&t=635s.  **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.

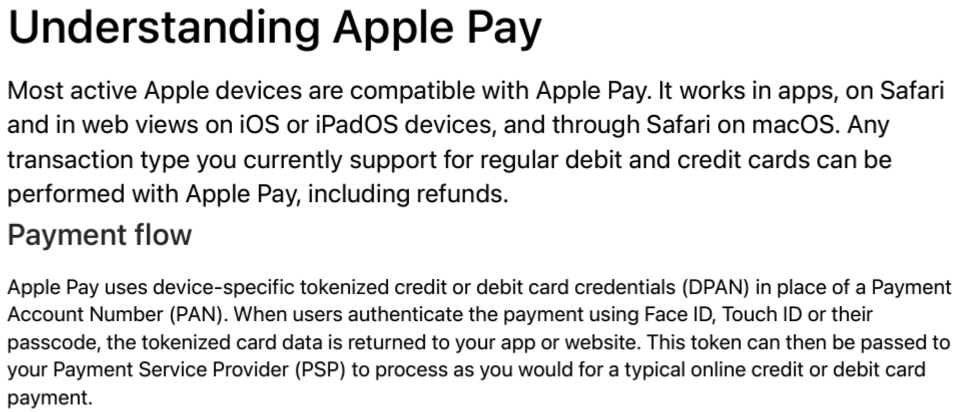
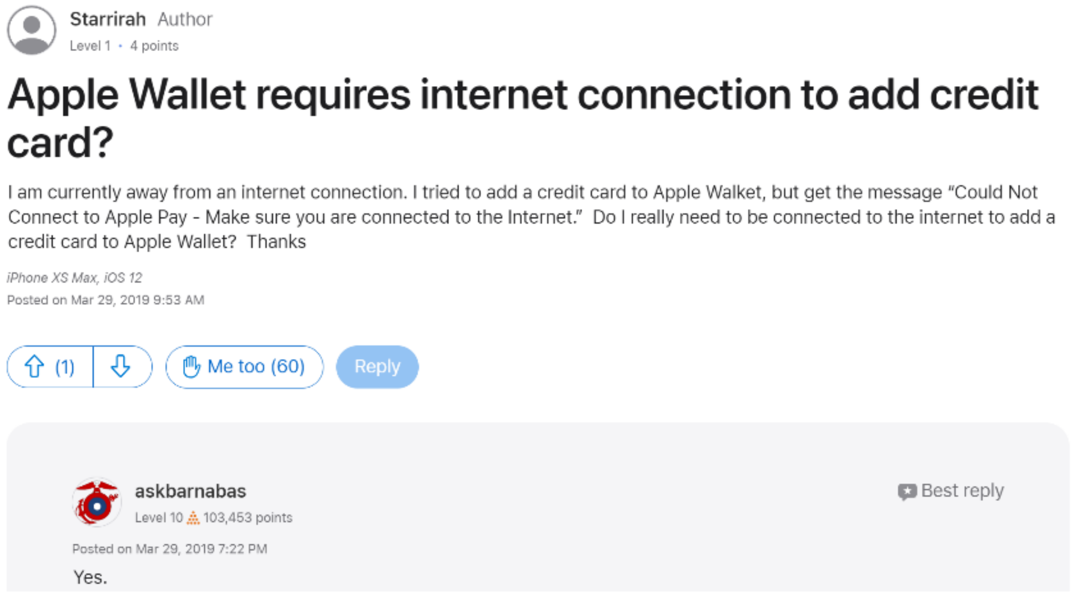
Claim Language	Accused Products
	 4. Confirm the payment. ○ iPhone or iPad with Face ID: Double-click the side button, then use Face ID or your passcode. ○ iPhone or iPad without Face ID: Use Touch ID or your passcode. ○ Apple Vision Pro: Use Optic ID or your passcode. ○ Apple Watch: Double-click the side button. ○ Mac with Touch ID: Place your finger on Touch ID. ○ 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.*, *Make purchases using Apple Pay*, Apple (Sept. 24, 2024), https://support.apple.com/en-us/102626; Apple Vision Pro User Guide, *Use Apple Pay in apps and Safari on Apple Vision Pro*, Apple, https://support.apple.com/guide/apple-vision-pro/use-apple-pay-in-apps-and-safari-tanf3cf449bb/1.0/visionos/1.0.
11[g]: a user-interface coupled to the processor, and	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—includes a user-interface (*e.g.*, side button, biometric sensors (*e.g.*, for Face ID, Touch ID, Optic ID, wrist detection), touch screen panel, keyboard) coupled to the processor.  **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. [. . .] 4. Confirm the payment. ○ iPhone or iPad with Face ID: Double-click the side button, then use Face ID or your passcode. ○ iPhone or iPad without Face ID: Use Touch ID or your passcode. ○ Apple Vision Pro: Use Optic ID or your passcode. ○ Apple Watch: Double-click the side button. ○ Mac with Touch ID: Place your finger on Touch ID. ○ 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.

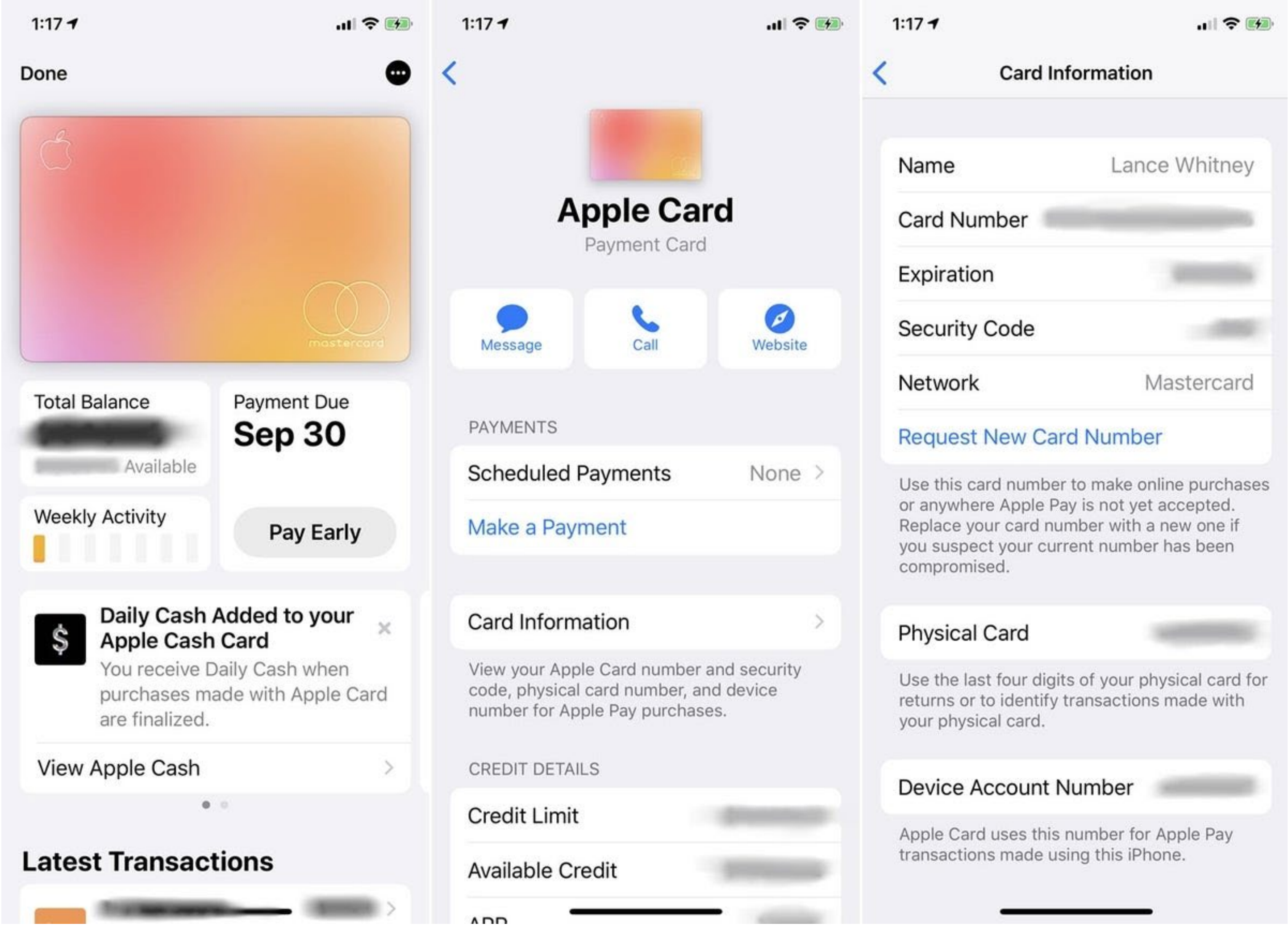
Claim Language	Accused Products
	 **How to use Apple Pay online with third-party browsers** You can use Apple Pay to pay online using third-party browsers on Mac, PC, and other devices by scanning a code with your iPhone or iPad.[4] 1. Tap the Apple Pay button or choose Apple Pay as your payment method. A code will be presented to you on the webpage. 2. Use your iPhone or iPad camera to scan the code on the third-party browser webpage. [. . .] 4. Confirm the payment. ○ iPhone or iPad with Face ID: Double-click the side button, then use Face ID or your passcode. ○ iPhone or iPad without Face ID: Use Touch ID or your passcode. *See, e.g.*, *Make purchases using Apple Pay*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102626.  Apple Pay is designed with your security and privacy in mind, making it a simpler and more secure way to pay than using your physical credit, debit, and prepaid cards. Apple Pay uses security features built-in to the hardware and software of your device to help protect your transactions. In addition, to use Apple Pay, you must have a passcode set on your device and, optionally, Face ID, Touch ID, or Optic ID. *See, e.g.*, *Apple Pay security and privacy overview*, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554.  **Pay in an app, an App Clip, or Safari** 1. During checkout, tap the Apple Pay button. [. . .] 3. Authenticate with Face ID, Touch ID, or your passcode to complete the payment.  **Use Apple Pay in third-party browsers on Mac, Window devices, and other devices** When you shop in a supported third-party web browser, you can complete the purchase with Apple Pay using the payment information on your iPhone. (Not available in all countries or regions.) 1. At checkout, click Apple Pay, then scan the code using your iPhone camera. [. . .] 3. Authenticate with Face ID, Touch ID, or your passcode to complete the payment. *See, e.g.*, iPhone User Guide – iOS 18, *Use Apple Pay in apps and on the web on iPhone*, Apple, https://support.apple.com/guide/iphone/use-apple-pay-in-apps-and-on-the-web-iph67e89f7c8/ios (last visited Dec. 30, 2024).

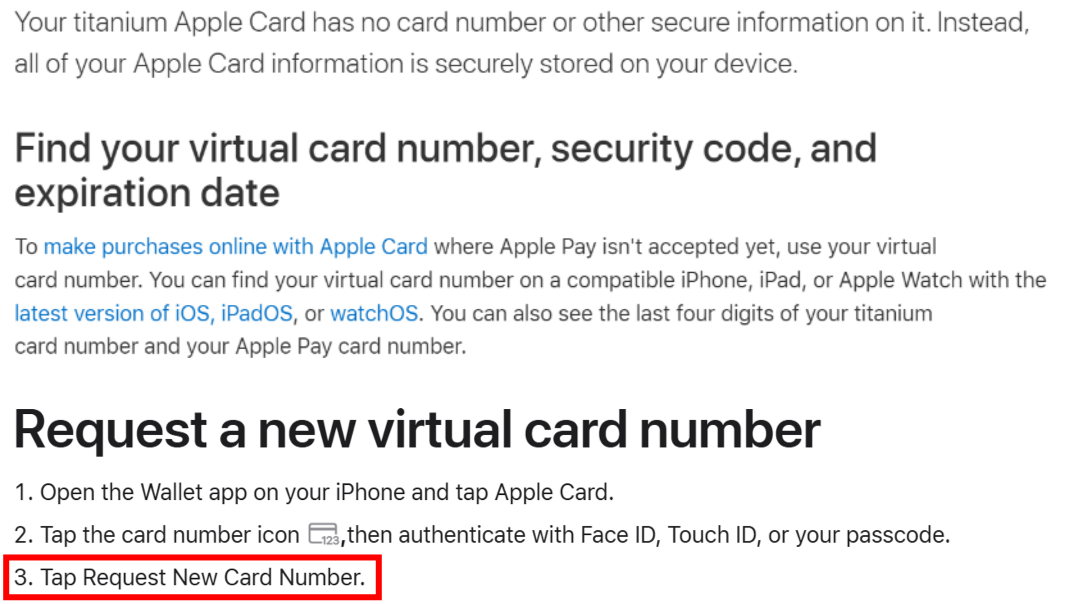
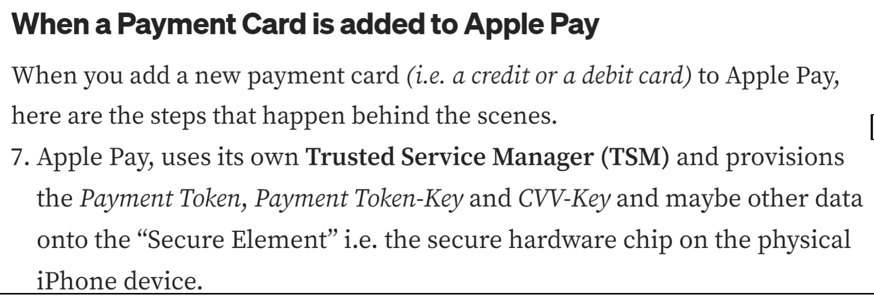
Claim Language	Accused Products
	 *Note:* You can't use Apple Pay, and any cards you added to Wallet are removed, if you unpair your Apple Watch or turn off your passcode. If you turn off wrist detection, you must enter your passcode each time you use Apple Pay. *See, e.g.*, Apple Watch User Guide – watchOS 11, *Apple Pay on Apple Watch*, Apple, https://support.apple.com/guide/watch/apple-pay-apd76424826d/watchos (last visited Dec. 30, 2024).  **Pay in an app, an App Clip, or Safari** 1. During checkout, tap the Apple Pay button. [. . .] 3. Authenticate with Face ID, Touch ID, or your passcode to complete the payment.  **Use Apple Pay in third-party browsers on Mac, Window devices, and other devices** When you shop in a supported third-party web browser, you can complete the purchase with Apple Pay using the payment information on your iPad. (Not available in all countries or regions.) 1. At checkout, click Apple Pay, then scan the code using your iPad camera. [. . .] 3. Authenticate with Face ID, Touch ID, or your passcode to complete the payment. *See, e.g.*, iPad User Guide – iPadOS 18, *Use Apple Pay in apps and on the web on iPad*, Apple, https://support.apple.com/guide/ipad/use-apple-pay-in-apps-and-on-the-web-ipad049d8c12/ipados (last visited Dec. 2, 2024).  **Make purchases** 1. When checking out from an online store, click Apple Pay. If you have more than one card on file with Apple, you can choose which card to use. You can also enter a new shipping address and contact information. 2. Place your finger on Touch ID to complete the purchase. If you haven't set up Touch ID, you can tap the Pay button in the Touch Bar and enter your password. If your Mac doesn't have a Touch Bar or you're using a Mac with Apple silicon, you can double-tap Touch ID and enter your password. *Note:* If the lid on your Mac is closed, you can complete your purchase using Touch ID on your Magic Keyboard (available on some models), or on your iPhone or Apple Watch and a card associated with that device. *See, e.g.*, Mac User Guide – macOS Sequoia 15, *Use Wallet & Apple Pay on Mac*, Apple, https://support.apple.com/guide/mac-help/use-wallet-apple-pay-on-mac-mchl4773988b/mac (last visited Dec. 2, 2024).

Claim Language	Accused Products
	 **Compatible Mac models** • Mac models with Touch ID • Mac models introduced in 2012 or later with an Apple Pay-enabled iPhone or Apple Watch • Mac computers with Apple silicon that are paired with a Magic Keyboard with Touch ID *See, e.g.*, Devices compatible with Apple Pay, Apple (Nov. 22, 2024), https://support.apple.com/en-us/102896; iMac – 2024- macOS Sequoia 15, *Magic Keyboard*, Apple, https://support.apple.com/guide/imac/magic-keyboard-apd0e7983e19/mac (last visited Dec. 30, 2024). To the extent that Mac models without Touch ID that are paired with an Apple Pay-enabled iPhone or Apple Watch or Mac models with Apple silicon that are paired with a Magic Keyboard with Touch ID do 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.*, providing a user interface that is functionally coupled to the device).  1. During checkout, tap the Apple Pay button. [. . .] 3. To complete the payment, double-click the top button, then glance at ◎ to authenticate with Optic ID, or enter your passcode. *See, e.g.*, Apple Vision Pro User Guide, *Use Apple Pay in apps and Safari on Apple Vision Pro*, Apple, https://support.apple.com/guide/apple-vision-pro/use-apple-pay-in-apps-and-safari-tanf3cf449bb/1.0/visionos/1.0 (last visited Dec. 2, 2024).
11[h]: wherein the wireless interface is operable to wirelessly obtain card device payment account information, and	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop computer, desktop computer, or spatial computer—includes a wireless interface (e.g., Wi-Fi, cellular, or NFC) that is operable to wirelessly obtain card device payment account information (*e.g.*, a device-specific tokenized credit or debit card credentials/ payment token/ Device Account Number ("DAN"), and associated expiration date and keys, last four digits of a physical card number, payment network, security code, expiration date, credit details, and, on information and belief, an Apple Card virtual account number ("VAN") and associated expiration date, security code). *See supra* limitation 11[e].  **Apple Card usage** A physical card can be ordered from Apple Card in Apple Wallet. After the user receives the physical card, it's activated using the NFC tag that's in the bifold envelope of the physical card. The tag is unique per card and can't be used to activate another user's card. Alternatively, the card can be manually activated in Apple Wallet settings. Additionally, the user can also choose to lock or unlock the physical card at any time from Apple Wallet. *See, e.g.*, *Apple Platform Security*, at 192 (Dec. 2024) *available at* https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; *see, e.g.*, Apple Platform Security, *Apple Card security*, Apple (May 7, 2024), https://support.apple.com/guide/security/apple-card-security-secb29b74e98/web.

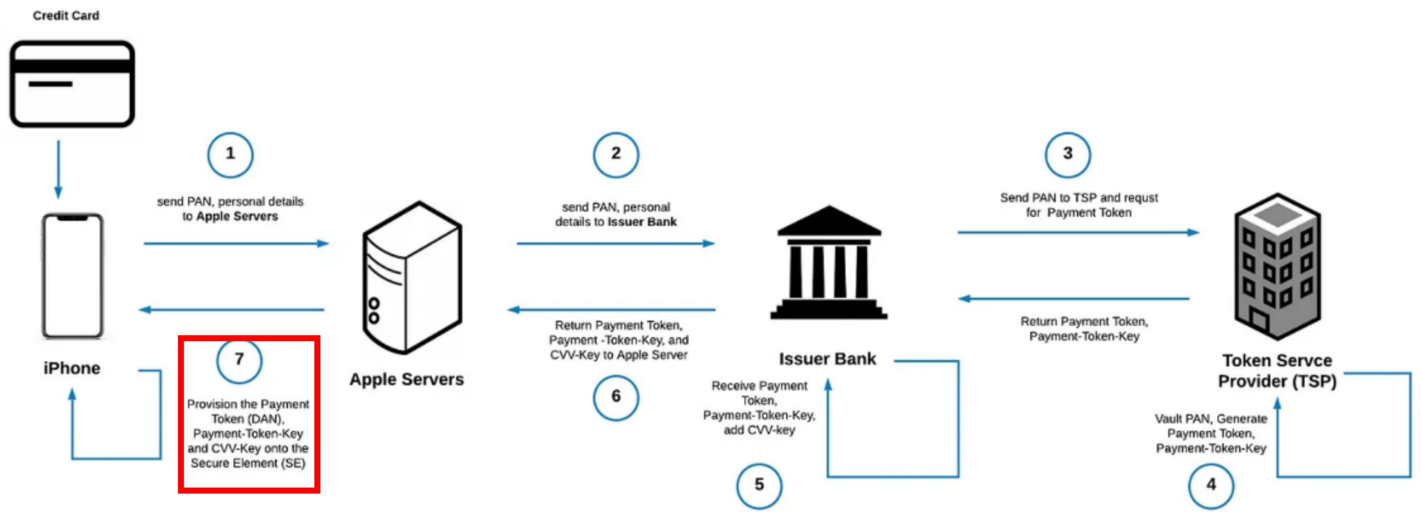
Claim Language	Accused Products
	 **When you add credit, debit, prepaid, or transit cards** [. . .] After your card is approved, your bank, your bank's authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such 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. *See, e.g.*, *Apple Pay security and privacy overview*, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554.  **Card provisioning security overview** Full card numbers aren't stored on the device or on Apple Pay servers. Instead, a unique Device Account Number is created by the card issuer, sent encrypted to Apple, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from most credit or debit card numbers, in that the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is never stored on Apple Pay servers or backed up to iCloud, and it's isolated from: • Devices that use biometric authentication • Apple Watch • Mac computers with Apple silicon that use the Magic Keyboard with Touch ID 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: • *When paired with an iPhone:* The watch must be within Bluetooth communications range • *When set up without an iPhone:* 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. *See, e.g.*, *Apple Platform Security*, at 179 (Dec. 2024) *available at* https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; *see also, e.g.*, Apple Platform Security, *Card provisioning security overview*, Apple (May 7, 2024), https://support.apple.com/en-gb/guide/security/sec0f005981a/web.

Claim Language	Accused Products
	 **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. **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, *Apple Pay Merchant Integration Guide* at 5 (Jan. 2024) *available at* https://developer.apple.com/apple-pay/Apple-Pay-Merchant-Integration-Guide.pdf.  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 Best reply Level 10 103,453 points Posted on Mar 29, 2019 7:22 PM Yes. *See, e.g.*, Starriah, *Apple Wallet requires internet connection to add credit card?*, Apple Support Community (Mar. 29, 2019), https://discussions.apple.com/thread/250267325?sortBy=best.

Claim Language	Accused Products
	 1:17 Done Total Balance [redacted] [redacted] Available Payment Due Sep 30 Weekly Activity Pay Early Daily Cash Added to your Apple Cash Card You receive Daily Cash when purchases made with Apple Card are finalized. View Apple Cash Latest Transactions [redacted] 1:17 Apple Card Payment Card Message Call Website PAYMENTS Scheduled Payments None Make a Payment Card Information View your Apple Card number and security code, physical card number, and device number for Apple Pay purchases. CREDIT DETAILS Credit Limit [redacted] Available Credit [redacted] APR 1:17 Card Information Name Lance Whitney Card Number [redacted] Expiration [redacted] Security Code [redacted] Network Mastercard Request New Card Number Use this card number to make online purchases or anywhere Apple Pay is not yet accepted. Replace your card number with a new one if you suspect your current number has been compromised. Physical Card [redacted] Use the last four digits of your physical card for returns or to identify transactions made with your physical card. Device Account Number [redacted] Apple Card uses this number for Apple Pay transactions made using this iPhone. *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; *see, e.g.*, Lance Whitney, *How to use your Apple Card without Apple Pay*, TechRepublic (Oct. 1, 2019), https://www.techrepublic.com/article/how-to-use-your-apple-card-without-apple-pay/.

Claim Language	Accused Products
	 Your titanium Apple Card has no card number or other secure information on it. Instead, all of your Apple Card information is securely stored on your device. **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. **Request a new virtual card number** 1. Open the Wallet app on your iPhone and tap Apple Card. 2. Tap the card number icon 123,then authenticate with Face ID, Touch ID, or your passcode. 3. Tap Request New Card Number. *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.  **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. [. . .] 7. Apple Pay, uses its own **Trusted Service Manager (TSM)** and provisions the *Payment Token*, *Payment Token-Key* and *CVV-Key* and maybe other data onto the "Secure Element" i.e. the secure hardware chip on the physical iPhone device.

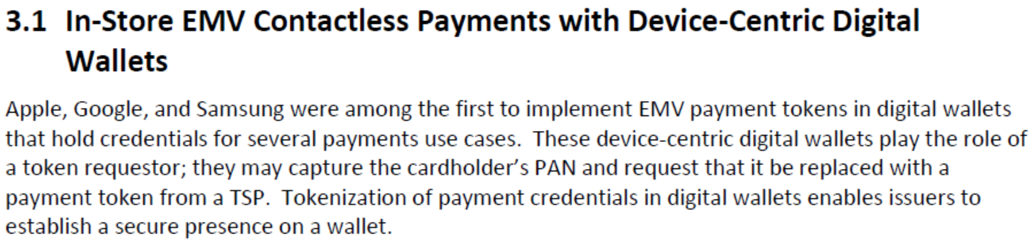
<table>
<tr><th>Claim Language</th><th>Accused Products</th></tr>
<tr><td></td><td>



Credit Card
1
send PAN, personal details to Apple Servers
2
send PAN, personal details to Issuer Bank
3
Send PAN to TSP and requst for Payment Token
iPhone
Apple Servers
Issuer Bank
Token Servce Provider (TSP)
Return Payment Token, Payment -Token-Key, and CVV-Key to Apple Server
Return Payment Token, Payment-Token-Key
7
Provision the Payment Token (DAN), Payment-Token-Key and CVV-Key onto the Secure Element (SE)
6
Receive Payment Token, Payment-Token-Key, add CVV-key
5
Vault PAN, Generate Payment Token, Payment-Token-Key
4

When a Payment Card is Added to the Apple Pay Wallet

See, e.g., Prashant Ram, *How Apple Pay works under the hood?*, codeburst (Nov. 5, 2019), https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7.

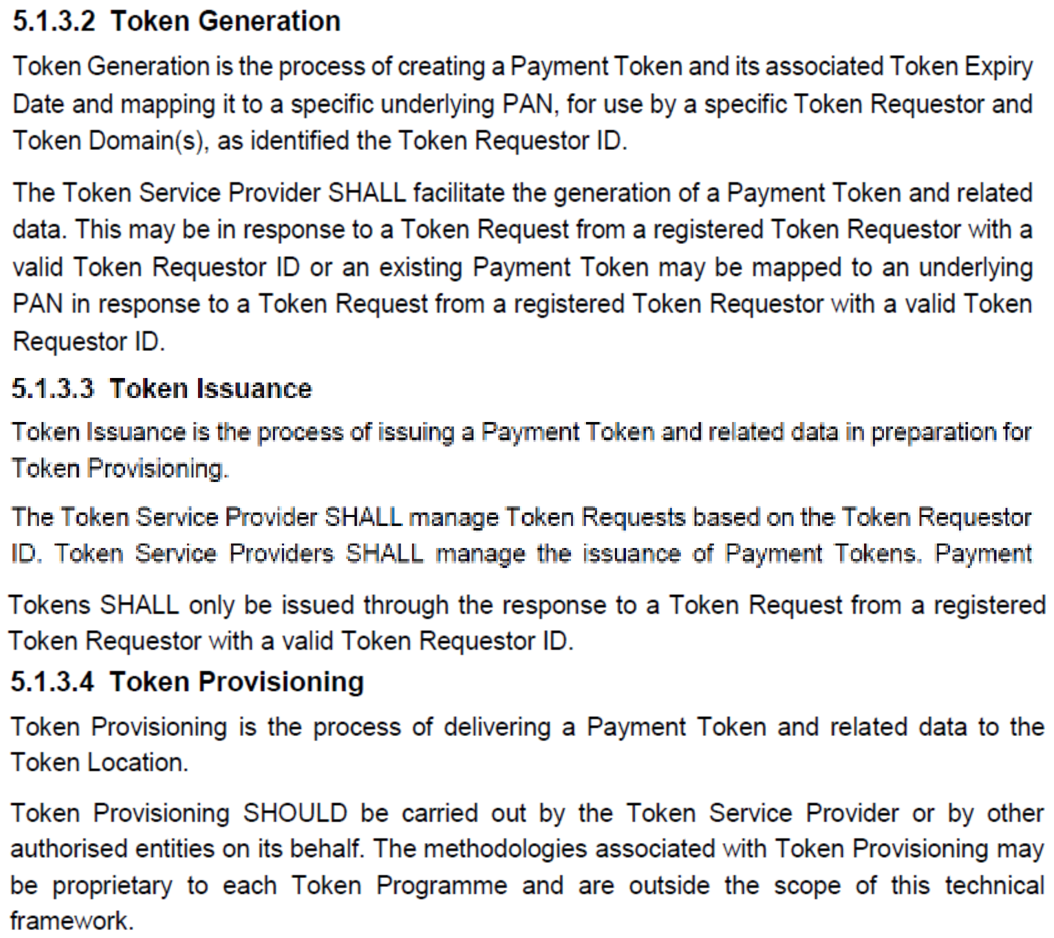
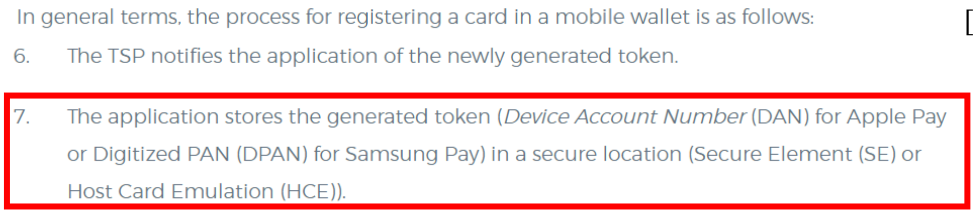


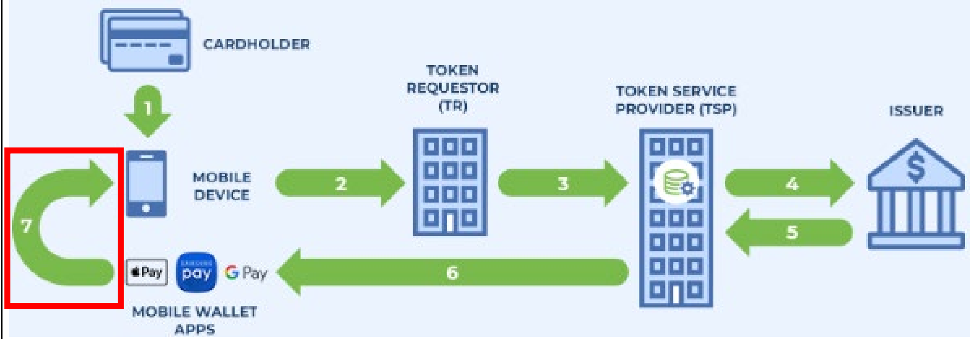
3.1 In-Store EMV Contactless Payments with Device-Centric Digital Wallets

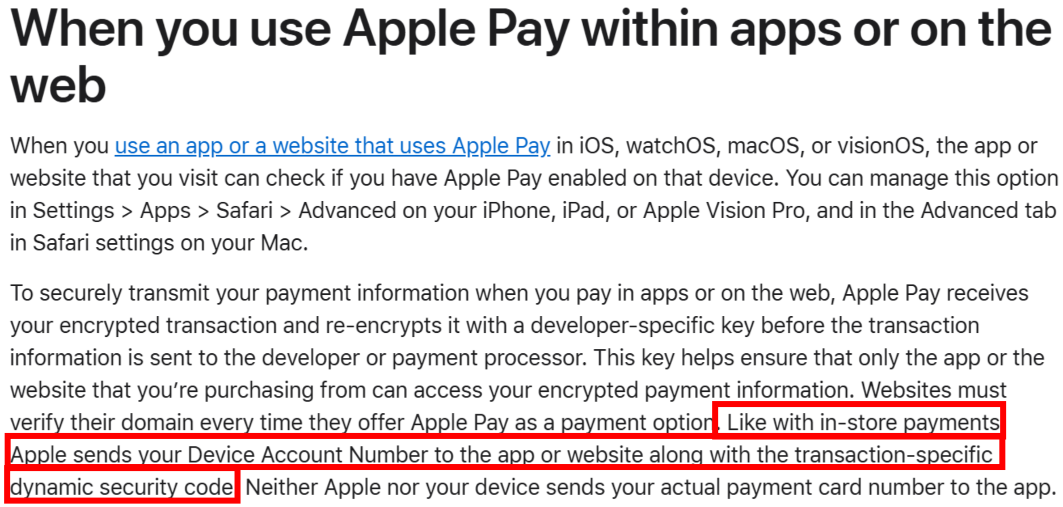
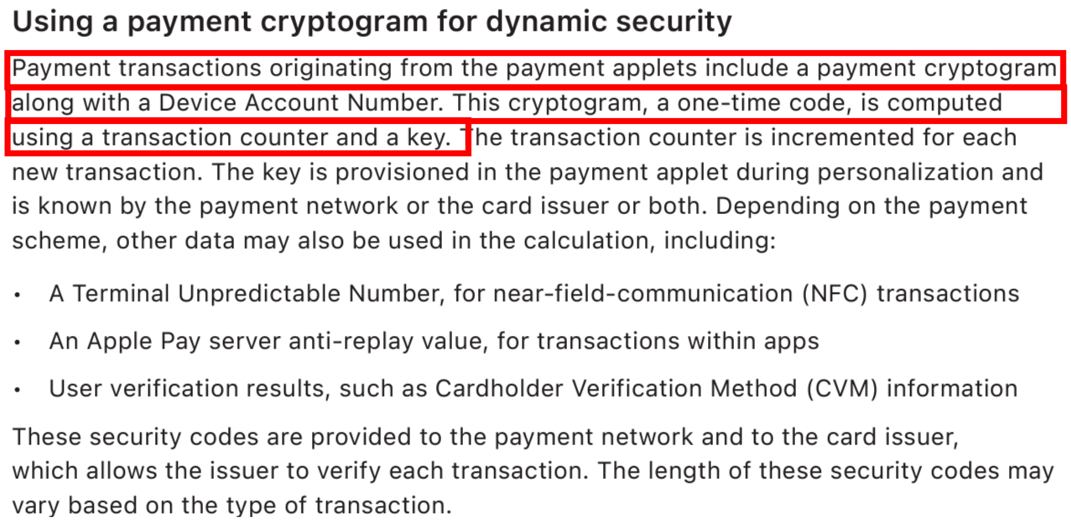
Apple, Google, and Samsung were among the first to implement EMV payment tokens in digital wallets that hold credentials for several payments use cases. These device-centric digital wallets play the role of a token requestor; they may capture the cardholder's PAN and request that it be replaced with a payment token from a TSP. Tokenization of payment credentials in digital wallets enables issuers to establish a secure presence on a wallet.

US Payments Forum, *EMV Payment Tokenization Primer and Lessons Learned* at 12 (June 2019), *available at* https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.

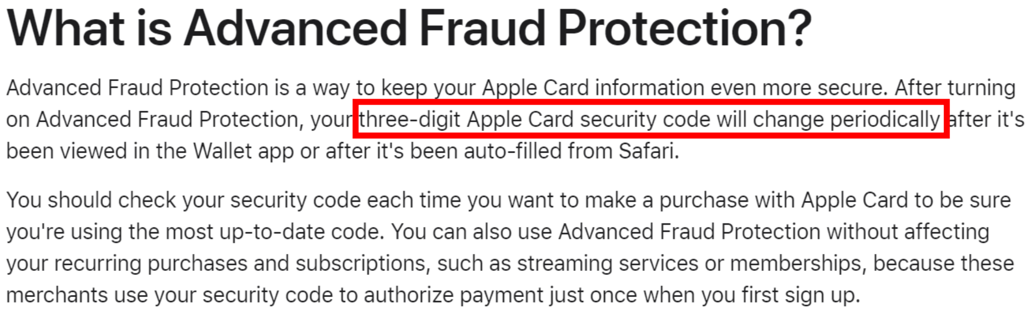
</td></tr>
</table>

Claim Language	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. *See, e.g.*, EMVCo, EMV® Payment Tokenisation Specification – Technical Framework v2.1 at 35–36 (Jun. 14, 2019).  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 (*Device Account Number* (DAN) for Apple Pay or Digitized PAN (DPAN) for Samsung Pay) in a secure location (Secure Element (SE) or Host Card Emulation (HCE)).

Claim Language	**Accused Products**
	 CARDHOLDER 1 TOKEN REQUESTOR (TR) TOKEN SERVICE PROVIDER (TSP) ISSUER 7 MOBILE DEVICE 2 3 4 5 6 Pay pay G Pay MOBILE WALLET APPS *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).
11[i]: wherein the processor is operable to generate limited-use payment information based on the card device payment account information, and	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop computer, desktop computer, or spatial computer—includes a processor that is operable to generate limited-use payment information (*e.g.*, a unique transaction code/ transaction-specific dynamic security code/ payment cryptogram/ dynamic cryptogram ("dynamic cryptogram") or a dynamic security code/ rotating Apple Card security code/ dynamic card verification value ("dynamic security code"), or any combination of the same with, *e.g.*, the DAN or , on information and belief, the VAN) based on the card device payment account information (*e.g.*, the DAN, or associated expiration date and keys, or, on information and belief, the VAN or associated expiration date and keys). For example, the dynamic cryptogram is generated based on the DAN or a key associated with the DAN (*e.g.*, a payment token key). The dynamic security code is generated using at least a key associated with, on information or belief, a DAN or VAN (*e.g.*, a CVV-key).

Claim Language	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, macOS, or visionOS, the app or website that you visit can check if you have Apple Pay enabled on that device. You can manage this option in Settings > Apps > Safari > Advanced on your iPhone, iPad, or Apple Vision Pro, and in the Advanced tab in Safari settings 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.*, *Apple Pay security and privacy overview*, 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.*, *Apple Platform Security*, at 183 (Dec. 2024) *available at* https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; *see also, e.g.*, Apple Platform Security, *Payment authorization with Apple Pay*, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/payment-authorization-with-apple-pay-secc1f57e189/web.

Claim Language	Accused Products

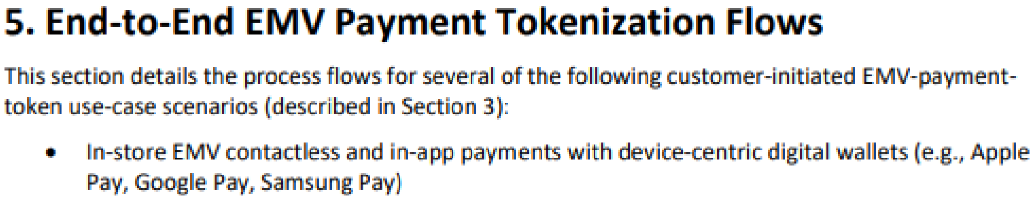


What is Advanced Fraud Protection?

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., *Use Advanced Fraud Protection with Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102427.

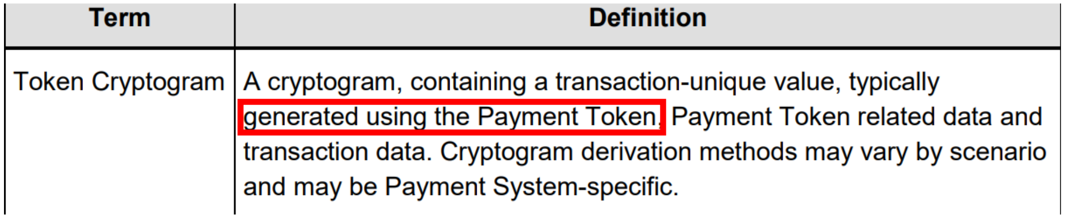


5. End-to-End EMV Payment Tokenization Flows

This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):

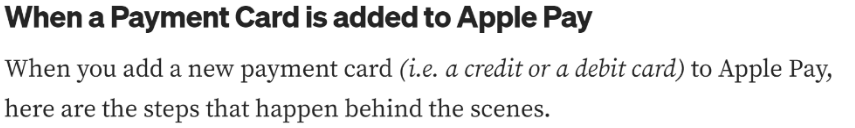
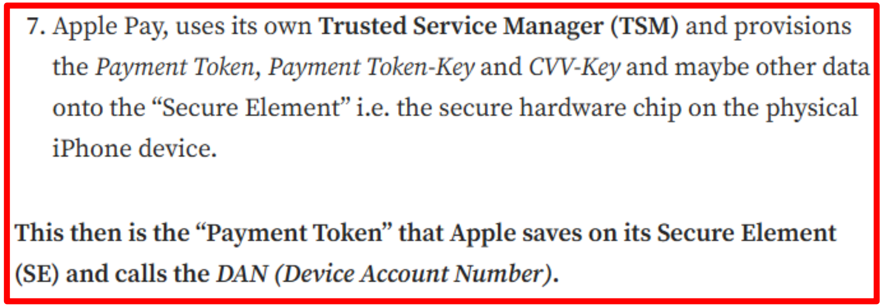
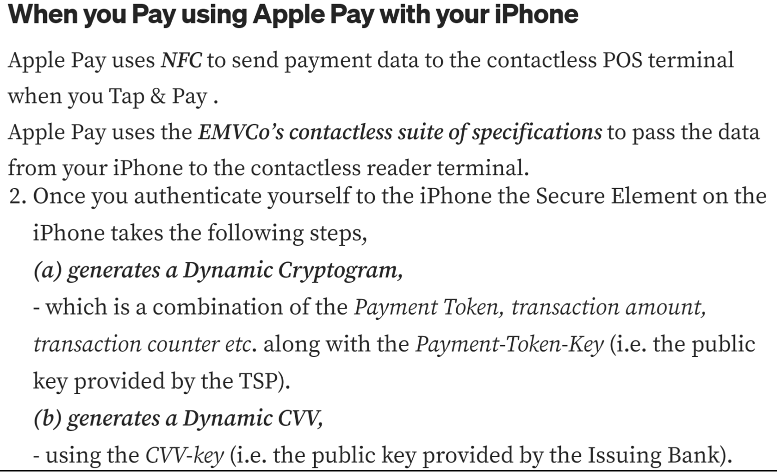
- In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)

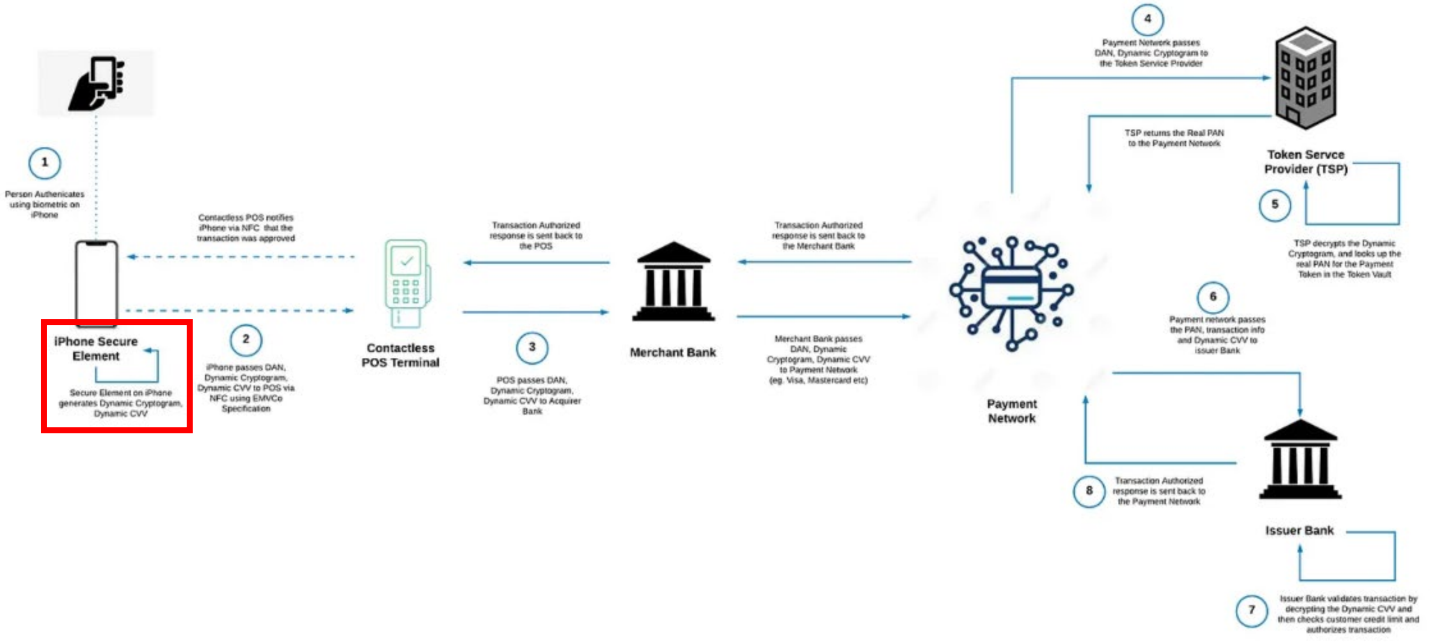
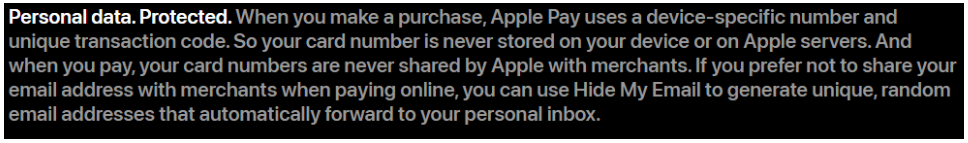
See, e.g., US Payments Forum, *EMV Payment Tokenization Primer and Lessons Learned* at 12, 23 (June 2019) *available at* https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.

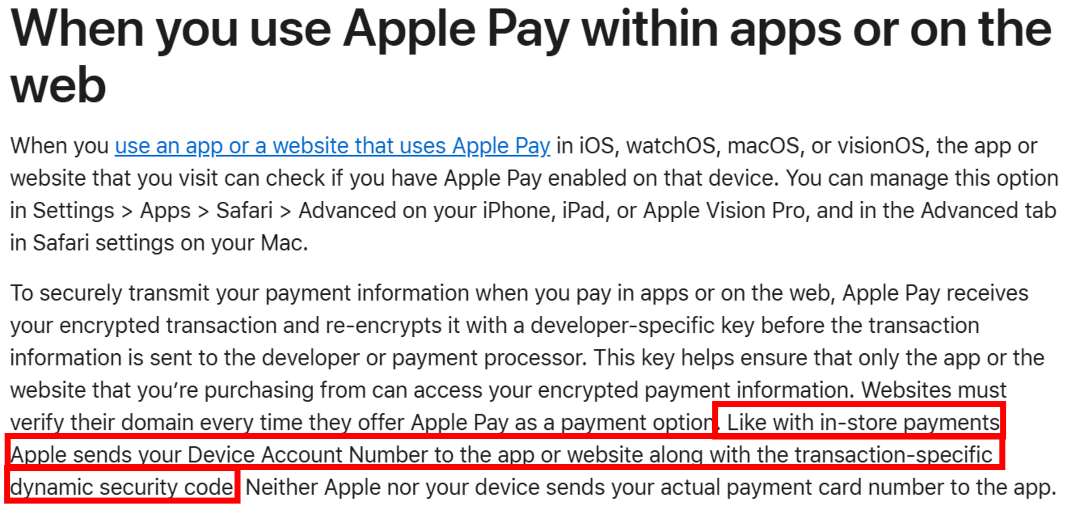
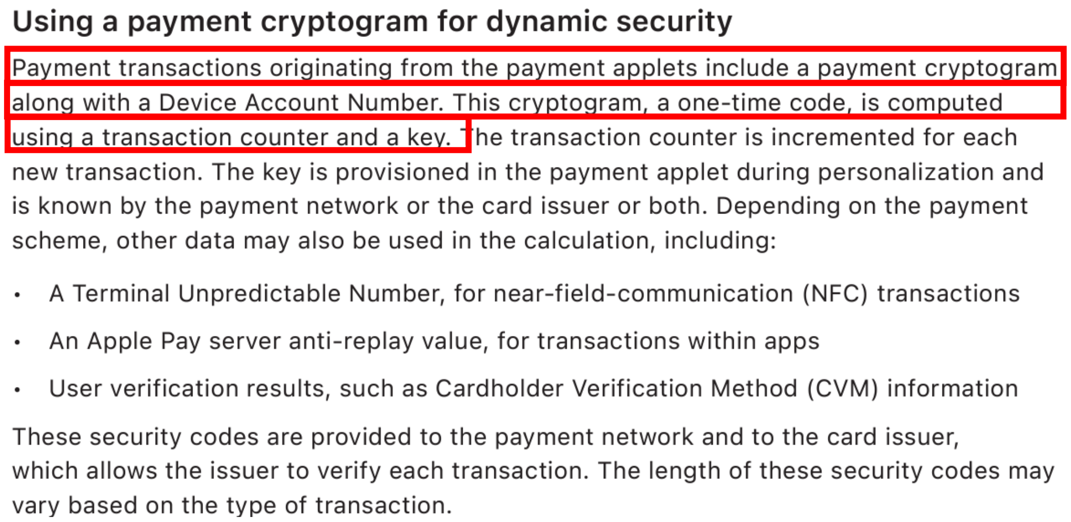


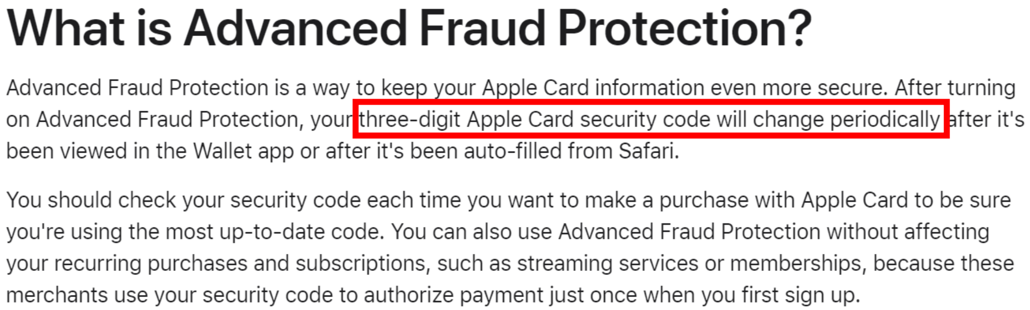
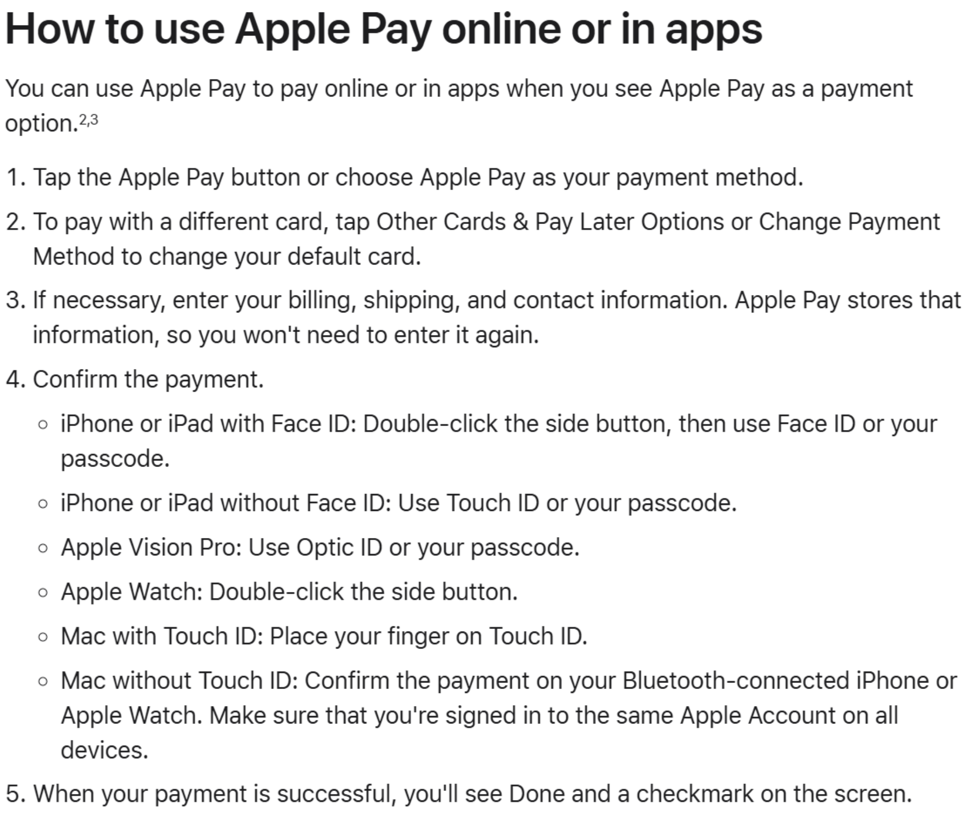
Term	Definition
Token Cryptogram	A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.

See, e.g., EMVCo, *EMV® Payment Tokenisation Specification – Technical Framework v2.1* at 10 (Jun. 14, 2019).

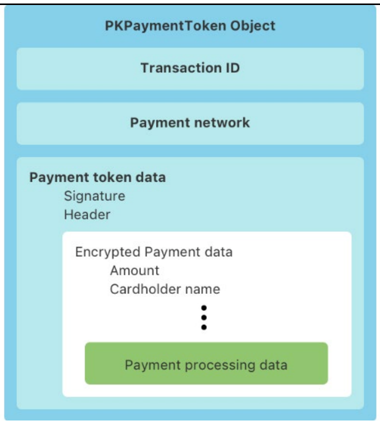
Claim Language	Accused Products
	 **When a Payment Card is added to Apple Pay** When you add a new payment card *(i.e. a credit or a debit card)* to Apple Pay, here are the steps that happen behind the scenes. [. . .]  7. Apple Pay, uses its own **Trusted Service Manager (TSM)** and provisions the *Payment Token*, *Payment Token-Key* and *CVV-Key* 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 *DAN (Device Account Number)*.**  **When you Pay using Apple Pay with your iPhone** Apple Pay uses *NFC* to send payment data to the contactless POS terminal when you Tap & Pay . Apple Pay uses the ***EMVCo's contactless suite of specifications*** 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) generates a Dynamic Cryptogram,* - which is a combination of the *Payment Token, transaction amount, transaction counter etc*. along with the *Payment-Token-Key* (i.e. the public key provided by the TSP). *(b) generates a Dynamic CVV,* - using the *CVV-key* (i.e. the public key provided by the Issuing Bank).

Claim Language	Accused Products
	 1 Person Authenicates using biometric on iPhone iPhone Secure Element Secure Element on iPhone generates Dynamic Cryptogram, Dynamic CVV 2 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 Contactless POS Terminal 3 POS passes DAN, Dynamic Cryptogram, Dynamic CVV to Acquirer Bank Transaction Authorized response is sent back to the POS Merchant Bank Merchant Bank passes DAN, Dynamic Cryptogram, Dynamic CVV to Payment Network (eg. Visa, Mastercard etc) Transaction Authorized response is sent back to the Merchant Bank Payment Network 4 Payment Network passes DAN, Dynamic Cryptogram to the Token Service Provider TSP returns the Real PAN to the Payment Network Token Servce Provider (TSP) 5 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 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 When you Pay using Apple Pay with your iPhone *See, e.g.*, Prashant Ram, *How Apple Pay works under the hood?*, codeburst (Nov. 5, 2019), https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7.
11[j]: wherein the personal computing device is operable to generate complete payment information, including the limited-use payment information, and to convey said complete payment information via at least one interface of a set comprising: said display; and the wireless interface, and	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—is operable to generate complete payment information (*e.g.*, the dynamic cryptogram, the dynamic security code, or any combination of the same with, *e.g.*, the DAN or the VAN), including the limited-use payment information (*e.g.*, the dynamic cryptogram or the dynamic security code), and to convey said complete payment information via at least one interface of a set comprising: said display (*e.g.*, shown in a browser); and the wireless interface (*e.g.*, Wi-Fi or cellular interface).  **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.*, *Apple Pay*, Apple, https://www.apple.com/apple-pay/ (last visited Dec. 30, 2024).

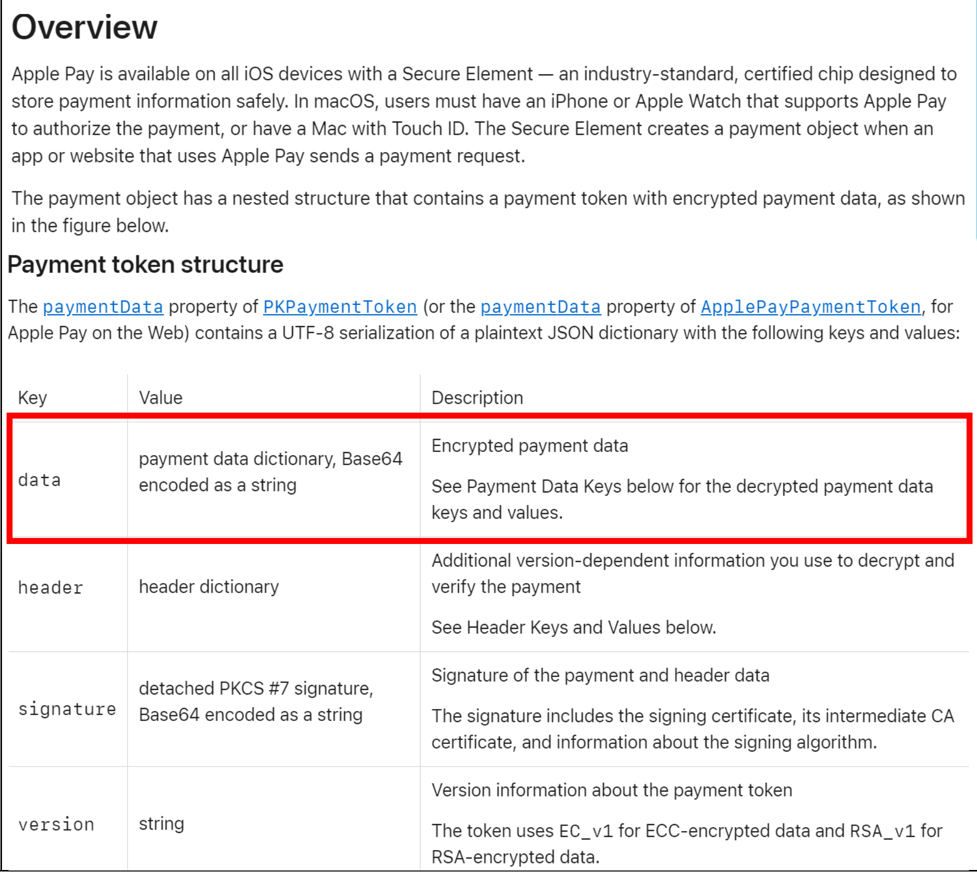
Claim Language	Accused Products
	 **When you use Apple Pay within apps or on the web** When you use an app or a website that uses Apple Pay in iOS, watchOS, macOS, or visionOS, the app or website that you visit can check if you have Apple Pay enabled on that device. You can manage this option in Settings > Apps > Safari > Advanced on your iPhone, iPad, or Apple Vision Pro, and in the Advanced tab in Safari settings 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.*, *Apple Pay security and privacy overview*, 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.*, *Apple Platform Security*, at 183 (Dec. 2024) *available at* https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; *see also, e.g.*, Apple Platform Security, *Payment authorization with Apple Pay*, Apple (Dec. 19, 2024), https://support.apple.com/guide/security/payment-authorization-with-apple-pay-secc1f57e189/web.

Claim Language	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.*, *Use Advanced Fraud Protection with Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102427.  **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. ○ iPhone or iPad with Face ID: Double-click the side button, then use Face ID or your passcode. ○ iPhone or iPad without Face ID: Use Touch ID or your passcode. ○ Apple Vision Pro: Use Optic ID or your passcode. ○ Apple Watch: Double-click the side button. ○ Mac with Touch ID: Place your finger on Touch ID. ○ 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.*, *Make purchases using Apple Pay*, Apple (Sept. 24, 2024), https://support.apple.com/en-us/102626; Apple Vision Pro User Guide, *Use Apple Pay in apps and Safari on Apple Vision Pro*, Apple, https://support.apple.com/guide/apple-vision-pro/use-apple-pay-in-apps-and-safari-tanf3cf449bb/1.0/visionos/1.0.

Claim Language	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.

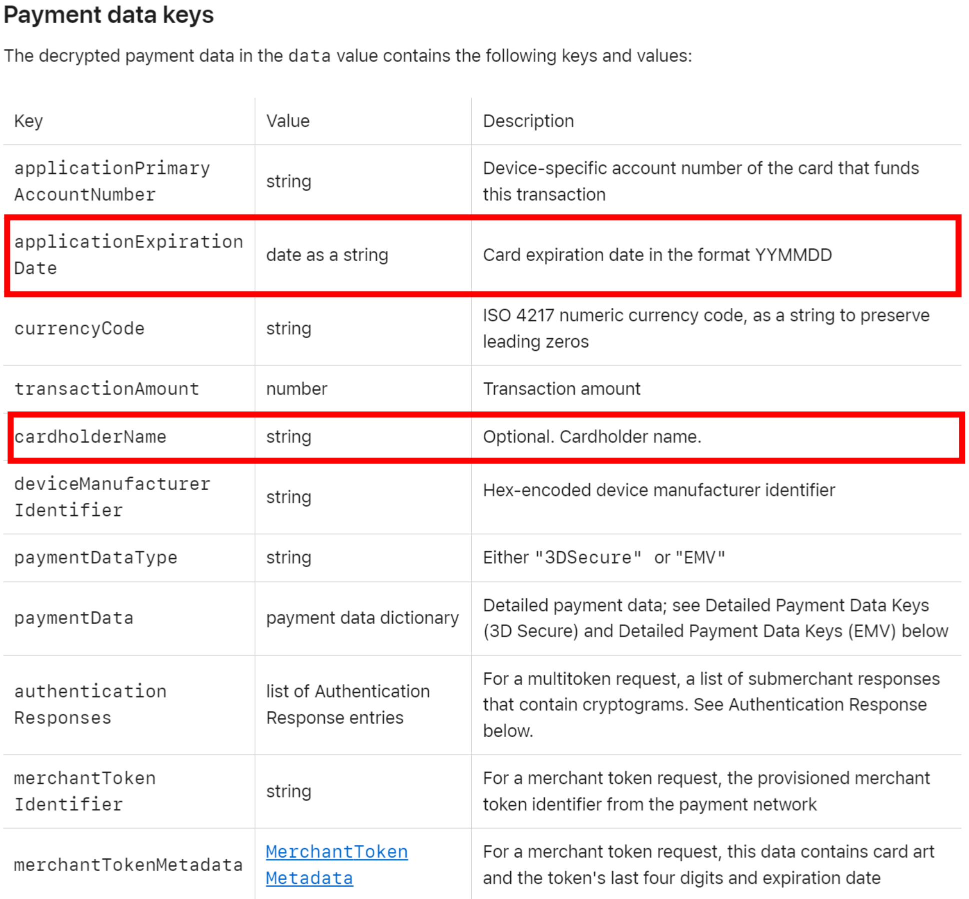
The payment object has a nested structure that contains a payment token with encrypted payment data, as shown in the figure below.

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
`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.
`header`	header dictionary	Additional version-dependent information you use to decrypt and verify the payment See Header Keys and Values below.
`signature`	detached PKCS #7 signature, Base64 encoded as a string	Signature of the payment and header data The signature includes the signing certificate, its intermediate CA certificate, and information about the signing algorithm.
`version`	string	Version information about the payment token The token uses `EC_v1` for ECC-encrypted data and `RSA_v1` for RSA-encrypted data.

Claim Language	Accused Products
	See screenshot and citation below

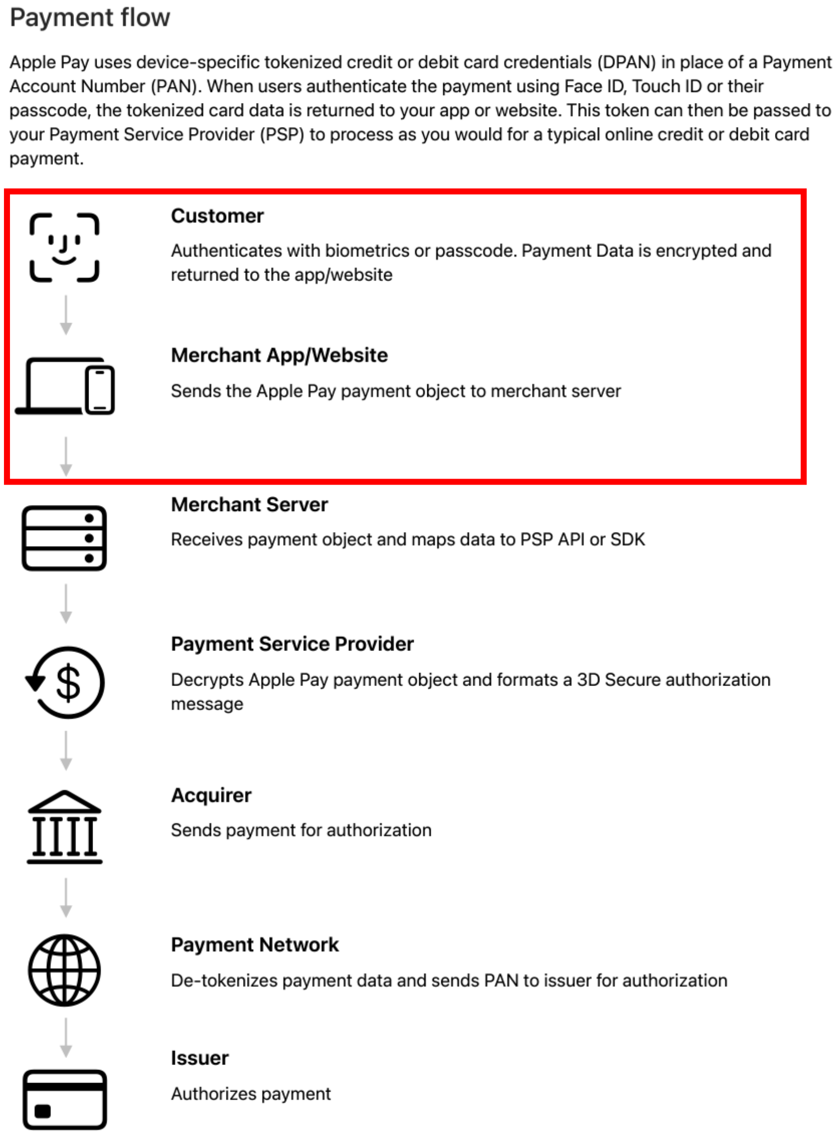


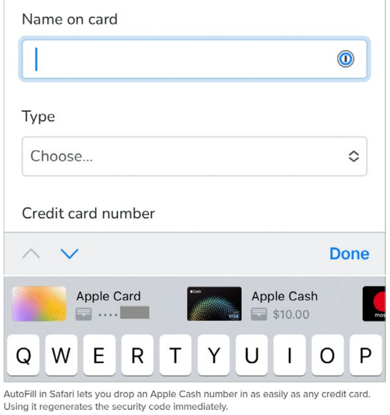
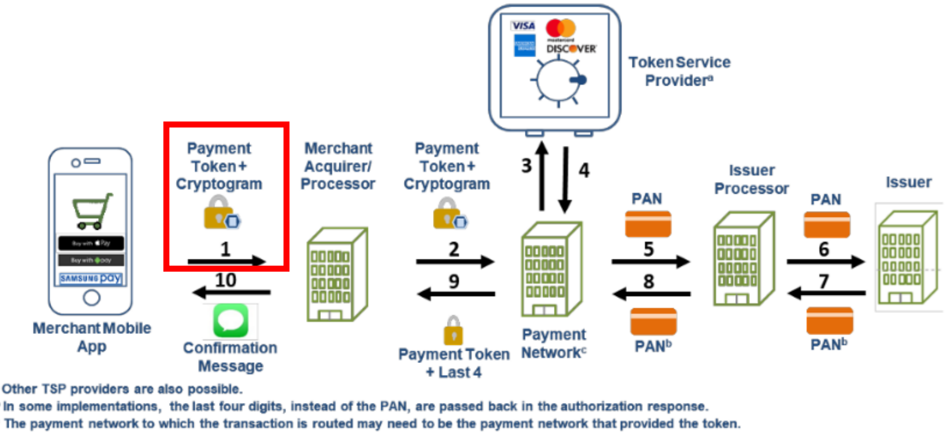
Payment data keys

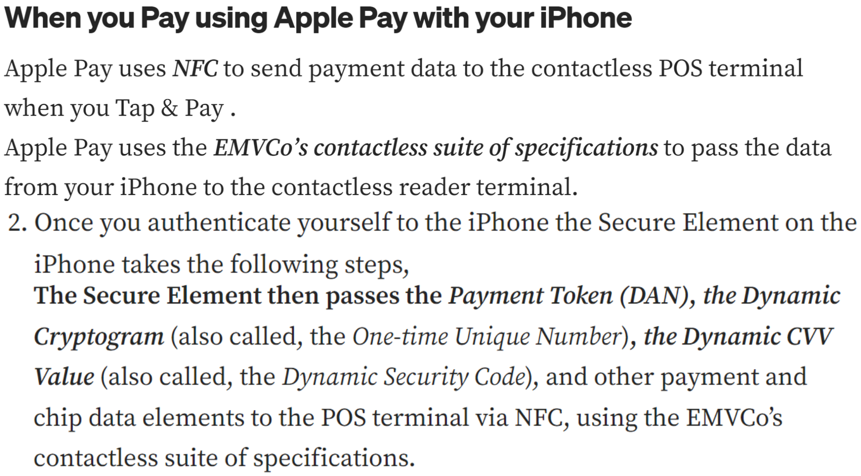
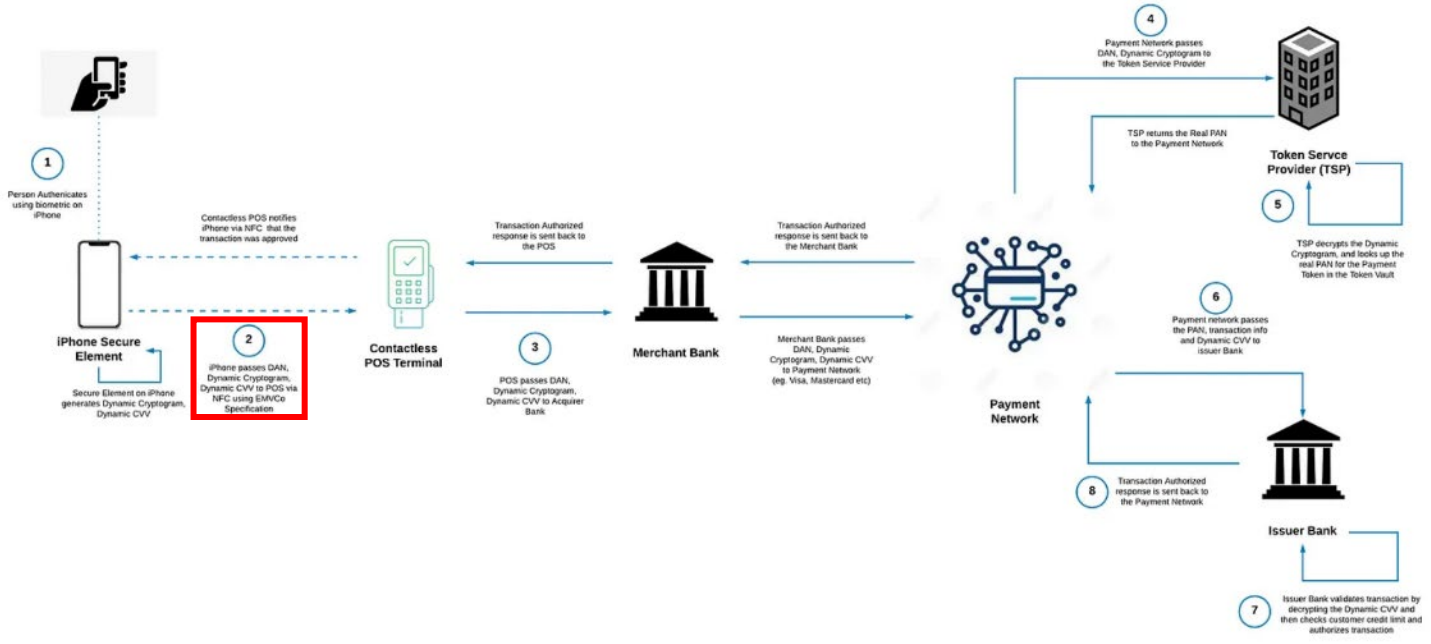
The decrypted payment data in the `data` value contains the following keys and values:

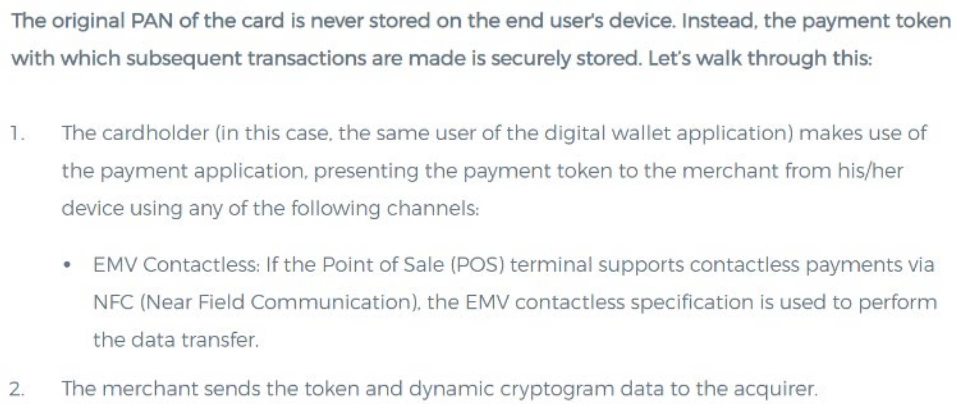
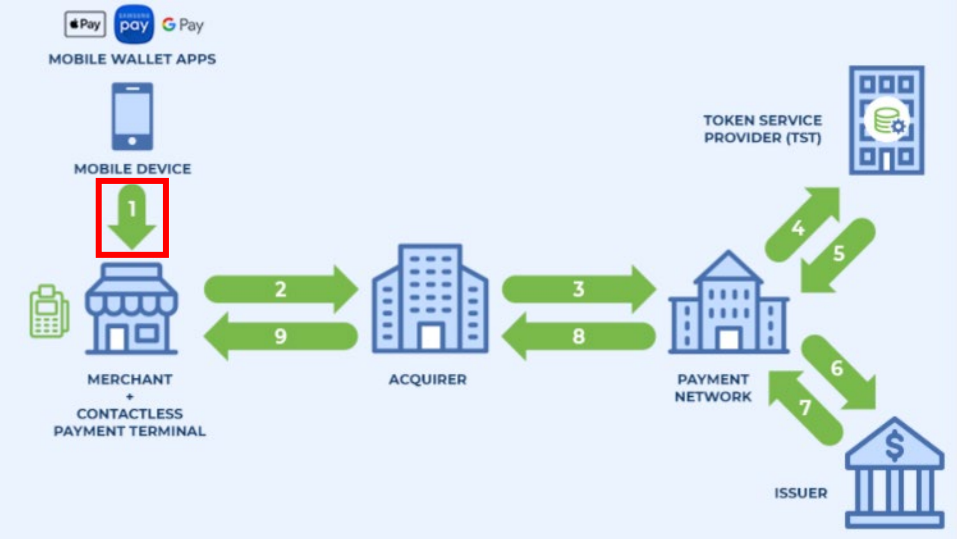
Key	Value	Description
`applicationPrimaryAccountNumber`	string	Device-specific account number of the card that funds this transaction
`applicationExpirationDate`	date as a string	Card expiration date in the format YYMMDD
`currencyCode`	string	ISO 4217 numeric currency code, as a string to preserve leading zeros
`transactionAmount`	number	Transaction amount
`cardholderName`	string	Optional. Cardholder name.
`deviceManufacturerIdentifier`	string	Hex-encoded device manufacturer identifier
`paymentDataType`	string	Either `"3DSecure"` or `"EMV"`
`paymentData`	payment data dictionary	Detailed payment data; see Detailed Payment Data Keys (3D Secure) and Detailed Payment Data Keys (EMV) below
`authenticationResponses`	list of Authentication Response entries	For a multitoken request, a list of submerchant responses that contain cryptograms. See Authentication Response below.
`merchantTokenIdentifier`	string	For a merchant token request, the provisioned merchant token identifier from the payment network
`merchantTokenMetadata`	`MerchantTokenMetadata`	For a merchant token request, this data contains card art and the token's last four digits and expiration date

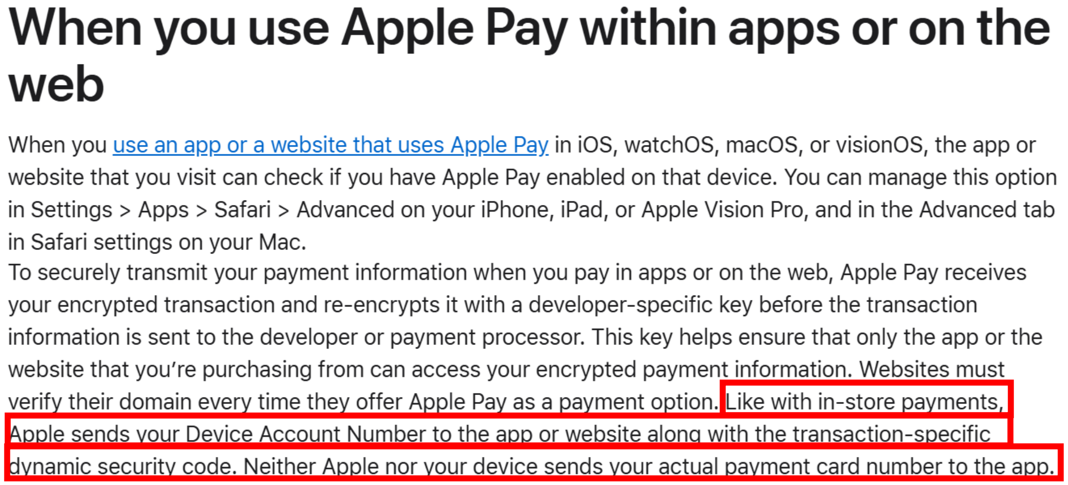
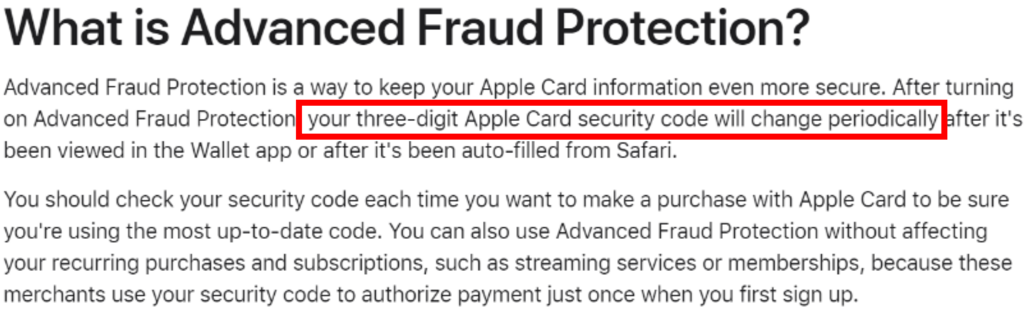
See, e.g., *Payment token format reference*, Apple Developer, https://developer.apple.com/documentation/passkit_apple_pay_and_wallet/apple_pay/payment_token_format_reference; *PKPayment*, Apple Developer, https://developer.apple.com/documentation/passkit_apple_pay_and_wallet/pkpayment.

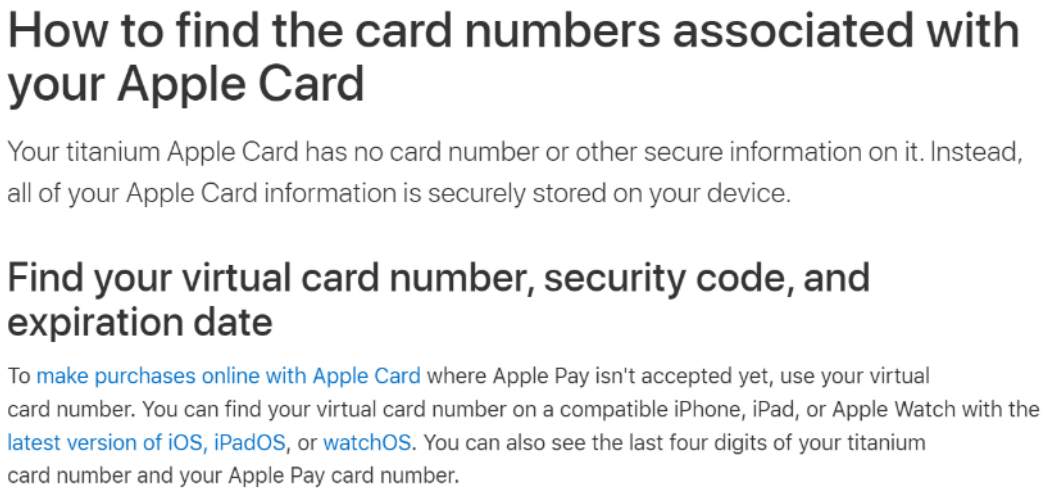
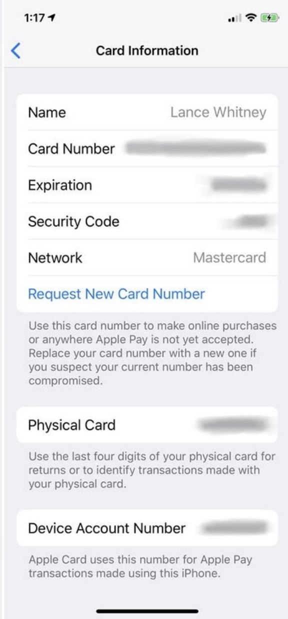
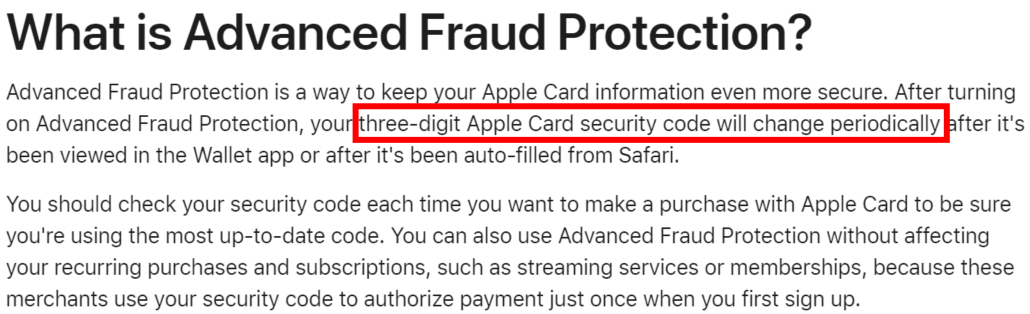
Claim Language	Accused Products
	 Payment flow Apple Pay uses device-specific tokenized credit or debit card credentials (DPAN) in place of a Payment Account Number (PAN). When users authenticate the payment using Face ID, Touch ID or their passcode, the tokenized card data is returned to your app or 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. **Customer** Authenticates with biometrics or passcode. Payment Data is encrypted and returned to the app/website **Merchant App/Website** Sends the Apple Pay payment object to merchant server **Merchant Server** Receives payment object and maps data to PSP API or SDK **Payment Service Provider** Decrypts Apple Pay payment object and formats a 3D Secure authorization message **Acquirer** Sends payment for authorization **Payment Network** De-tokenizes payment data and sends PAN to issuer for authorization **Issuer** Authorizes payment *See, e.g.*, *Apple Pay Merchant Integration Guide* (Jan. 2024) *available at* http://developer.apple.com/apple-pay/Apple-Pay-Merchant-Integration-Guide.pdf; *Get started with Apple Pay on the Web*, Apple Developer, https://developer.apple.com/videos/play/tech-talks/111381/.

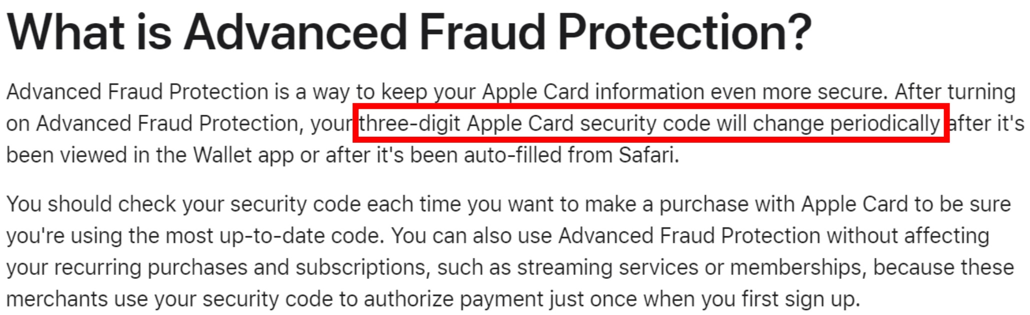
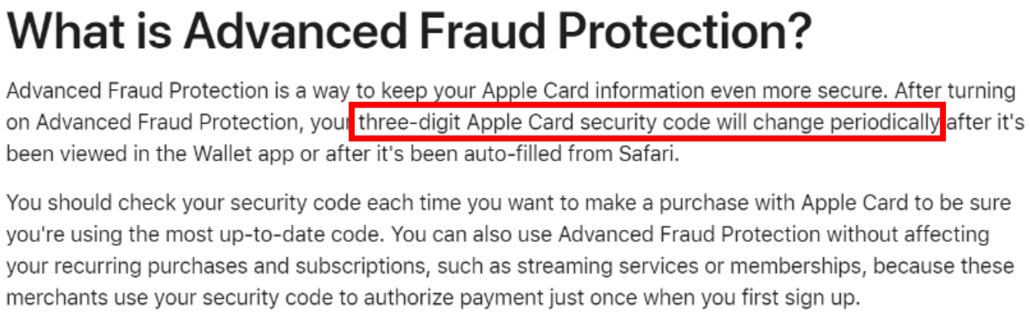
Claim Language	Accused Products
	 Name on card Type Choose... Credit card number Done Apple Card ···· Apple Cash $10.00 Q W E R T Y U I O P AutoFill in Safari lets you drop an Apple Cash number in as easily as any credit card. Using it regenerates the security code immediately. *See, e.g.*, Filipe Espósito, *iOS 16 to add virtual cards support in Safari for online shopping*, 9to5MAC (Jul. 6, 2022, 12:25 pm PT), https://9to5mac.com/2022/07/06/ios-16-virtual-cards-support-safari/; Glenn Fleishman, *How to pay even more safely with Apple Cash*, Macworld (Apr. 12, 2024), https://www.macworld.com/article/2270855/safely-use-apple-cash.html. **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)  Token Service Provider[a] VISA DISCOVER Merchant Mobile App Payment Token+ Cryptogram 1 10 Confirmation Message Merchant Acquirer/ Processor Payment Token+ Cryptogram 2 9 Payment Token + Last 4 3 4 Payment Network[c] PAN 5 8 PAN[b] Issuer Processor PAN 6 7 PAN[b] Issuer [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, *EMV Payment Tokenization Primer and Lessons Learned* 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.

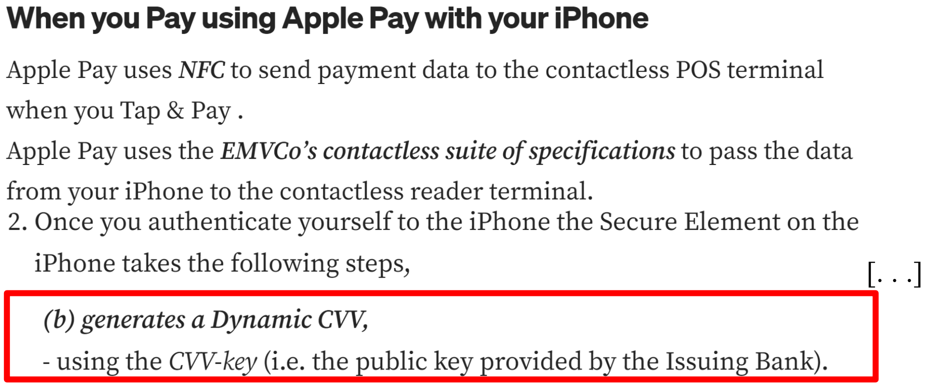
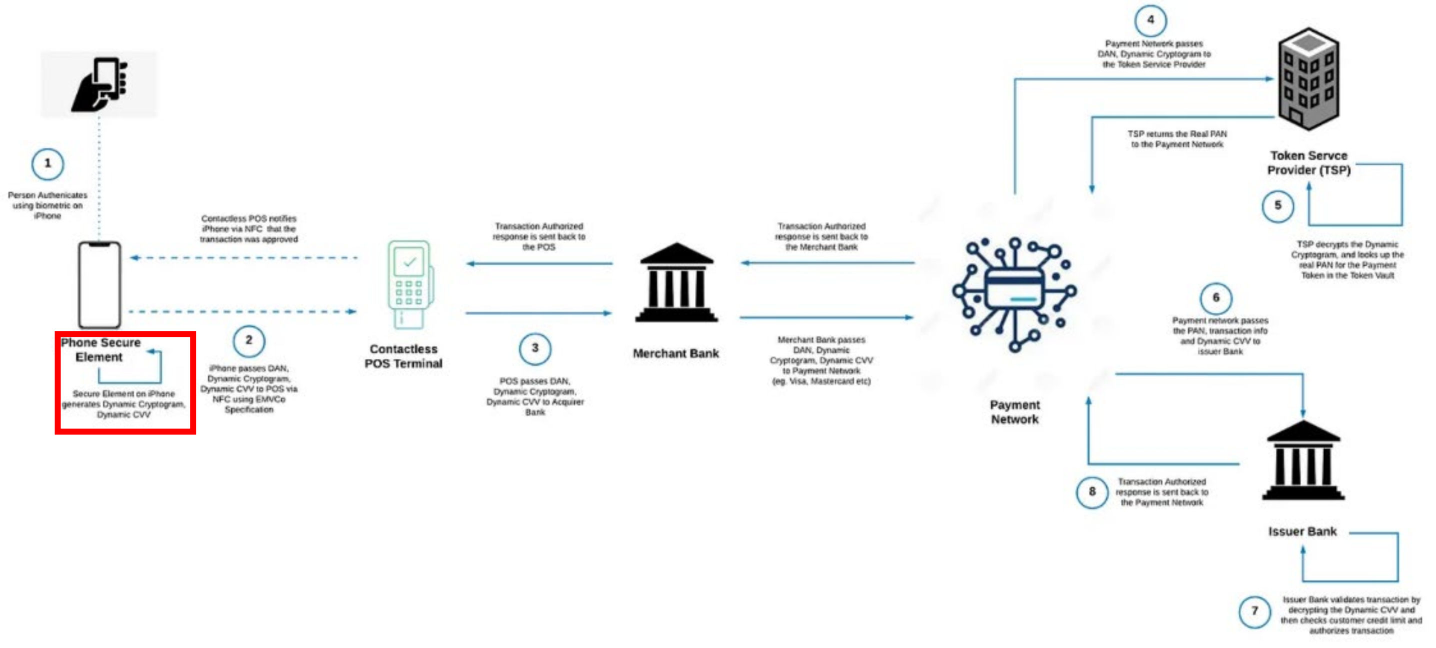
Claim Language	**Accused Products**
	 **When you Pay using Apple Pay with your iPhone** Apple Pay uses *NFC* to send payment data to the contactless POS terminal when you Tap & Pay . Apple Pay uses the ***EMVCo's contactless suite of specifications*** to pass the data from your iPhone to the contactless 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 *Payment Token (DAN), the Dynamic Cryptogram*** (also called, the *One-time Unique Number*), ***the Dynamic CVV Value*** (also called, the *Dynamic Security Code*), and other payment and chip data elements to the POS terminal via NFC, using the EMVCo's contactless suite of specifications.  1 Person Authenicates using biometric on iPhone iPhone Secure Element Secure Element on iPhone generates Dynamic Cryptogram, Dynamic CVV Contactless POS notifies iPhone via NFC that the transaction was approved 2 iPhone passes DAN, Dynamic Cryptogram, Dynamic CVV to POS via NFC using EMVCo Specification Contactless POS Terminal Transaction Authorized response is sent back to the POS 3 POS passes DAN, Dynamic Cryptogram, Dynamic CVV to Acquirer Bank Merchant Bank Transaction Authorized response is sent back to the Merchant Bank Merchant Bank passes DAN, Dynamic Cryptogram, Dynamic CVV to Payment Network (eg. Visa, Mastercard etc) Payment Network 4 Payment Network passes DAN, Dynamic Cryptogram to the Token Service Provider TSP returns the Real PAN to the Payment Network Token Servce Provider (TSP) 5 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 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 When you Pay using Apple Pay with your iPhone *See, e.g.*, Prashant Ram, *How Apple Pay works under the hood?*, codeburst (Nov. 5, 2019), https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7.

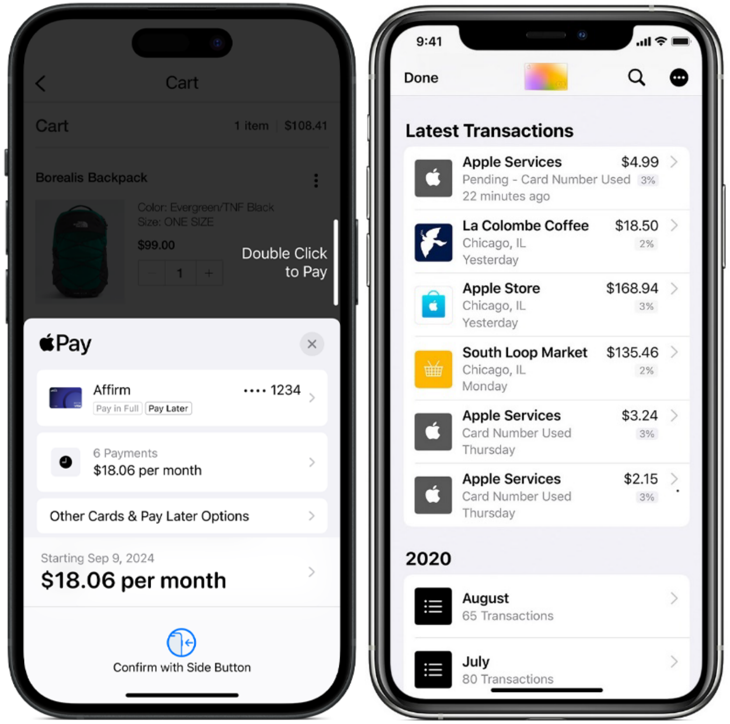
Claim Language	**Accused Products**
	 The original PAN of the card is never stored on the end user's device. Instead, the payment token with which subsequent transactions are made is securely stored. Let's walk through this: 1. The cardholder (in this case, the same user of the digital wallet application) 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.  Pay pay G Pay MOBILE WALLET APPS MOBILE DEVICE 1 TOKEN SERVICE PROVIDER (TST) 4 5 MERCHANT + CONTACTLESS PAYMENT TERMINAL 2 9 ACQUIRER 3 8 PAYMENT NETWORK 6 7 ISSUER *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.

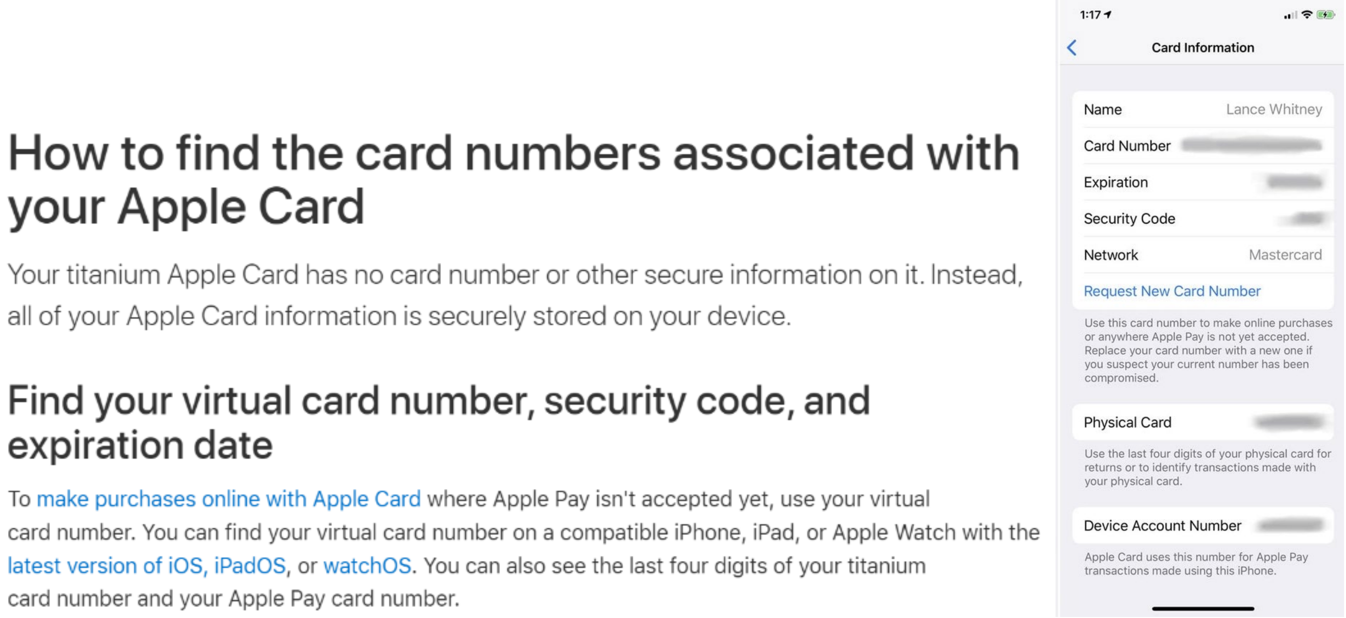
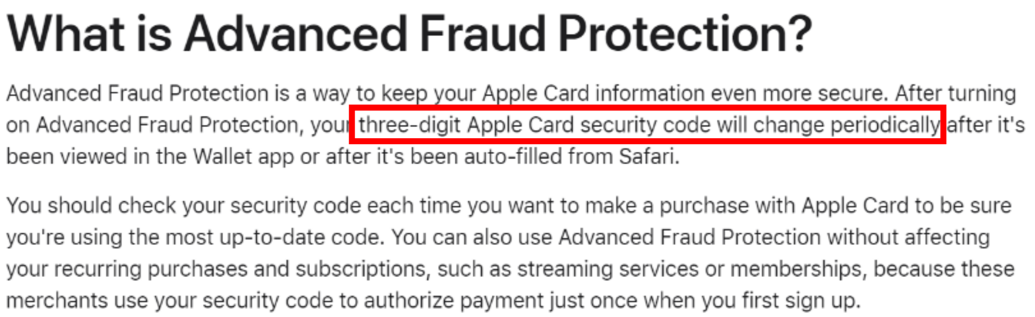
Claim Language	Accused Products
11[k]: wherein the limited-use payment information is configured to be used in place of a card issuer payment information.	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—generates a limited-use payment information (*e.g.*, the dynamic cryptogram or the dynamic security code) that is configured to be used in place of a card issuer payment information (*e.g.*, PAN or associated expiration date or CVV).  **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, macOS, or visionOS, the app or website that you visit can check if you have Apple Pay enabled on that device. You can manage this option in Settings > Apps > Safari > Advanced on your iPhone, iPad, or Apple Vision Pro, and in the Advanced tab in Safari settings 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.*, *Apple Pay security and privacy overview*, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554.  **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.*, *Use Advanced Fraud Protection with Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102427.
12. The system of claim 11, wherein the thin payment device bears no fixed payment numbers, and bears only: the cardholders name; a brand logo; and the card payment network logo.	The Apple Card is a thin payment device and bears no fixed payment numbers and bears only the cardholders name; a brand logo; and the card payment network logo. *See supra* Claim 2.

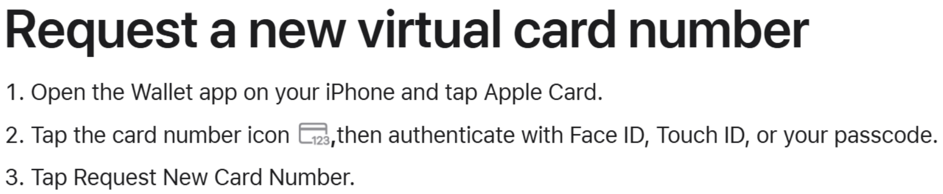
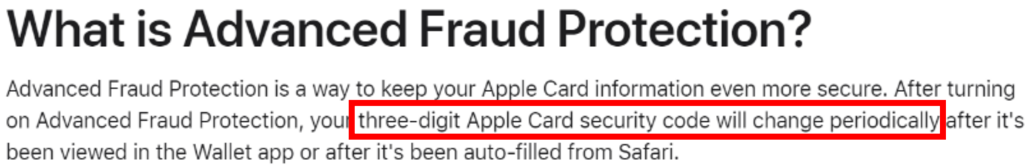
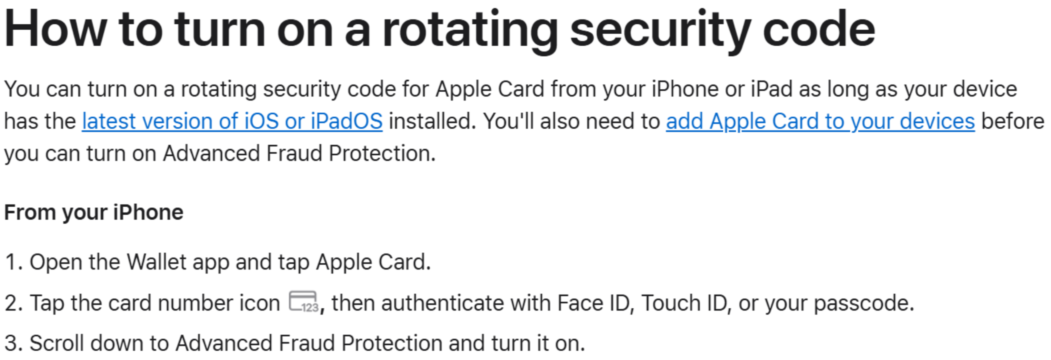
Claim Language	**Accused Products**
13[a] The system of claim 11 wherein the personal computing device is configured for presenting on the display a limited-use card security code number for use in payments in place of card issuer payment information, and	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—is configured for presenting on the display a limited-use card security code number (*e.g.*, the dynamic security code) for use in payments in place of card issuer payment information (*e.g.*, a CVV associated with the PAN).  How to find the card numbers associated with your Apple Card Your titanium Apple Card has no card number or other secure information on it. Instead, all of your Apple Card information is securely stored on your device. 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.  Card Information Name Lance Whitney Card Number [redacted] Expiration [redacted] Security Code [redacted] Network Mastercard Request New Card Number Use this card number to make online purchases or anywhere Apple Pay is not yet accepted. Replace your card number with a new one if you suspect your current number has been compromised. Physical Card [redacted] Use the last four digits of your physical card for returns or to identify transactions made with your physical card. Device Account Number [redacted] Apple Card uses this number for Apple Pay transactions made using this iPhone. *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; *see, e.g.*, Lance Whitney, *How to use your Apple Card without Apple Pay*, TechRepublic (Oct. 1, 2019), https://www.techrepublic.com/article/how-to-use-your-apple-card-without-apple-pay/; Andrew O'Hara, *Tips and tricks for mastering Apple Card*, AppleInsider (Aug. 20, 2019), https://appleinsider.com/articles/19/08/20/tips-and-tricks-for-mastering-apple-card ("If you want to use your Apple Card online, and the retailer doesn't support Apple Pay or autofill in Safari, you have to manually enter in your card number. Those details can be readily found within the Wallet app.").  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.*, *Use Advanced Fraud Protection with Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102427.

Claim Language	**Accused Products**
13[b] wherein the personal computing device is further configured to generate said limited-use card security code responsive to an input request from a valid user, via said user-interface, and	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—is further configured to generate said limited-use card security code (*e.g.*, dynamic security code) responsive to an input request from a valid user, via said user-interface (*e.g.*, a request to turn on Advanced Fraud Protection, user views the dynamic security code on Wallet app, or causes auto-fill of dynamic security code on Safari).  **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.*, *Use Advanced Fraud Protection with Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102427.
13[c] wherein said limited-use number is generated on the personal computing device from at least one information from a set comprising: a payment device user information; a payment device account number; a payment device sequence counter; a payment device identifier; payment device secrets; a payment device key; computing device secrets; computing device keys; payment device issuer secrets; payment device issuer keys; a time; an expiration date; an amount; a merchant locality; an online location; a transaction information; and a cryptographic combination of at least two of the above.	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—generates the limited-use number (*e.g.*, the dynamic security code), on information and belief, from at least one information of a set comprising a payment device user information; a payment device account number; a payment device sequence counter (*e.g.*, on information and belief, a counter to ensure the dynamic security code is transaction-specific); a payment device identifier; payment device secrets; a payment device key; computing device secrets; computing device keys; payment device issuer secrets; payment device issuer keys (*e.g.*, a CVV-key); a time; an expiration date; an amount; a merchant locality; an online location; a transaction information; and a cryptographic combination of at least two of the above. *See supra* limitation 11[i]. For example, the dynamic security code is generated using at least a key (*e.g.*, a CVV-key).  **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.*, *Use Advanced Fraud Protection with Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102427.

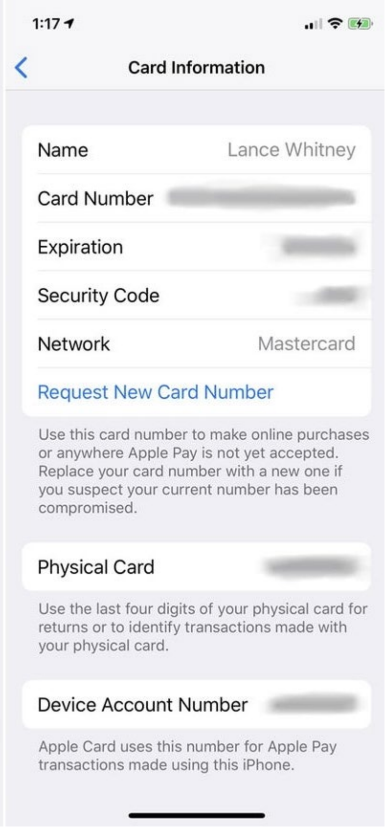
Claim Language	Accused Products
	 **When you Pay using Apple Pay with your iPhone** Apple Pay uses *NFC* to send payment data to the contactless POS terminal when you Tap & Pay . Apple Pay uses the ***EMVCo's contactless suite of specifications*** to pass the data from your iPhone to the contactless reader terminal. 2. Once you authenticate yourself to the iPhone the Secure Element on the iPhone takes the following steps, [. . .] *(b) generates a Dynamic CVV,* - using the *CVV-key* (i.e. the public key provided by the Issuing Bank).  1 Person Authenicates using biometric on iPhone Phone Secure Element Secure Element on iPhone generates Dynamic Cryptogram, Dynamic CVV Contactless POS notifies iPhone via NFC that the transaction was approved 2 iPhone passes DAN, Dynamic Cryptogram, Dynamic CVV to POS via NFC using EMVCo Specfication Contactless POS Terminal Transaction Authorized response is sent back to the POS 3 POS passes DAN, Dynamic Cryptogram, Dynamic CVV to Acquirer Bank Merchant Bank Transaction Authorized response is sent back to the Merchant Bank Merchant Bank passes DAN, Dynamic Cryptogram, Dynamic CVV to Payment Network (eg. Visa, Mastercard etc) Payment Network 4 Payment Network passes DAN, Dynamic Cryptogram to the Token Service Provider TSP returns the Real PAN to the Payment Network Token Servce Provider (TSP) 5 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 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 When you Pay using Apple Pay with your iPhone *See, e.g.*, Prashant Ram, *How Apple Pay works under the hood?*, codeburst (Nov. 5, 2019), https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7; Zahid Shaikh, *Apple Pay and the DAN*, sardine (Aug. 15, 2023), https://www.sardine.ai/blog/apple-pay-and-the-dan ("The CVV (3 or 4 digit security number) is also protected securely. Apple Pay generates a new CVV for every transaction, This transaction-specific dynamic security code (CVV) is more secure than magnetic swipes which helps avoid malware hacks.").

Claim Language	**Accused Products**
	 Cart Cart 1 item | $108.41 Borealis Backpack Color: Evergreen/TNF Black Size: ONE SIZE $99.00 Double Click to Pay Pay Affirm •••• 1234 Pay in Full Pay Later 6 Payments $18.06 per month Other Cards & Pay Later Options Starting Sep 9, 2024 $18.06 per month Confirm with Side Button 9:41 Done Latest Transactions Apple Services $4.99 Pending - Card Number Used 3% 22 minutes ago La Colombe Coffee $18.50 Chicago, IL 2% Yesterday Apple Store $168.94 Chicago, IL 3% Yesterday South Loop Market $135.46 Chicago, IL 2% Monday Apple Services $3.24 Card Number Used 3% Thursday Apple Services $2.15 Card Number Used 3% Thursday 2020 August 65 Transactions July 80 Transactions *See, e.g.*, *Apple Pay*, Apple, https://www.apple.com/apple-pay/ (last visited Dec. 30, 2024); John M Evans, *Apple Pay History*, Apple Community (Aug. 23, 2021 1:02 PM), https://discussions.apple.com/thread/253075944?sortBy=rank.
14[a] The system as described in claim 11 wherein the personal computing device is configured for presenting on the display, a limited-use card account number, and a limited-duration expiration date, for use in payments in place of a card issuer payment information, and	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—is configured for presenting on the display, a limited-use card account number (*e.g.*, VAN and associated security code or dynamic security code), and, on information and belief, a limited-duration expiration date, for use in payments in place of a card issuer payment information (*e.g.*, PAN or associated expiration date or CVV).

Claim Language	**Accused Products**
	 How to find the card numbers associated with your Apple Card Your titanium Apple Card has no card number or other secure information on it. Instead, all of your Apple Card information is securely stored on your device. 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. 1:17 Card Information Name Lance Whitney Card Number [redacted] Expiration [redacted] Security Code [redacted] Network Mastercard Request New Card Number Use this card number to make online purchases or anywhere Apple Pay is not yet accepted. Replace your card number with a new one if you suspect your current number has been compromised. Physical Card [redacted] Use the last four digits of your physical card for returns or to identify transactions made with your physical card. Device Account Number [redacted] Apple Card uses this number for Apple Pay transactions made using this iPhone. *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.  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.*, *Use Advanced Fraud Protection with Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102427.
14[b] wherein said personal computing device is further configured to generate said limited-use card payment information responsive to an input request from a valid user, and	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—is configured to generate said limited-use card payment information responsive to an input request from a valid user (*e.g.*, on information and belief, request for a new VAN, turning on an dynamic security code).

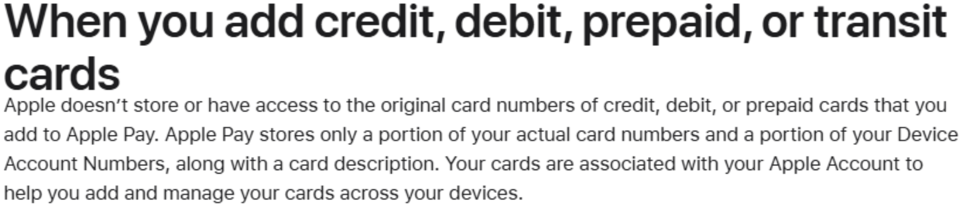
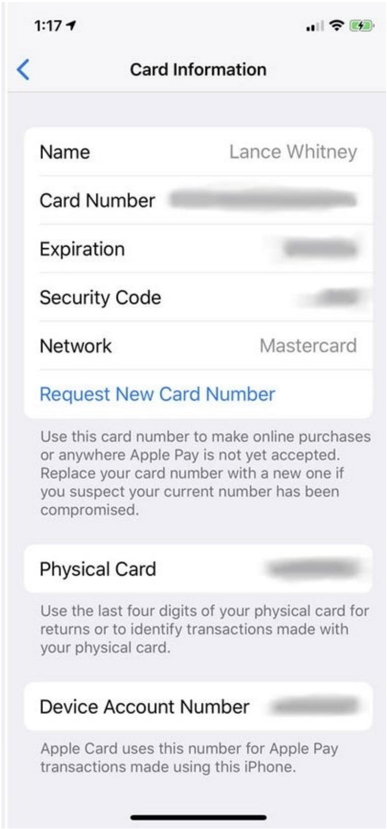
Claim Language	Accused Products
	 **Request a new virtual card number** 1. Open the Wallet app on your iPhone and tap Apple Card. 2. Tap the card number icon ,then authenticate with Face ID, Touch ID, or your passcode. 3. Tap Request New Card Number. *See, e.g.*, *How to find the card numbers associated with your Apple Card*, Apple (Mar. 4, 2024), https://support.apple.com/en-us/118544; Christian Zibreg, *Apple Card will let you generate virtual card numbers for online purchases*, iDownloadBlog (Apr. 19, 2019), https://www.idownloadblog.com/2019/04/01/apple-card-virtual-numbers/.  **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. [. . .]  **How to turn on a rotating security code** You can turn on a rotating security code for Apple Card from your iPhone or iPad as long as your device has the latest version of iOS or iPadOS installed. You'll also need to add Apple Card to your devices before you can turn on Advanced Fraud Protection. **From 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. 3. Scroll down to Advanced Fraud Protection and turn it on. *See, e.g.*, *Use Advanced Fraud Protection with Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102427.
14[c] wherein the personal computing device is configured to identify a valid device-user through at least one user-validation input available to the personal computing device, of a set comprising: a touch ID sensor operable to identify the touch a valid user; a user entering of a valid passcode on a touch sensor-array; a user entering of	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—is configured to identify a valid device-user through at least one user-validation input available to the personal computing device, of a set comprising a touch ID sensor operable to identify the touch a valid user (*e.g.*, Touch ID); a user entering of a valid passcode on a touch sensor-array (*e.g.*, passcode); a user entering of a valid passcode on a key-pad; a user entering of a valid PIN or Key-Code on the user-interface; a user entering of a valid password on the user-interface; a valid user swiping or gesturing on a touch sensor-array; a valid sequence of a user tapping of the device detectable by device accelerometer; a valid user sequence of user motioning of the device detectable by device motion sensor unit; a skin-contact sensing identifying a valid user on a device contact sensor (*e.g.*, Touch ID); a touching of an identified user's skin on a device touch sensor array (*e.g.*, Touch ID); a device biometric recognition of a valid user via a device biometric sensing (*e.g.*, Touch ID, Face ID); and a biometric sensing of the device remaining continuously in the proximity possession of a valid user via device skin-proximity sensor.

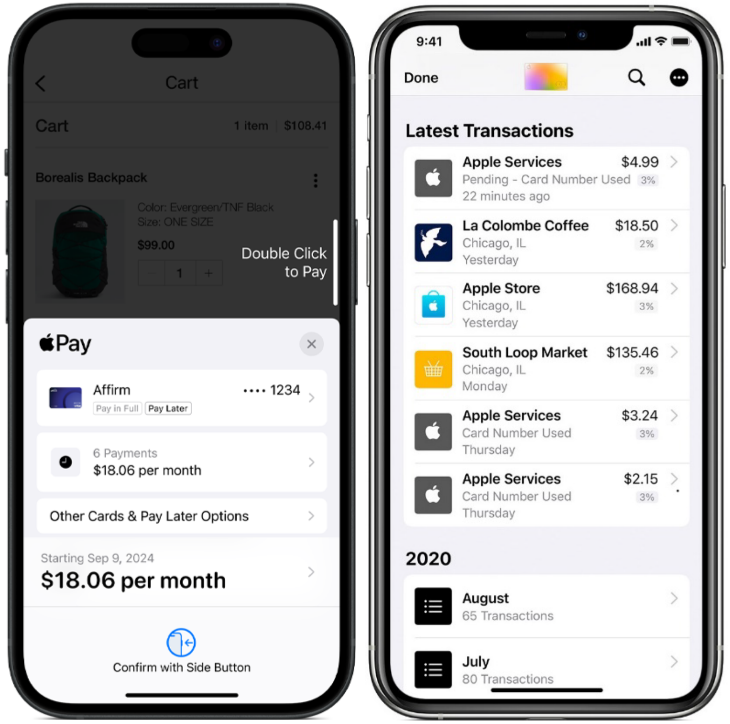
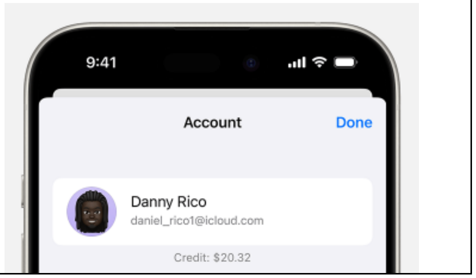
Claim Language	**Accused Products**
a valid passcode on a key-pad; a user entering of a valid PIN or Key-Code on the user-interface; a user entering of a valid password on the user-interface; a valid user swiping or gesturing on a touch sensor-array; a valid sequence of a user tapping of the device detectable by device accelerometer; a valid user sequence of user motioning of the device detectable by device motion sensor unit; a skin-contact sensing identifying a valid user on a device contact sensor; a touching of an identified user's skin on a device touch sensor array; a device biometric recognition of a valid user via a device biometric sensing; and a biometric sensing of the device remaining continuously in the proximity possession of a valid user via device skin-proximity sensor; and,	*See supra* limitation 14[b].
14[d] wherein the personal computing device conveys the limited-use payment information through the user interface.	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—conveys the limited-use payment information (*e.g.*, as identified above) through the user interface (*e.g.*, display). *See supra* limitation 14[a].

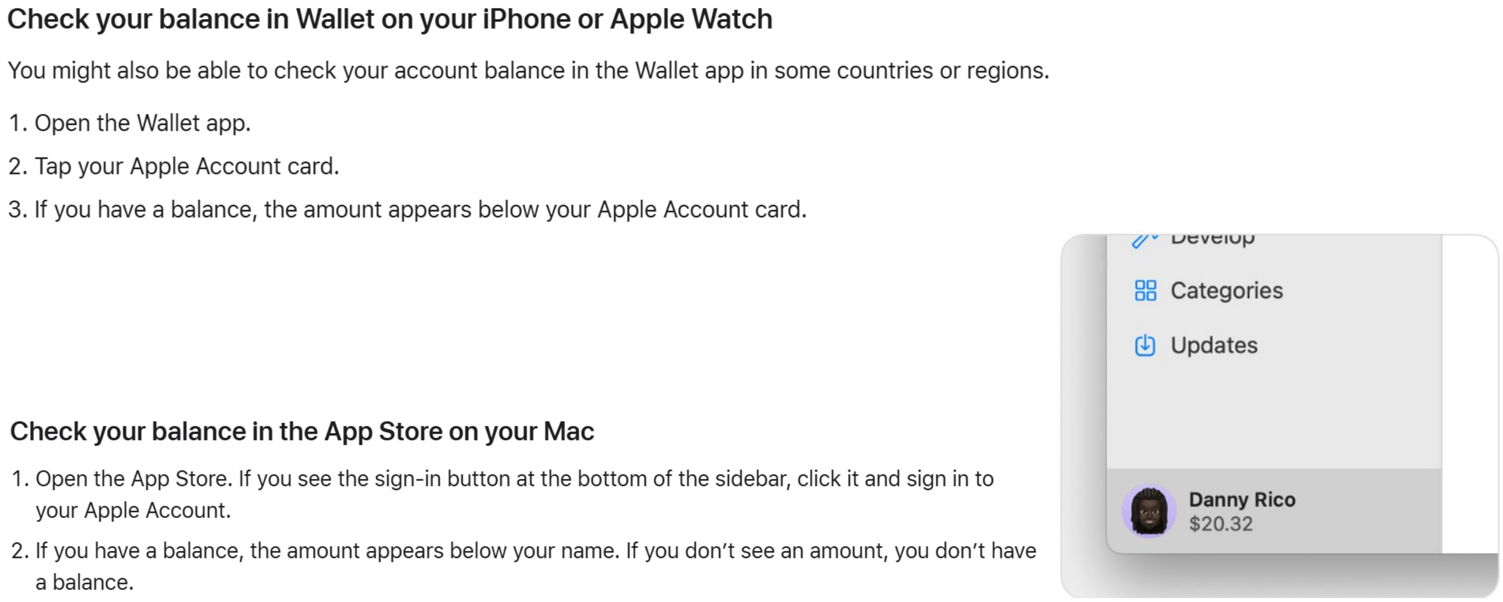
Claim Language	**Accused Products**
	 1:17 Card Information Name Lance Whitney Card Number [redacted] Expiration [redacted] Security Code [redacted] Network Mastercard Request New Card Number Use this card number to make online purchases or anywhere Apple Pay is not yet accepted. Replace your card number with a new one if you suspect your current number has been compromised. Physical Card [redacted] Use the last four digits of your physical card for returns or to identify transactions made with your physical card. Device Account Number [redacted] Apple Card uses this number for Apple Pay transactions made using this iPhone. *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.

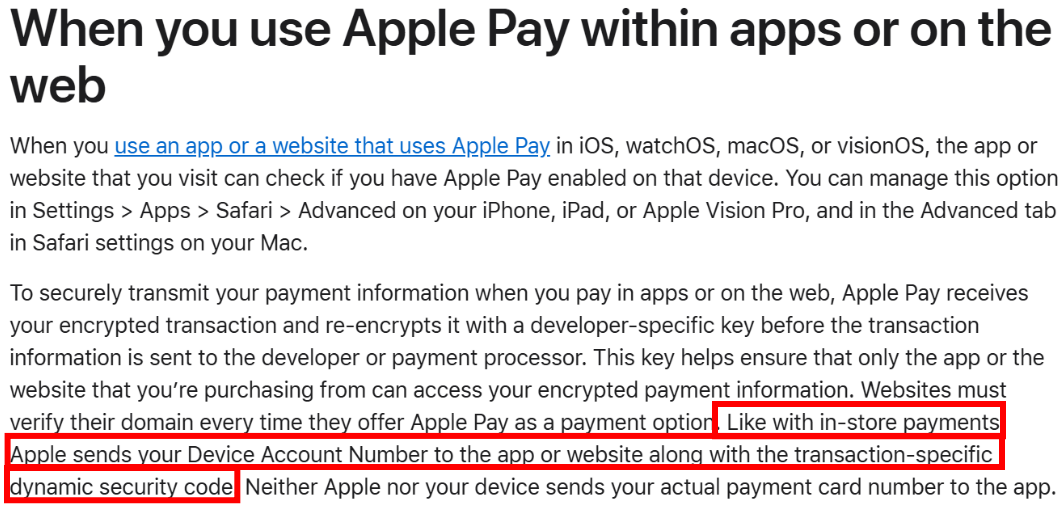
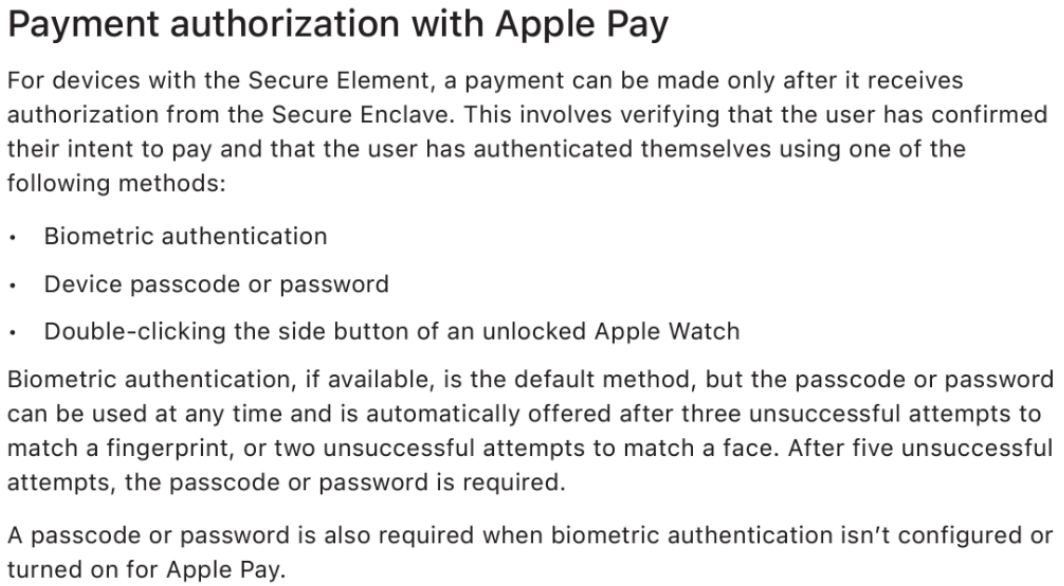
III. Claim 15 and Dependent Claims 16–20

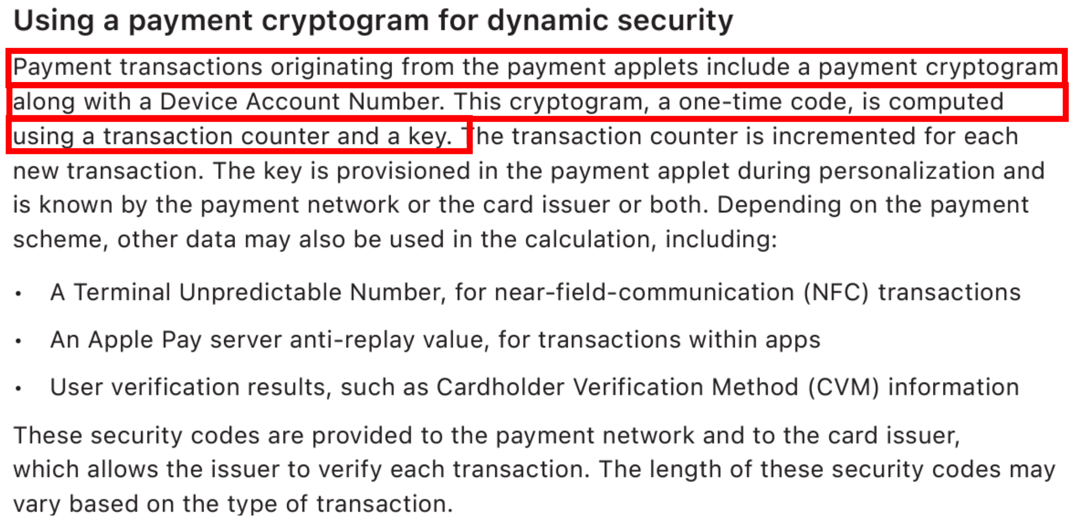
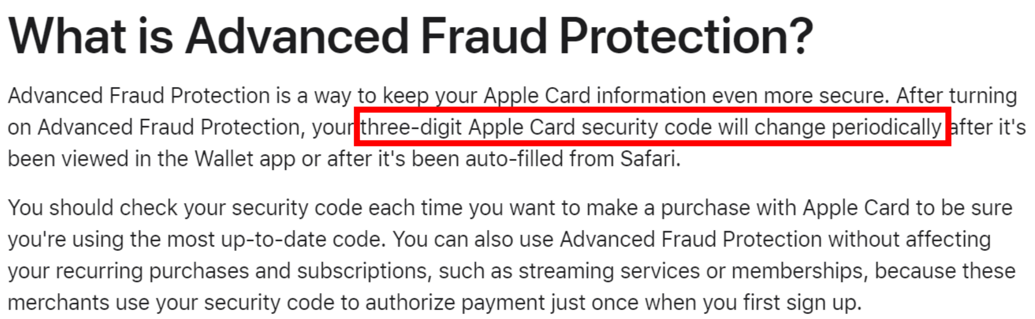
Claim Language	**Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card**
15[pre] An online payment system comprising:	To the extent the preamble is limiting, the combination of an Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—with an Apple Card is an online payment system. *See supra* Claim 11[pre].
15[a] a thin card-shaped payment card device that bears no fixed payment numbers on the card device; and	The Apple Card is a thin card-shaped payment card device that bears no fixed payment numbers on the card device. *See supra* limitation 11[a].
15[b] a computing device operable for completing an online payment transaction and comprising:	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—is a computing device operable for completing an online payment transaction. *See supra*, limitation 11[pre], 11[b].
15[c] a display;	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—includes a display. *See supra*, limitation 11[f].
15[d] a user-interface;	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—includes a user interface (*e.g.*, side button, biometric sensors (*e.g.*, for Face ID, Touch ID, Optic ID, wrist detection), touch screen panel, keyboard). *See supra*, limitation 11[g].
15[e] a processor; and	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—includes a processor (*e.g.*, system processor, processor of secure element, processor of secure enclave, or combination of the same). *See supra*, limitation 11[c].
15[f] a memory for storing a payment card information accessible to the processor,	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—includes a memory (*e.g.*, system memory, memory of secure element, memory of secure enclave, memory of eSIM/SIM, or combination of the same). for storing a payment card information accessible to the processor. *See supra*, limitation 11[d].

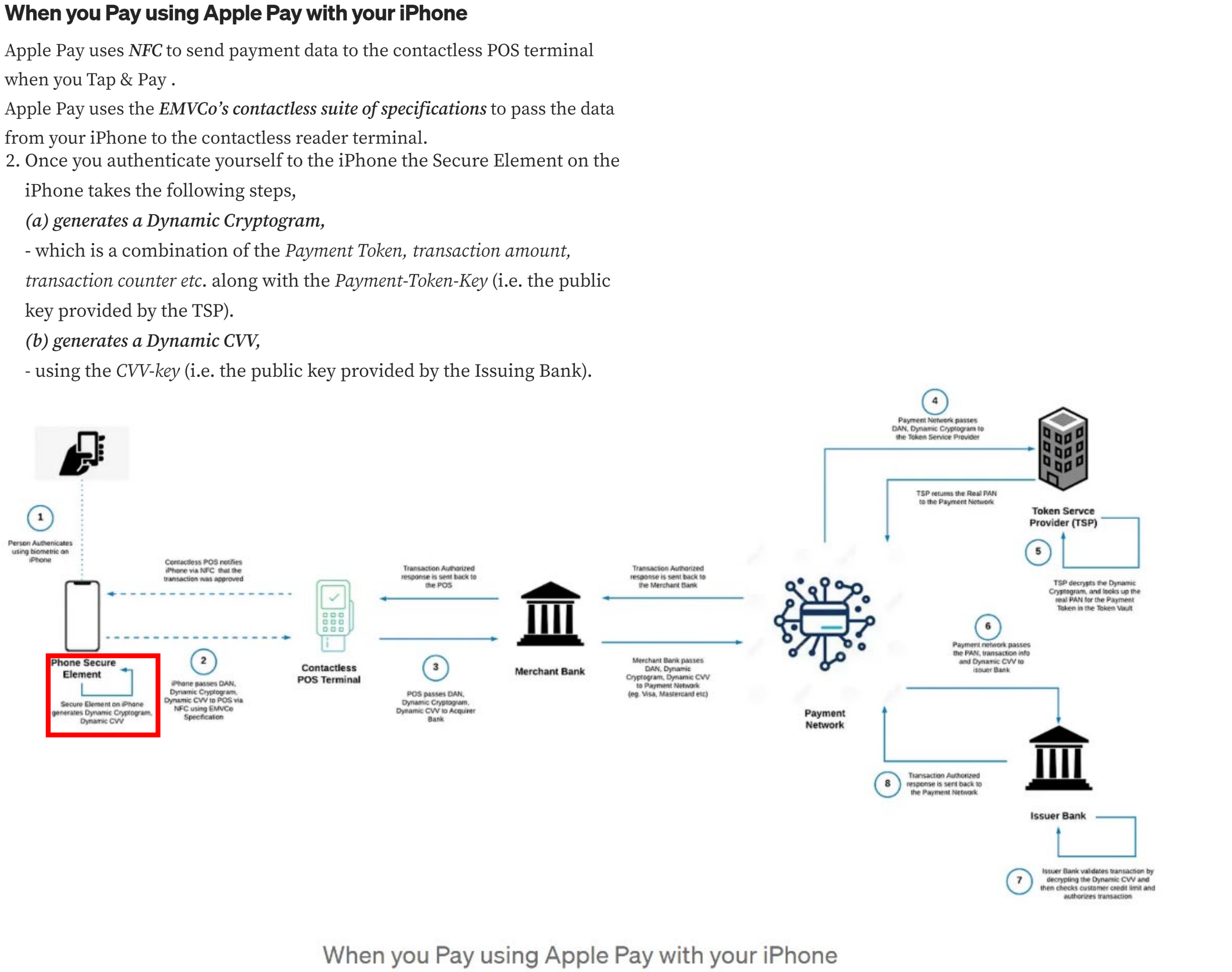
Claim Language	Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card
	 **When you add credit, debit, prepaid, or transit cards** Apple doesn't store or have access to the original card numbers of credit, debit, or prepaid cards that you add to Apple Pay. Apple Pay stores only a portion 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. *See, e.g.*, *Apple Pay security and privacy overview*, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554.  1:17 Card Information Name Lance Whitney Card Number [redacted] Expiration [redacted] Security Code [redacted] Network Mastercard Request New Card Number Use this card number to make online purchases or anywhere Apple Pay is not yet accepted. Replace your card number with a new one if you suspect your current number has been compromised. Physical Card [redacted] Use the last four digits of your physical card for returns or to identify transactions made with your physical card. Device Account Number [redacted] Apple Card uses this number for Apple Pay transactions made using this iPhone. *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.

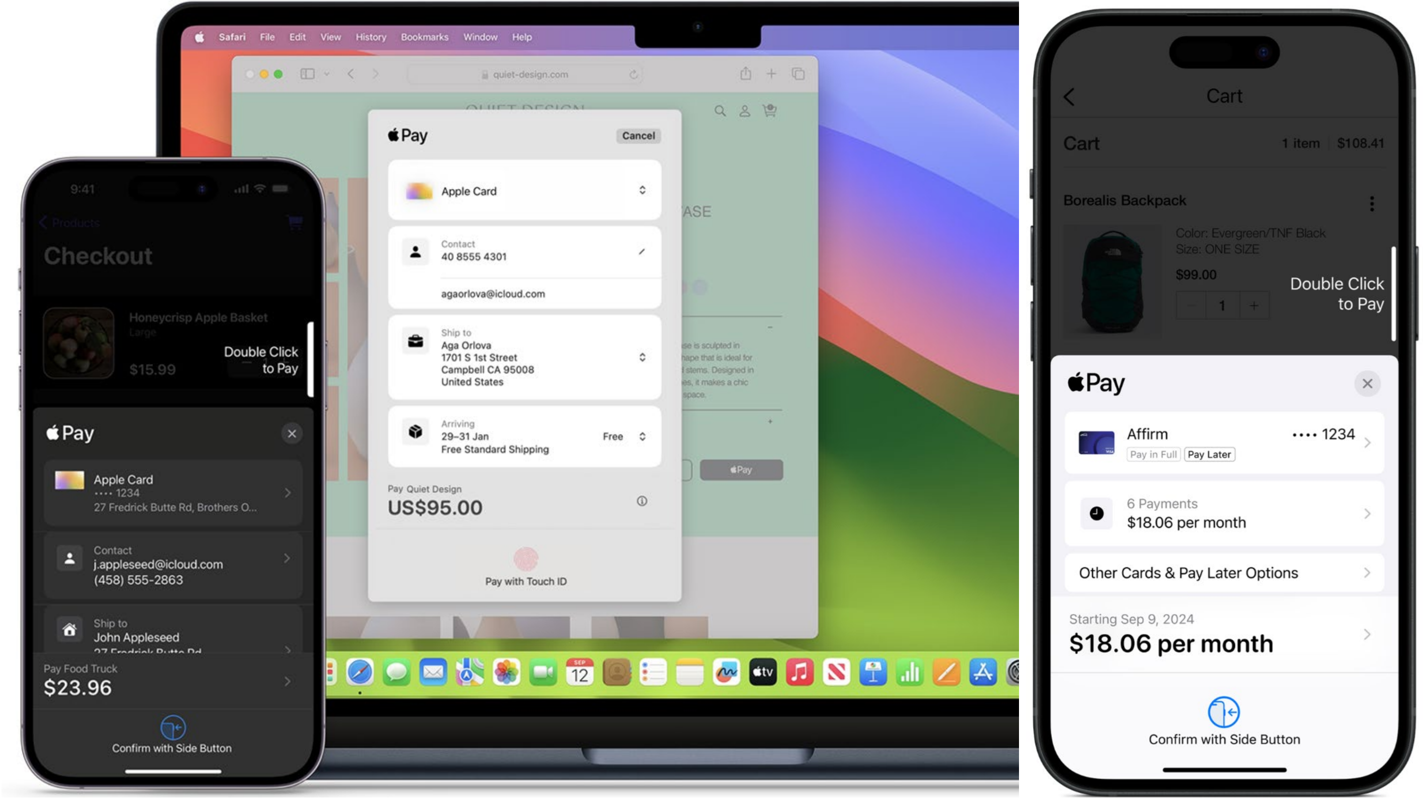
Claim Language	Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card
	 Cart Cart 1 item | $108.41 Borealis Backpack Color: Evergreen/TNF Black Size: ONE SIZE $99.00 1 Double Click to Pay Pay Affirm •••• 1234 Pay in Full Pay Later 6 Payments $18.06 per month Other Cards & Pay Later Options Starting Sep 9, 2024 $18.06 per month Confirm with Side Button 9:41 Done Latest Transactions Apple Services $4.99 Pending - Card Number Used 3% 22 minutes ago La Colombe Coffee $18.50 Chicago, IL 2% Yesterday Apple Store $168.94 Chicago, IL 3% Yesterday South Loop Market $135.46 Chicago, IL 2% Monday Apple Services $3.24 Card Number Used 3% Thursday Apple Services $2.15 Card Number Used 3% Thursday 2020 August 65 Transactions July 80 Transactions *See, e.g.*, *Apple Pay*, Apple, https://www.apple.com/apple-pay/ (last visited Dec. 30, 2024); John M Evans, *Apple Pay History*, Apple Community (Aug. 23, 2021 1:02 PM), https://discussions.apple.com/thread/253075944?sortBy=rank; *Apple introduces Apple Pay Later to allow consumers to pay for purchases over time*, Apple Newsroom (Mar. 28, 2023), https://www.apple.com/newsroom/2023/03/apple-introduces-apple-pay-later/; Rhett Intriago, *How to See Apple Pay History on iPhone*, iPhone Life (May 20, 2024), https://www.iphonelife.com/content/how-to-see-apple-pay-history. **Check your balance in the App Store on your iPhone, iPad, or Apple Vision Pro** 1. Open the App Store app. 2. Tap your photo, initials, or the sign-in button ⊙ at the top of the screen. You might be asked to sign in to your Apple Account. 3. If you have a balance, the amount appears. If you don't see an amount, you don't have a balance.  Danny Rico daniel_rico1@icloud.com Credit: $20.32

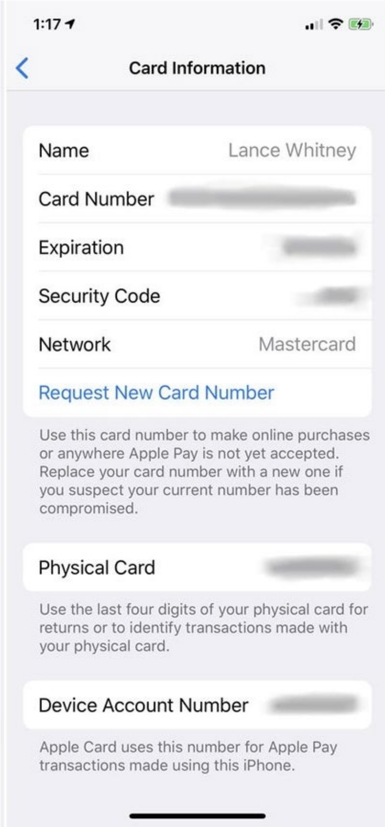
Claim Language	**Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card**
	 **Check your balance in Wallet on your iPhone or Apple Watch** You might also be able to check your account balance in the Wallet app in some countries or regions. 1. Open the Wallet app. 2. Tap your Apple Account card. 3. If you have a balance, the amount appears below your Apple Account card. **Check your balance in the App Store on your Mac** 1. Open the App Store. If you see the sign-in button at the bottom of the sidebar, click it and sign in to your Apple Account. 2. If you have a balance, the amount appears below your name. If you don't see an amount, you don't have a balance. *See, e.g.*, *Check your Apple Account balance*, Apple (Dec. 9, 2024), https://support.apple.com/en-us/119902.
15[g] wherein card issuer provided payment card information is wirelessly downloaded into the computing device, and	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—wirelessly (*e.g.*, via Wi-Fi, cellular, or NFC interfaces) downloads card issuer provided payment card information (*e.g.*, four digits of a physical card number, payment network, security code, expiration date, credit details, and, on information and belief, an VAN and associated expiration date or security code). *See supra*, limitations 11[e], 11[h].
15[h] wherein at least one of the set comprising: the computing device; and the card-shaped payment device, is configured to dynamically generate a limited-use payment information, upon the authorization of a valid computing device user, and	At least one of the set comprising an Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—and the Apple Card (*e.g.*, the Apple Pay and/or Apple Wallet-enabled computing device) is configured to dynamically generate a limited-use payment information (*e.g.*, the dynamic cryptogram, the dynamic security code, or any combination of the same with, *e.g.*, the DAN or, on information and belief, a VAN), upon the authorization of a valid computing device user (*e.g.*, side button or Home button double click, passcode, password, Face ID, Touch ID, Optic ID, wrist detection). *See supra*, limitation 11[i].

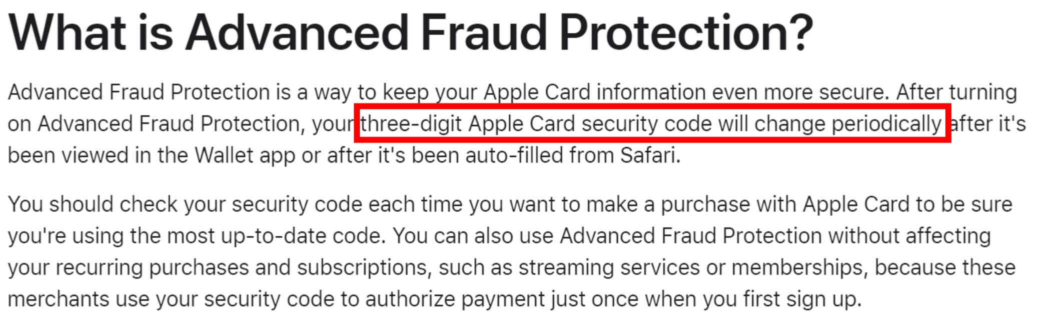
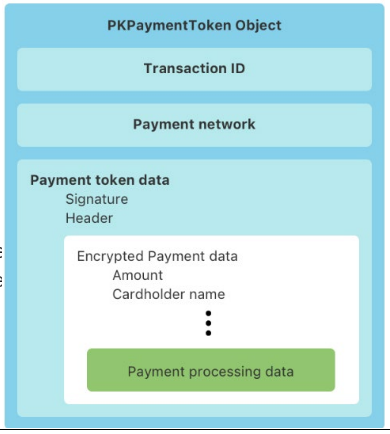
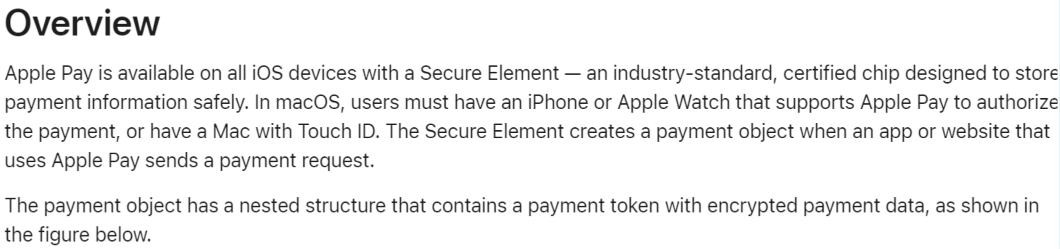
Claim Language	**Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card**
	 When you use Apple Pay within apps or on the web When you use an app or a website that uses Apple Pay in iOS, watchOS, macOS, or visionOS, the app or website that you visit can check if you have Apple Pay enabled on that device. You can manage this option in Settings > Apps > Safari > Advanced on your iPhone, iPad, or Apple Vision Pro, and in the Advanced tab in Safari settings 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.*, *Apple Pay security and privacy overview*, Apple (Oct. 8, 2024), https://support.apple.com/en-us/101554.  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.

Claim Language	**Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card**
	 **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.*, *Apple Platform Security*, at 182, 183 (Dec. 2024) *available at* https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; *see also, e.g.*, Apple Platform Security, *Payment authorization with Apple Pay*, 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.*, *Use Advanced Fraud Protection with Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102427.

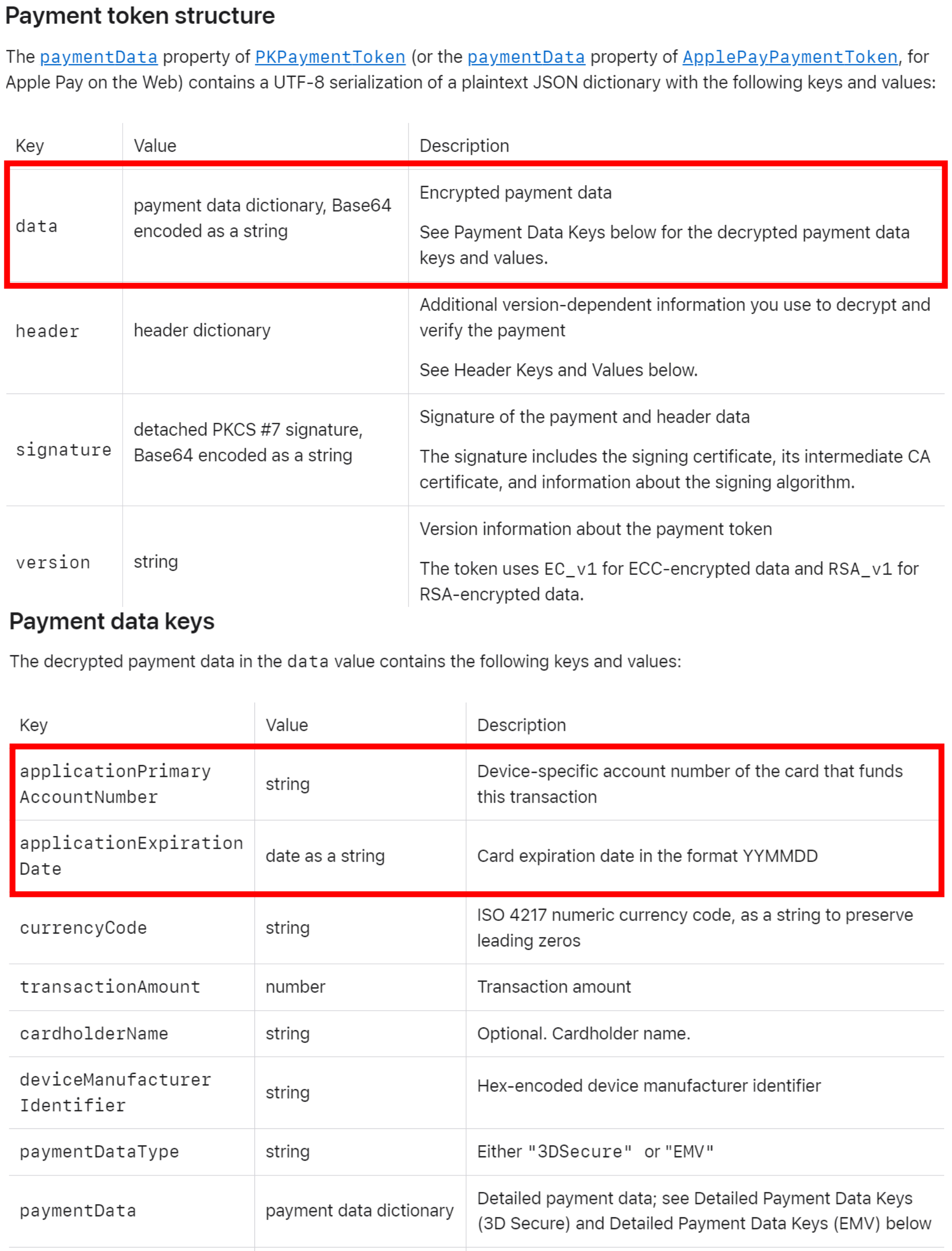
Claim Language	Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card
	 **When you Pay using Apple Pay with your iPhone** Apple Pay uses ***NFC*** to send payment data to the contactless POS terminal when you Tap & Pay . Apple Pay uses the ***EMVCo's contactless suite of specifications*** 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) generates a Dynamic Cryptogram,* - which is a combination of the *Payment Token, transaction amount, transaction counter etc*. along with the *Payment-Token-Key* (i.e. the public key provided by the TSP). *(b) generates a Dynamic CVV,* - using the *CVV-key* (i.e. the public key provided by the Issuing Bank). 1 Person Authenicates using biometric on iPhone Contactless POS notifies iPhone via NFC that the transaction was approved Phone Secure Element Secure Element on iPhone generates Dynamic Cryptogram, Dynamic CVV 2 iPhone passes DAN, Dynamic Cryptogram, Dynamic CVV to POS via NFC using EMVCo Specification Contactless POS Terminal Transaction Authorized response is sent back to the POS 3 POS passes DAN, Dynamic Cryptogram, Dynamic CVV to Acquirer Bank Merchant Bank Transaction Authorized response is sent back to the Merchant Bank Merchant Bank passes DAN, Dynamic Cryptogram, Dynamic CVV to Payment Network (eg. Visa, Mastercard etc) Payment Network 4 Payment Network passes DAN, Dynamic Cryptogram to the Token Service Provider TSP returns the Real PAN to the Payment Network Token Servce Provider (TSP) 5 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 8 Transaction Authorized response is sent back to the Payment Network Issuer Bank 7 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, *How Apple Pay works under the hood?*, codeburst (Nov. 5, 2019), https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7.

Claim Language	**Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card**
	 Checkout Honeycrisp Apple Basket $15.99 Double Click to Pay Pay Apple Card •••• 1234 27 Fredrick Butte Rd, Brothers O... Contact j.appleseed@icloud.com (458) 555-2863 Ship to John Appleseed Pay Food Truck $23.96 Confirm with Side Button Pay Cancel Apple Card Contact 40 8555 4301 agaorlova@icloud.com Ship to Aga Orlova 1701 S 1st Street Campbell CA 95008 United States Arriving 29–31 Jan Free Standard Shipping Free Pay Quiet Design US$95.00 Pay with Touch ID Cart Cart 1 item $108.41 Borealis Backpack Color: Evergreen/TNF Black Size: ONE SIZE $99.00 Double Click to Pay Pay Affirm •••• 1234 Pay in Full Pay Later 6 Payments $18.06 per month Other Cards & Pay Later Options Starting Sep 9, 2024 $18.06 per month Confirm with Side Button *See, e.g.*, Apple, *Apple Pay Merchant Integration Guide* at 3 (Jan. 2024) *available at* http://developer.apple.com/apple-pay/Apple-Pay-Merchant-Integration-Guide.pdf; *Apple Pay*, Apple, https://www.apple.com/apple-pay/ (last visited Dec. 30, 2024); *Get started with Apple Pay on the Web*, Apple Developer, https://developer.apple.com/videos/play/tech-talks/111381/.
15[i] wherein the payment information provided by the computing device is used in online transactions in place of a card issuers payment card information.	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—provides the payment information (*e.g.*, the dynamic cryptogram, the dynamic security code, and any combination of the same with the DAN or, on information and belief the VAN) that is used in online transactions (*e.g.*, online and in apps) in place of a card issuers payment card information (*e.g.*, the PAN or associated expiration date or CVV). *See supra* limitation 11[k].
16. The system of claim 15 wherein the card device bears no fixed payment numbers, and bears only: the cardholders name; the brand logo; and the card payment network logo.	An Apple Card bears no fixed payment numbers, and bears only: the cardholders name (*e.g.*, "Marisa Robertson"); the brand logo (*e.g.*, Apple logo); and the card payment network logo (*e.g.*, "MasterCard"). *See supra* claim 12.

Claim Language	**Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card**
17. The system of claim 15 wherein the dynamically generated limited-use payment information is displayable on a display of the computing device.	An Apple Pay and/or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—dynamically generates limited-use payment information (*e.g.*, dynamic security code) that is displayable on a display of the computing device. *See supra* limitation 11[i], 11[j], 15[h].  1:17 Card Information Name Lance Whitney Card Number [redacted] Expiration [redacted] Security Code [redacted] Network Mastercard Request New Card Number Use this card number to make online purchases or anywhere Apple Pay is not yet accepted. Replace your card number with a new one if you suspect your current number has been compromised. Physical Card [redacted] Use the last four digits of your physical card for returns or to identify transactions made with your physical card. Device Account Number [redacted] Apple Card uses this number for Apple Pay transactions made using this iPhone. *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.

Claim Language	Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card
	 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.*, *Use Advanced Fraud Protection with Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102427.
18. The system of claim 15 wherein the limited-use payment information includes a static limited-use card account number, a limited-duration card expiration date, and a limited-use card security code and, wherein the dynamically generated limited-use payment information is conveyed by the computing device to complete an online transaction.	An Apple Pay or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—dynamically generates limited-use payment information (*e.g.*, as described above) that includes a static limited-use card account number (*e.g.*, the DAN or, on information and belief, the VAN), on information and belief, a limited-duration card expiration date (*e.g.*, an expiration date associated with the DAN or, on information and belief, of the VAN), and a limited-use card security code. (*e.g.*, the dynamic security code), and conveys the limited-use payment information to complete an online transaction. *See supra* limitation 11[i], 11[j], 15[h].  PKPaymentToken Object Transaction ID Payment network Payment token data Signature Header Encrypted Payment data Amount Cardholder name Payment processing data  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.

Claim Language	Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card



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:

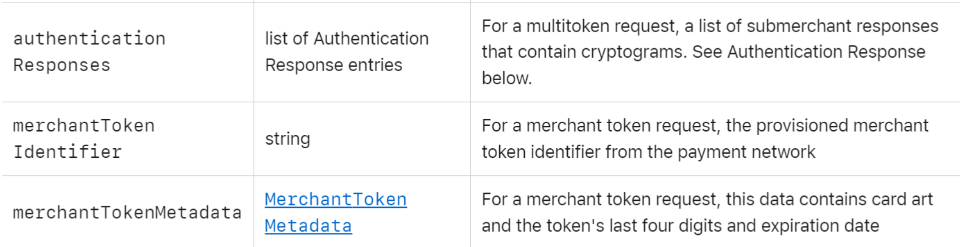
Key	Value	Description
data	payment data dictionary, Base64 encoded as a string	Encrypted payment data See Payment Data Keys below for the decrypted payment data keys and values.
header	header dictionary	Additional version-dependent information you use to decrypt and verify the payment See Header Keys and Values below.
signature	detached PKCS #7 signature, Base64 encoded as a string	Signature of the payment and header data The signature includes the signing certificate, its intermediate CA certificate, and information about the signing algorithm.
version	string	Version information about the payment token The token uses EC_v1 for ECC-encrypted data and RSA_v1 for RSA-encrypted data.

Payment data keys

The decrypted payment data in the data value contains the following keys and values:

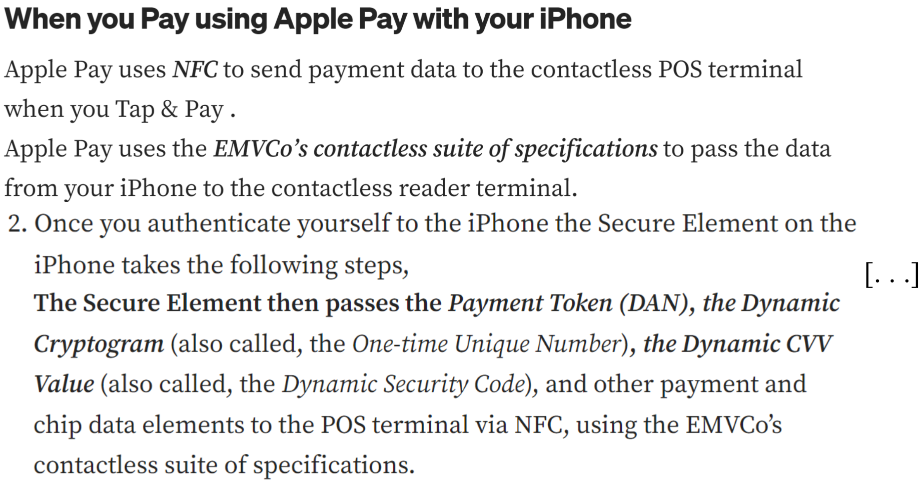
Key	Value	Description
applicationPrimaryAccountNumber	string	Device-specific account number of the card that funds this transaction
applicationExpirationDate	date as a string	Card expiration date in the format YYMMDD
currencyCode	string	ISO 4217 numeric currency code, as a string to preserve leading zeros
transactionAmount	number	Transaction amount
cardholderName	string	Optional. Cardholder name.
deviceManufacturerIdentifier	string	Hex-encoded device manufacturer identifier
paymentDataType	string	Either "3DSecure" or "EMV"
paymentData	payment data dictionary	Detailed payment data; see Detailed Payment Data Keys (3D Secure) and Detailed Payment Data Keys (EMV) below

Claim Language	Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card



`authenticationResponses`	list of Authentication Response entries	For a multitoken request, a list of submerchant responses that contain cryptograms. See Authentication Response below.
`merchantTokenIdentifier`	string	For a merchant token request, the provisioned merchant token identifier from the payment network
`merchantTokenMetadata`	`MerchantTokenMetadata`	For a merchant token request, this data contains card art and the token's last four digits and expiration date

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; *PKPayment*, Apple Developer, https://developer.apple.com/documentation/passkit_apple_pay_and_wallet/pkpayment.



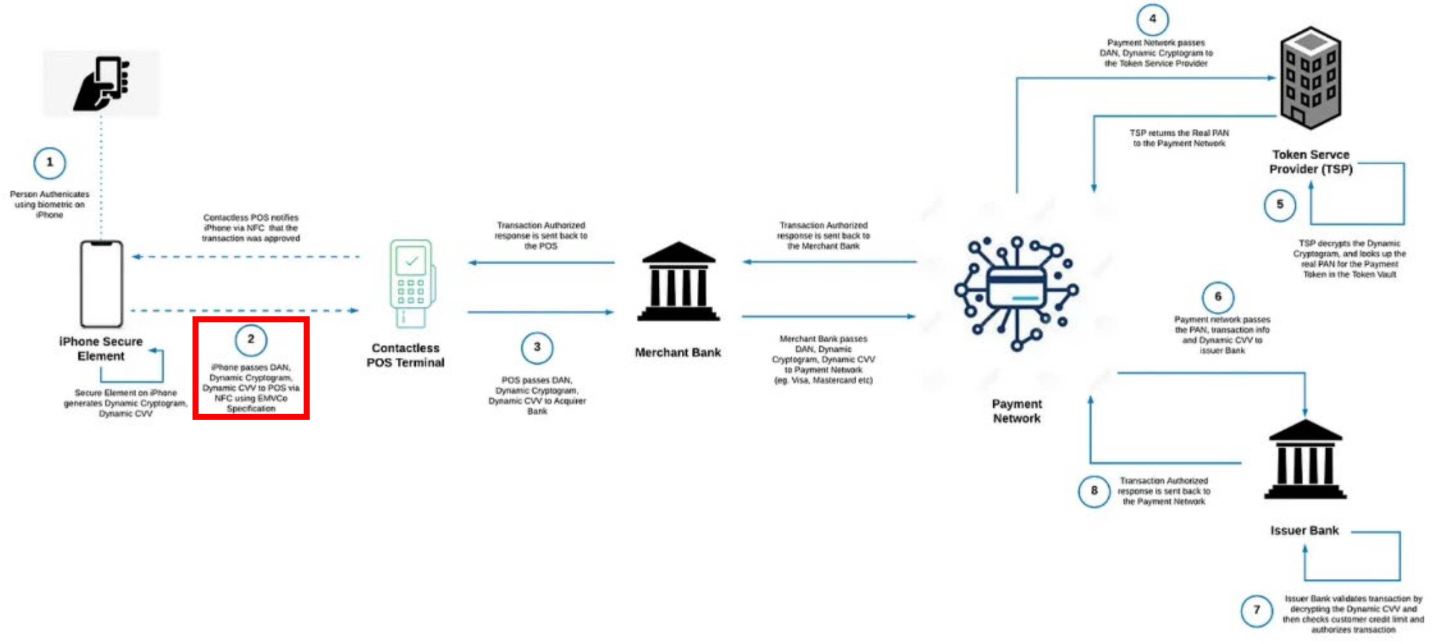
When you Pay using Apple Pay with your iPhone

Apple Pay uses ***NFC*** to send payment data to the contactless POS terminal when you Tap & Pay .

Apple Pay uses the ***EMVCo's contactless suite of specifications*** to pass the data from your iPhone to the contactless reader terminal.

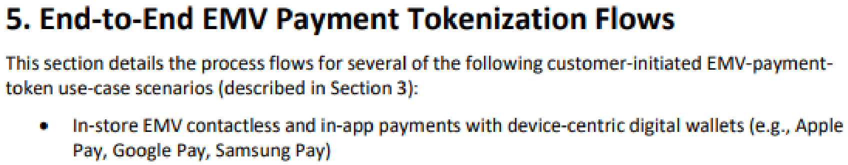
2. Once you authenticate yourself to the iPhone the Secure Element on the iPhone takes the following steps, [. . .] **The Secure Element then passes the *Payment Token (DAN)*, *the Dynamic Cryptogram*** (also called, the *One-time Unique Number*)**, *the Dynamic CVV Value*** (also called, the *Dynamic Security Code*), and other payment and chip data elements to the POS terminal via NFC, using the EMVCo's contactless suite of specifications.

<table>
<tr><th>Claim Language</th><th>Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card</th></tr>
<tr><td></td><td>


4
Payment Network passes DAN, Dynamic Cryptogram to the Token Service Provider
TSP returns the Real PAN to the Payment Network
Token Servce Provider (TSP)
5
TSP decrypts the Dynamic Cryptogram, and looks up the real PAN for the Payment Token in the Token Vault
1
Person Authenicates using biometric on iPhone
Contactless POS notifies iPhone via NFC that the transaction was approved
Transaction Authorized response is sent back to the POS
Transaction Authorized response is sent back to the Merchant Bank
iPhone Secure Element
Secure Element on iPhone generates Dynamic Cryptogram, Dynamic CVV
2
iPhone passes DAN, Dynamic Cryptogram, Dynamic CVV to POS via NFC using EMVCo Specification
Contactless POS Terminal
3
POS passes DAN, Dynamic Cryptogram, Dynamic CVV to Acquirer Bank
Merchant Bank
Merchant Bank passes DAN, Dynamic Cryptogram, Dynamic CVV to Payment Network (eg. Visa, Mastercard etc)
6
Payment network passes the PAN, transaction info and Dynamic CVV to issuer Bank
Payment Network
8
Transaction Authorized response is sent back to the Payment Network
Issuer Bank
7
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, *How Apple Pay works under the hood?*, codeburst (Nov. 5, 2019), https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7.



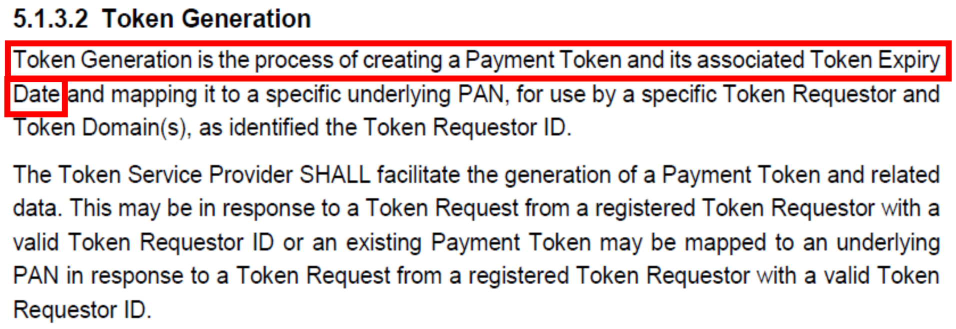
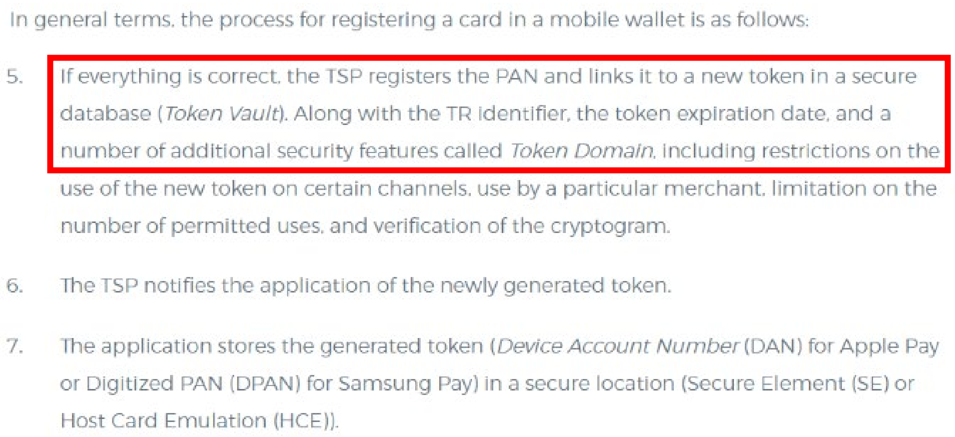
5. End-to-End EMV Payment Tokenization Flows

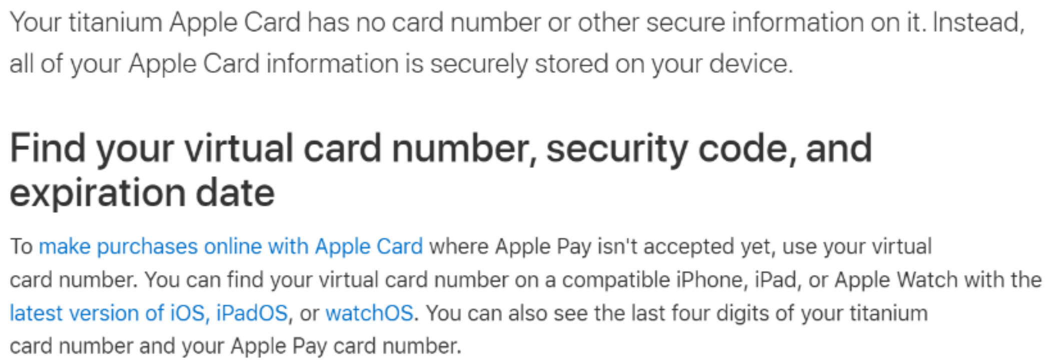
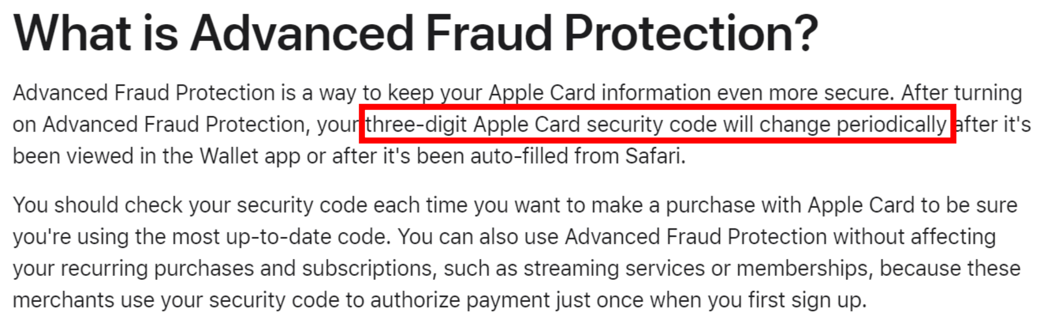
This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):

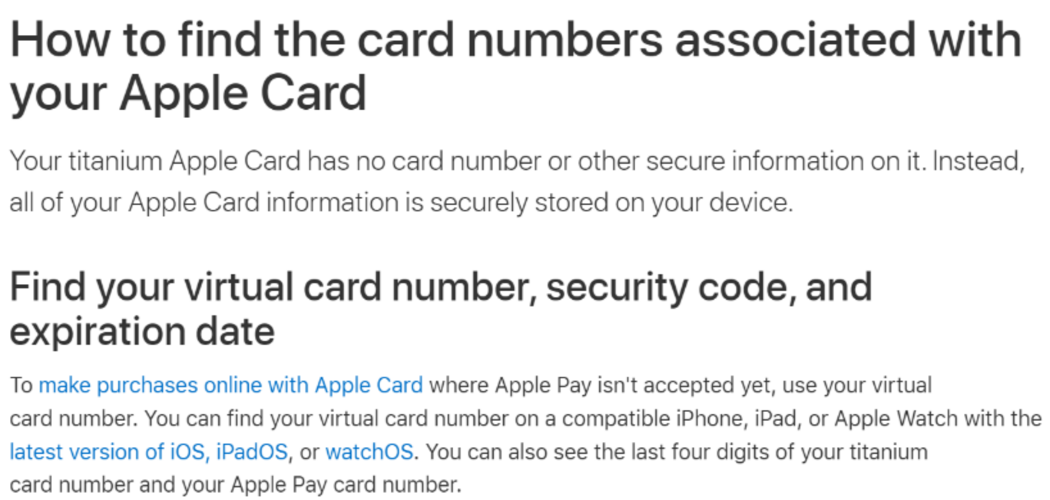
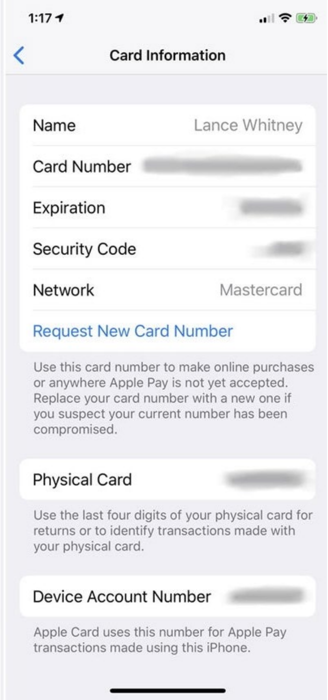
- In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)

See, e.g., US Payments Forum, *EMV Payment Tokenization Primer and Lessons Learned* at 19-21, 23 (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.").

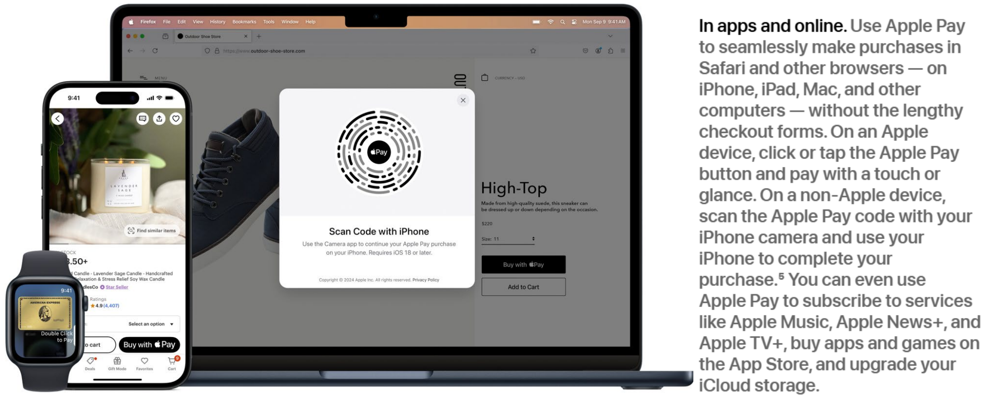
</td></tr>
</table>

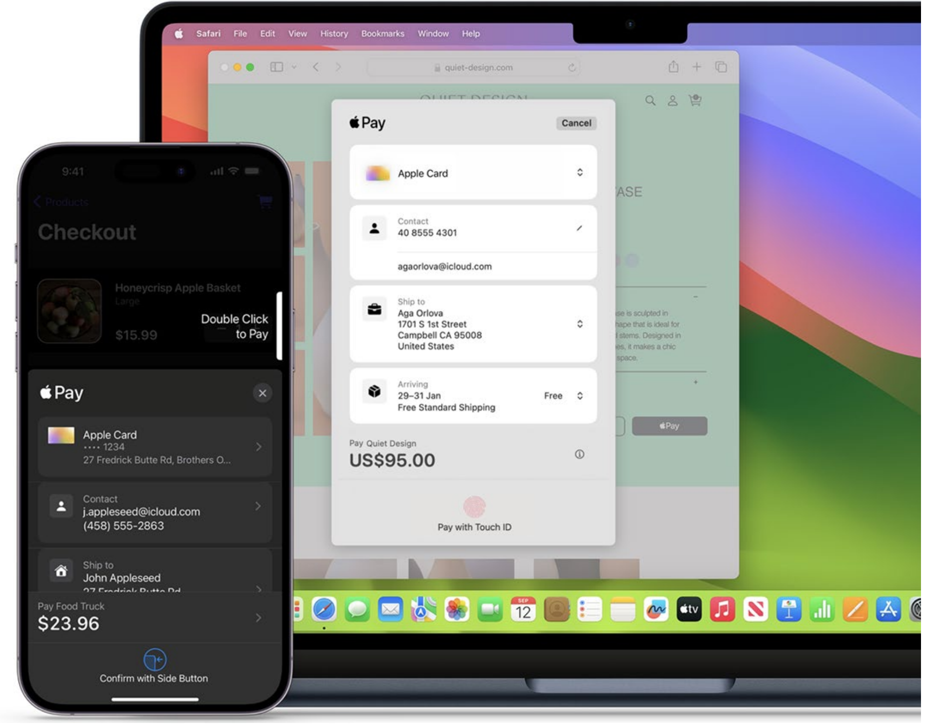
Claim Language	Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card
	 **5.1.3.2 Token Generation** Token Generation is the process of creating a Payment Token and its associated Token Expiry Date and mapping it to a specific underlying PAN, for use by a specific Token Requestor and 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, *EMV® Payment Tokenisation Specification – Technical Framework v2.1* 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 (*Token Vault*). Along with the TR identifier, the token expiration date, and a number of additional security features called *Token Domain*, 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 (*Device Account Number* (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.*, *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.

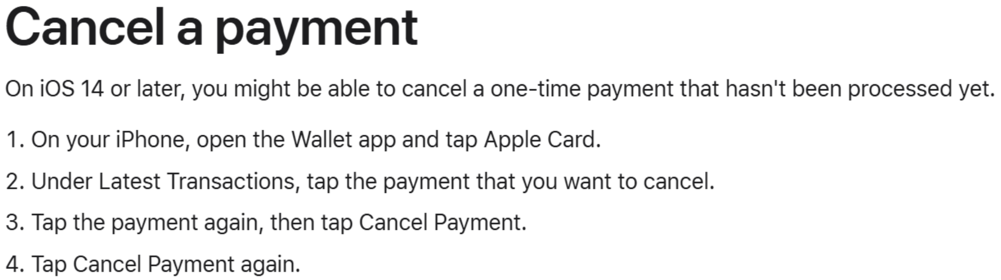
Claim Language	Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card
	 Your titanium Apple Card has no card number or other secure information on it. Instead, all of your Apple Card information is securely stored on your device. Find your virtual card number, security code, and expiration 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. *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.  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.*, *Use Advanced Fraud Protection with Apple Card*, Apple (Dec. 17, 2024), https://support.apple.com/en-us/102427.

Claim Language	**Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card**
	 How to find the card numbers associated with your Apple Card Your titanium Apple Card has no card number or other secure information on it. Instead, all of your Apple Card information is securely stored on your device. 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.  1:17 Card Information Name Lance Whitney Card Number [redacted] Expiration [redacted] Security Code [redacted] Network Mastercard Request New Card Number Use this card number to make online purchases or anywhere Apple Pay is not yet accepted. Replace your card number with a new one if you suspect your current number has been compromised. Physical Card [redacted] Use the last four digits of your physical card for returns or to identify transactions made with your physical card. Device Account Number [redacted] Apple Card uses this number for Apple Pay transactions made using this iPhone. *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; *see, e.g.*, Lance Whitney, *How to use your Apple Card without Apple Pay*, TechRepublic (Oct. 1, 2019), https://www.techrepublic.com/article/how-to-use-your-apple-card-without-apple-pay/; Andrew O'Hara, *Tips and tricks for mastering Apple Card*, AppleInsider (Aug. 20, 2019), https://appleinsider.com/articles/19/08/20/tips-and-tricks-for-mastering-apple-card ("If you want to use your Apple Card online, and the retailer doesn't support Apple Pay or autofill in Safari, you have to manually enter in your card number. Those details can be readily found within the Wallet app.").
19[a] The system of claim 15 wherein the computing device is operable to generate a limited-use card security code number, for use in place of a card issuers card security code by generating said limited-use number via cryptographically combining information from at least one of a set comprising: a user information; an internet	An Apple Pay or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—generates a limited-use card security code number (*e.g.*, the dynamic security code), for use in place of a card issuers card security code (*e.g.*, CVV associated with the PAN) by generating said limited-use number via cryptographically combining information from at least one of a set comprising, on information and belief, a user information; an internet address; an email address; a device transaction sequence counter (*e.g.*, on information and belief, a transaction counter); a device account number; device identifiers; device secrets; device keys; issuer secrets; issuer keys (*e.g.*, a CVV-key); a payment card account number; a payment card security code; a time; an expiration date; an amount; a merchant locality; a transaction information; and a cryptographic combination of at least two of the above set. *See supra* limitation 11[i], 11[j], 13[c].

Claim Language	**Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card**
address; an email address; a device transaction sequence counter; a device account number; device identifiers; device secrets; device keys; issuer secrets; issuer keys; a payment card account number; a payment card security code; a time; an expiration date; an amount; a merchant locality; a transaction information; and a cryptographic combination of at least two of the above set, and	
19[b] wherein the computing device is operable to display the generated limited-use card security code on the display.	An Apple Pay or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—displays the generated limited-use card security code (*e.g.*, dynamic security code) on the display. *See supra* limitation 13[a].
20[a] The system of claim 15 wherein the computing device is further operable to obtain a user payment approval through at least one user-interface element of the computing device, from a set comprising: a display interface, a touch-screen interface, a touch ID button, input buttons, a touch key-pad, a key-pad, a key-board, an optical sensor array, a	An Apple Pay or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—obtains a user payment approval (*e.g.*, double-clicking the side button or Home button or selecting a payment method and authenticating with passcode, password, Face ID, Touch ID, or wrist detection, or, on information and belief, Optic ID) through at least one user-interface element of the computing device, from a set comprising: a display interface, a touch-screen interface (*e.g.*, passcode, password), a touch ID button (*e.g.*, Touch ID), input buttons (*e.g.*, side button double-click or Home button), a touch key-pad, a key-pad, a key-board (*e.g.*, passcode, password), an optical sensor array, a motion detection unit, an accelerometer, the swiping of a recognized user skin over a device sensor array, a biometric sensor (*e.g.*, Face ID and, on information and belief, Optic ID), a wireless interface, an NFC interface, an RF interface, a device biometric sensing the device is continuously remaining in contact with a valid user (*e.g.*, wrist detection). *See supra* limitations 11[g], 15[h].

Claim Language	**Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card**
motion detection unit, an accelerometer, the swiping of a recognized user skin over a device sensor array, a biometric sensor, a wireless interface, an NFC interface, an RF interface, a device biometric sensing the device is continuously remaining in contact with a valid user; and,	
20[b] wherein the computing device is operable to display at least one of a set comprising: the transaction information, the merchant information, the time, the location of the transaction, the payment bank logo, the card issuer icon, the payment card image, and the amount, on a display of the computing device, and,	An Apple Pay or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—displays at least one of a set comprising: the transaction information, the merchant information, the time, the location of the transaction, the payment bank logo, the card issuer icon, the payment card image, and the amount, on a display of the computing device  Scan Code with iPhone High-Top Buy with Pay Add to Cart Double Click to Pay **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.*, *Apple Pay*, Apple, https://www.apple.com/apple-pay/ (last visited Dec. 30, 2024); John M Evans, *Apple Pay History*, Apple Community (Aug. 23, 2021 1:02 PM), https://discussions.apple.com/thread/253075944?sortBy=rank.

Claim Language	**Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card**
	 9:41 Checkout Honeycrisp Apple Basket $15.99 Double Click to Pay Pay Apple Card •••• 1234 27 Fredrick Butte Rd, Brothers O... Contact j.appleseed@icloud.com (458) 555-2863 Ship to John Appleseed Pay Food Truck $23.96 Confirm with Side Button Safari File Edit View History Bookmarks Window Help quiet-design.com Pay Cancel Apple Card Contact 40 8555 4301 agaorlova@icloud.com Ship to Aga Orlova 1701 S 1st Street Campbell CA 95008 United States Arriving 29–31 Jan Free Standard Shipping Free Pay Quiet Design US$95.00 Pay with Touch ID *See, e.g.*, Apple, *Apple Pay Merchant Integration Guide* at 3 (Jan. 2024) *available at* http://developer.apple.com/apple-pay/Apple-Pay-Merchant-Integration-Guide.pdf; *Get started with Apple Pay on the Web*, Apple Developer, https://developer.apple.com/videos/play/tech-talks/111381/.
20[c] a user input providing for at least one user action from a set comprising: an approving of a transaction, a denying of a transaction, and an adjusting of a transaction, via the user-interface.	An Apple Pay or Apple Wallet-enabled computing device—such as a smartphone, smartwatch, tablet, laptop or desktop computer, or spatial computer—obtains a user input providing for at least one user action from a set comprising: an approving of a transaction (*e.g.*, by confirming the payment and authorizing), a denying of a transaction (*e.g.*, cancelling the payment or closing out of the browser or application), and an adjusting of a transaction, via the user-interface. *See supra* claim 20[a].

Claim Language	Apple Pay and/or Apple Wallet-Enabled Computing Device with Apple Card
	 **Cancel a payment** On iOS 14 or later, you might be able to cancel a one-time payment that hasn't been processed yet. 1. On your iPhone, open the Wallet app and tap Apple Card. 2. Under Latest Transactions, tap the payment that you want to cancel. 3. Tap the payment again, then tap Cancel Payment. 4. Tap Cancel Payment again. *See, e.g.*, *How to make Apple Card payments*, Apple (Dec. 16, 2024), https://support.apple.com/en-us/102534.

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 '820 Patent and all processes employed by Defendants that practice the methods claimed by the'820 Patent, consisting of at least Defendant's payment cards and products that support Apple Pay (alone or with Apple Wallet), including the following Apple-branded payment cards, smartphones, smartwatches, tablets, laptop computers, desktop computers, spatial computers, and accessories.[1]

I. Accused Payment Cards

The accused payment cards include the Apple Card.

II. 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

[1] *See, e.g.*, *Devices compatible with Apple Pay*, Apple (Nov. 22, 2024), https://support.apple.com/en-us/102896; https://www.apple.com/apple-card/ (last visited Dec. 30, 2024).

[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/.

Product	**Model No.**		**Product**	**Model No.**
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").

III. <u>Accused Smartwatches</u>

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

[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 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
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.

IV. <u>Accused Tablets</u>

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

[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 (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
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.

V. <u>Accused Laptop Computers</u>

The accused laptop computers include Mac models with Touch ID, Mac models introduced in 2012 or later with an Apple Pay-enabled iPhone or Apple Watch, and Mac models with Apple silicon that are paired with a Magic Keyboard with Touch ID.[5]

Product	Model No.		Product	Model No.
MacBook Pro (14-inch, Nov 2023)	Mac15,3, MR7J3xx/A, MR7K3xx/A, MRX23xx/A, MTL73xx/A, MTL83xx/A, MTLC3xx/A, MXE03xx/A, MXE13xx/A		MacBook Pro (Retina, 13-inch, Late 2013)*	MacBookPro11,1, ME864xx/A, ME865xx/A, ME866xx/A
MacBook Pro (14-inch, Nov 2023)	Mac15,6, Mac15,8, Mac15,10, FRX33xx/A, FRX43xx/A, FRX54xx/A, FRX63xx/A, FRX73xx/A, FRX83xx/A, MRX33xx/A, MRX43xx/A, MRX53xx/A, MRX63xx/A, MRX73xx/A, MRX83xx/A		MacBook Pro (Retina, 15-inch, Early 2013)*	MacBookPro10,1, ME664xx/A, ME665xx/A

[5] *See, e.g.*, *Mac computers with Apple silicon*, Apple (Sept. 18, 2024), https://support.apple.com/en-us/116943; *Identify your MacBook Pro model*, Apple (Nov. 8, 2024), https://support.apple.com/en-us/108052; *Identify your MacBook Air model*, Apple (Sept. 16, 2024), https://support.apple.com/en-us/102869.

Product	**Model No.**		**Product**	**Model No.**
MacBook Pro (16-inch, Nov 2023)	Mac15,7, Mac15,9, Mac15,11; FRW13xx/A, FRW23xx/A, FRW33xx/A, FRW43xx/A, FRW63xx/A, FRW73xx/A, FUW63xx/A, FUW73xx/A, MRW13xx/A, MRW23xx/A, MRW33xx/A, MRW43xx/A, MRW63xx/A, MRW73xx/A		MacBook Pro (Retina, 13-inch, Early 2013)*	MacBookPro10,2, MD212xx/A, ME662xx/A
MacBook Pro (14-inch, 2023)	Mac14,5, Mac14,9, MPHE3xx/A, MPHF3xx/A, MPHG3xx/A, MPHH3xx/A, MPHJ3xx/A, MPHK3xx/A		MacBook Pro (Retina, 13-inch, Late 2012)*	MacBookPro10,2, MD212xx/A, MD213xx/A
MacBook Pro (16-inch, 2023)	Mac14,6, Mac14,10, MNWG3xx/A, MNW93xx/A, MNWK3xx/A, MNWD3xx/A, MNWF3xx/A, MNW83xx/A, MNWJ3xx/A, MNWC3xx/A		MacBook Pro (Retina, 15-inch, Mid 2012)*	MacBookPro10,1
MacBook Pro (13-inch, M2, 2022)	Mac14,7, MNEH3xx/A, MNEJ3xx/A, MNEP3xx/A, MNEQ3xx/A		MacBook Pro (15-inch, Mid 2012)*	MacBookPro9,1, MD103xx/A, MD104xx/A
MacBook Pro (14-inch, 2021)	MacBookPro18,3, MacBookPro18,4, MKGP3xx/A, MKGQ3xx/A, MKGR3xx/A, MKGT3xx/A		MacBook Pro (13-inch, Mid 2012)*	MacBookPro9,2, MD101xx/A, MD102xx/A
MacBook Pro (16-inch, 2021)	MacBookPro18,1, MacBookPro18,2, MK183xx/A, MK193xx/A, MK1A3xx/A, MK1E3xx/A, MK1F3xx/A, MK1H3xx/A		MacBook Air (15-inch, M3, 2024)	Mac15,13, MRYM3xx/A, MRYP3xx/A, MRYR3xx/A, MRYU3xx/A, MRYN3xx/A, MRYQ3xx/A, MRYT3xx/A, MRYV3xx/A, MXD13xx/A, MXD23xx/A, MXD33xx/A, MXD43xx/A
MacBook Pro (13-inch, M1, 2020)	MacBookPro17,1, MYD83xx/A, MYD92xx/A, MYDA2xx/A, MYDC2xx/A		MacBook Air (13-inch, M3, 2024)	Mac15,12, MRXN3xx/A, MRXQ3xx/A, MRXT3xx/A, MRXV3xx/A, MRXP3xx/A, MRXR3xx/A, MRXU3xx/A, MRXW3xx/A, MXCR3xx/A, MXCT3xx/A, MXCU3xx/A, MXCV3xx/A
MacBook Pro (13-inch, 2020, Two Thunderbolt 3 ports)	MacBookPro16,3, MXK32xx/A, MXK52xx/A, MXK62xx/A, MXK72xx/A		MacBook Air (15-inch, M2, 2023)	Mac14,15, MQKP3xx/A, MQKQ3xx/A, MQKR3xx/A, MQKT3xx/A, MQKU3xx/A, MQKV3xx/A, MQKW3xx/A, MQKX3xx/A
MacBook Pro (13-inch, 2020, Four Thunderbolt 3 ports)	MacBookPro16,2, MWP42xx/A, MWP52xx/A, MWP62xx/A, MWP72xx/A, MWP82xx/A		MacBook Air (M2, 2022)	Mac14,2, MLXW3xx/A, MLXX3xx/A, MLXY3xx/A, MLY03xx/A, MLY13xx/A, MLY23xx/A, MLY33xx/A, MLY43xx/A

Product	**Model No.**		**Product**	**Model No.**
MacBook Pro (16-inch, 2019)	MacBookPro16,1, MacBookPro16,4, MVVJ2xx/A, MVVK2xx/A, MVVL2xx/A, MVVM2xx/A		MacBook Air (M1, 2020)	MacBookAir10,1, MGN63xx/A, MGN93xx/A, MGND3xx/A, MGN73xx/A, MGNA3xx/A, MGNE3xx/A
MacBook Pro (13-inch, 2019, Two Thunderbolt 3 ports)	MacBookPro15,4, MUHN2xx/A, MUHP2xx/a, MUHQ2xx/A, MUHR2xx/A, MUHR2xx/B		MacBook Air (Retina, 13-inch, 2020)	MacBookAir9,1, MVH22xx/A, MVH42xx/A, MVH52xx/A, MWTJ2xx/A, MWTK2xx/A, MWTL2xx/A
MacBook Pro (15-inch, 2019)	MacBookPro15,1, MacBookPro15,3, MV902xx/A, MV912xx/A, MV922xx/A, MV932xx/A, MV942xx/A, MV952xx/A		MacBook Air (Retina, 13-inch, 2019)	MacBookAir8,2, MVFH2xx/A, MVFJ2xx/A, MVFK2xx/A, MVFL2xx/A, MVFM2xx/A, MVFN2xx/A, MVH62xx/A, MVH82xx/A
MacBook Pro (13-inch, 2019, Four Thunderbolt 3 ports)	MacBookPro15,2, MV962xx/A, MV972xx/A, MV982xx/A, MV992xx/A, MV9A2xx/A		MacBook Air (Retina, 13-inch, 2018)	MacBookAir8,1, MRE82xx/A, MREA2xx/A, MREE2xx/A, MRE92xx/A, MREC2xx/A, MREF2xx/A, MUQT2xx/A, MUQU2xx/A, MUQV2xx/A
MacBook Pro (15-inch, 2018)	MacBookPro15,1, MR932xx/A, MR942xx/A, MR952xx/A, MR962xx/A, MR972xx/A, MUQH2xx/A		MacBook Air (13-inch, 2017)*	MacBookAir7,2, MQD32xx/A, MQD42xx/A, MQD52xx/A
MacBook Pro (13-inch, 2018, Four Thunderbolt 3 ports)	MacBookPro15,2, MR9Q2xx/A, MR9R2xx/A, MR9T2xx/A, MR9U2xx/A, MR9V2xx/A		MacBook Air (13-inch, Early 2015)*	MacBookAir7,2, Part Numbers: MJVE2xx/A, MJVG2xx/A, MMGF2xx/A, MMGG2xx/A
MacBook Pro (15-inch, 2017)	MacBookPro14,3, MPTR2xx/A, MPTT2xx/A, MPTU2xx/A, MPTV2xx/A, MPTW2xx/A, MPTX2xx/A		MacBook Air (11-inch, Early 2015)*	MacBookAir7,1, MJVM2xx/A, MJVP2xx/A
MacBook Pro (13-inch, 2017, Four Thunderbolt 3 ports)	MacBookPro14,2, MPXV2xx/A, MPXW2xx/A, MPXX2xx/A, MPXY2xx/A, MQ002xx/A, MQ012xx/A		MacBook Air (13-inch, Early 2014)*	MacBookAir6,2, MD760xx/B, MD761xx/B
MacBook Pro (13-inch, 2017, Two Thunderbolt 3 ports)	MacBookPro14,1, MPXQ2xx/A, MPXR2xx/A, MPXT2xx/A, MPXU2xx/A		MacBook Air (11-inch, Early 2014)*	MacBookAir6,1, MD711xx/B, MD712xx/B
MacBook Pro (15-inch, 2016)*	MacBookPro13,3, MLH32xx/A, MLH42xx/A, MLH52xx/A, MLW72xx/A, MLW82xx/A, MLW92xx/A		MacBook Air (13-inch, Mid 2013)*	MacBookAir6,2, MD760xx/A, MD761xx/A
MacBook Pro (13-inch, 2016, Four	MacBookPro13,2, MLH12xx/A, MLVP2xx/A, MNQF2xx/A,		MacBook Air (11-inch, Mid 2013)*	MacBookAir6,1, MD711xx/A, MD712xx/A

Product	**Model No.**		**Product**	**Model No.**
Thunderbolt 3 ports)*	MNQG2xx/A, MPDK2xx/A, MPDL2xx/A			
MacBook Pro (13-inch, 2016, Two Thunderbolt 3 ports)*	MacBookPro13,1, MLL42xx/A, MLUQ2xx/A		MacBook Air (13-inch, Mid 2012)*	MacBookAir5,2, MD231xx/A, MD232xx/A
MacBook Pro (Retina, 15-inch, Mid 2015)*	MacBookPro11,4, MacBookPro11,5, MJLQ2xx/A, MJLT2xx/A, MJLU2xx/A		MacBook Air (11-inch, Mid 2012)*	MacBookAir5,1, MD223xx/A, MD224xx/A
MacBook Pro (Retina, 13-inch, Early 2015)*	MacBookPro12,1, MF839xx/A, MF840xx/A, MF841xx/A, MF843xx/A		MacBook (Retina, 12-inch, 2017)	MacBook10,1, MNYF2XX/A, MNYG2XX/A, MNYH2XX/A, MNYJ2XX/A, MNYK2XX/A, MNYL2XX/A, MNYM2XX/A, MNYN2XX/A
MacBook Pro (Retina, 15-inch, Mid 2014)*	MacBookPro11,2, MacBookPro11,3, MGXC2xx/A, MGXA2xx/A		MacBook (Retina, 12-inch, Early 2016)*	MacBook9,1, MLH72xx/A, MLH82xx/A, MLHA2xx/A, MLHC2xx/A, MLHE2xx/A, MLHF2xx/A, MMGL2xx/A,
MacBook Pro (Retina, 13-inch, Mid 2014)*	MacBookPro11,1, MGX72xx/A, MGX82xx/A, MGX92xx/A		MacBook (Retina, 12-inch, Early 2015)*	MacBook8,1, MF855xx/A, MF865xx/A, MJY32xx/A, MJY42xx/A, MK4M2xx/A, MK4N2xx/A
MacBook Pro (Retina, 15-inch, Late 2013)*	MacBookPro11,2, MacBookPro11,3, ME293xx/A, ME294xx/A			

*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.

VI. <u>Accused Desktop Computers</u>

The accused desktop computers include Mac models with Touch ID, Mac models introduced in 2012 or later with an Apple Pay-enabled iPhone or Apple Watch, and Mac models with Apple silicon that are paired with a Magic Keyboard with Touch ID.[6]

Product	**Model No.**		**Product**	**Model No.**
iMac (24-inch, 2023)	Mac15,5, MQRJ3xx/A, MQRK3xx/A, MQRL3xx/A, MQRM3xx/A,		iMac (21.5-inch, Late 2013)*	iMac14,1, ME086xx/A, ME087xx/A

[6] *See, e.g.*, *Mac computers with Apple silicon*, Apple (Sept. 18, 2024), https://support.apple.com/en-us/116943; *Identify your iMac model*, Apple (Nov. 8, 2024), https://support.apple.com/en-us/108054; *Identify your Mac mini model*, Apple (Dec. 10, 2024), https://support.apple.com/en-us/102852; *Identify your Mac Studio model*, Apple (Sept. 16, 2024), https://support.apple.com/en-us/102231; *Identify your Mac Pro Model*, Apple (Sept. 16, 2024), https://support.apple.com/en-us/102887.

Product	**Model No.**		**Product**	**Model No.**
	MQRN3xx/A, MQRP3xx/A, MQRQ3xx/A, MQRR3xx/A, MQRT3xx/A, MQRU3xx/A, MQRV3xx/A, MQRW3xx/A, MQRX3xx/A, MQRY3xx/A			
iMac (24-inch, 2023)	Mac15,4, MQR93xx/A, MQRA3xx/A, MQRC3xx/A, MQRD3xx/A		iMac (27-inch, Late 2012)*	iMac13,2, MD095xx/A, MD096xx/A
iMac (24-inch, M1, 2021)	iMac21,1, MGPC3xx/A, MGPD3xx/A, MGPF3xx/A, MGPG3xx/A, MGPH3xx/A, MGPJ3xx/A, MGPK3xx/A, MGPL3xx/A, MGPM3xx/A, MGPN3xx/A, MGPP3xx/A, MGPQ3xx/A, MGPR3xx/A, MGPT3xx/A		iMac (21.5-inch, Late 2012)*	iMac13,1, MD093xx/A, MD094xx/A
iMac (24-inch, M1, 2021)	iMac21,2, MGTF3xx/a, MJV83xx/a, MJV93xx/a, MJVA3xx/a		Mac mini (2023)	Mac14,3, MMFJ3xx/A, MMFK3xx/A
iMac (Retina 5K, 27-inch, 2020)	iMac20,1, iMac20,2, MXWT2xx/A, MXWU2xx/A, MXWV2xx/A		Mac mini (2023)	Mac14,12, MNH73xx/A
iMac (Retina 5K, 27-inch, 2019)	iMac19,1, MRQYxx/A, MRR0xx/A, MRR1xx/A		Mac mini (M1, 2020)	Macmini9,1, MGNR3xx/A, MGNT3xx/A
iMac (Retina 4K, 21.5-inch, 2019)	iMac19,2, MRT3xx/A, MRT4xx/A, MHK23xx/A		Mac mini (2018)	Macmini8,1, MRTR2xx/A, MRTT2xx/A, MXNF2xx/A, MXNG2xx/A
iMac Pro	iMacPro1,1, MQ2Y2xx/A, MHLV3xx/A		Mac mini (Late 2014)*	Macmini7,1, MGEM2xx/A, MGEN2xx/A, MGEQ2xx/A
iMac (Retina 5K, 27-inch, 2017)	iMac18,3, MNE92xx/A, MNEA2xx/A, MNED2xx/A		Mac mini (Late 2012)*	Macmini6,1; Macmini6,2, MD387xx/A; MD388xx/A, MD389xx/A
iMac (Retina 4K, 21.5-inch, 2017)	iMac18,2, MNDY2xx/A, MNE02xx/A		Mac Studio (2023)	Mac14,13, MQH73xx/A
iMac (21.5-inch, 2017)	iMac18,1, MMQA2xx/A, MHK03xx/A		Mac Studio (2023)	Mac14,14, MQH63xx/A
iMac (Retina 5K, 27-inch, Late 2015)*	iMac17,1, MK462xx/A, MK472xx/A, MK482xx/A		Mac Studio (2022)	Mac13,1, MJMV2xx/a
iMac (Retina 4K, 21.5-inch, Late 2015)*	iMac16,2, MK452xx/A		Mac Studio (2022)	Mac13,2, MJMW3xx/a
iMac (21.5-inch, Late 2015)*	iMac16,1, MK142xx/A, MK442xx/A		Mac Pro (2023)	Mac14,8
iMac (Retina 5K, 27-inch, Mid 2015)*	iMac15,1, MF885xx/A		Mac Pro (Rack, 2023)	Mac14,8

Product	**Model No.**		**Product**	**Model No.**
iMac (Retina 5K, 27-inch, Late 2014)*	iMac15,1, MF886xx/A		Mac Pro (Late 2013)	MacPro6,1, ME253xx/A, MD878xx/A
iMac (21.5-inch, Mid 2014)*	iMac14,4, MF883xx/A, MG022xx/A		Mac Pro (Mid 2012)*	MacPro5,1, MD770xx/A, MD771xx/A
iMac (27-inch, Late 2013)*	iMac14,2, ME086xx/A, ME088xx/A		Mac Pro Server (Mid 2012)*	MacPro5,1, MD772xx/A

*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.

VII. Accused Spatial Computers

The accused spatial computers include the Apple Vision Pro.

Product	**Model No.**
Vision Pro	RealityDevice14,1, A2117, MQL83LL/A, MQL93LL/A, MQLA3LL/A

VIII. Accused Accessories

The accused accessories include a Magic Keyboard with Touch ID.[7]

Product	**Model No.**
Magic Keyboard with Touch ID (2nd generation)	A2449
Magic Keyboard with Touch ID and Numeric Keypad (2nd generation)	A2520
Magic Keyboard with Touch ID (1st generation)	A1644
Magic Keyboard with Touch ID and Numeric Keypad (1st generation)	A1843

[7] *Mac computers with Apple silicon*, Apple (Sept. 18, 2024), https://support.apple.com/en-us/116943.