

Exhibit C to CardWare’s Preliminary Infringement Contentions
Infringement of U.S. Patent No. 11,176,538

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 Google LLC (“Google” or “Defendant”), including technical documentation such as schematics and datasheets, and source code.

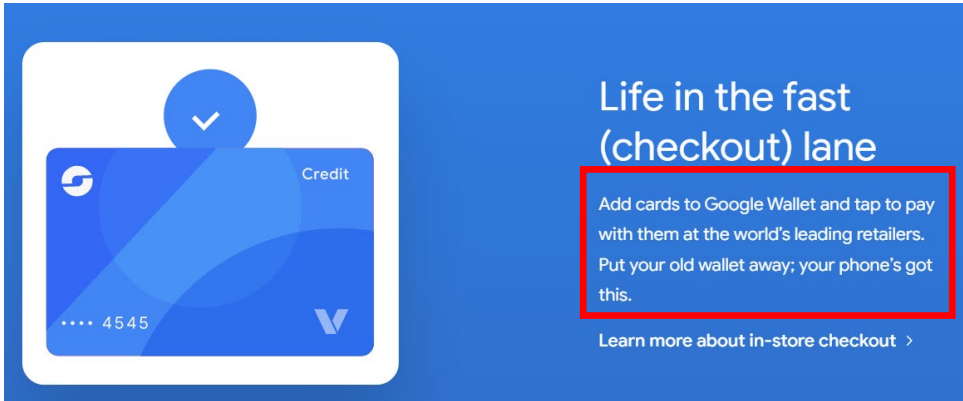
Google infringed and continues to infringe U.S. Patent No. 11,176,538 (the “’538 patent”) by making, using, selling or offering for sale, and/or importing into the United States devices and applications implementing a method of performing a transaction, covered by one or more claims of the ’538 patent. CardWare’s allegations include all such devices, unless otherwise noted or prohibited by license (“Accused Products”). *See infra* Appendix. Google has also infringed by performing such transactions and/or contributing to and/or inducing infringement by others, for the reasons set forth herein.

To the extent certain acts or steps constituting part of the infringement are performed by another entity besides Google (*e.g.*, a third party payment processor or token service provider), those acts may be attributed to Google because Google and the other entity, or entities, are acting in a joint enterprise with respect to the infringement, or, in the alternative, Google 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 ’538 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 preliminary infringement contentions.

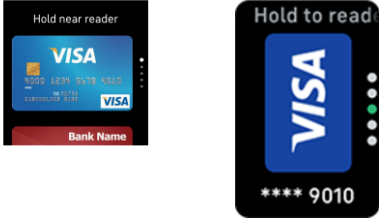
I. Claim 1 and Dependent Claims 2–18

Claim No.	Accused Products
1[pre] A method of performing a payment transaction, the method comprising:	<p>To the extent the preamble is limiting, a Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone or smartwatch, performs a method of performing a payment transaction comprising the following limitations.</p> <div>  <div> <h3>Takeaways</h3> <ul style="list-style-type: none"> Pixel is powered by all the smarts of Google, including the Tensor chip Ask Google Assistant to make a call from your Pixel Buds, so you can keep your hands free¹ Google apps come loaded on every Pixel, including Google Maps to help you get to your destination,² and Google Wallet to give you an easy way to pay when you arrive³ </div> </div> <p>Get help paying the tab [. . .]</p> <div> <p>Knox picked up the bill and paid with Google Wallet, which lets you store your credit and debit cards and pay quickly from your Pixel phone or Pixel Watch.³</p> <p>See, e.g., Google Pixel 9 Pro Fold, https://store.google.com/config/pixel_9_pro_fold; <i>An even better way to use your favorite Google apps.</i>, Google, https://store.google.com/intl/en/ideas/articles/google-software-features/; <i>Install and update apps on Google Pixel Watch</i>, Google, https://support.google.com/googlepixelwatch/answer/13044412 (“Google Pixel Watch 2 is preloaded with more apps like Calendar, Fitbit, Google Wallet, Google Maps, YouTube Music and more.”); <i>Device Tokenization - Supported Devices</i>, Google Pay, https://developers.google.com/pay/issuers/overview/supported-devices (“Google Pay is compatible with the majority of modern Android devices across a wide variety of manufacturers and form factors, including mobile phones, tablets, and Wear OS by Google devices.”)..</p> </div>

Claim No.	Accused Products
	<div data-bbox="422 224 903 824">  </div> <div data-bbox="903 662 1848 824"> <p>Beginning to roll out today, Google Wallet will join Fitbit Pay as a new payment option for Sense 2 and Versa 4 users, allowing you even more opportunities to go about your day hands-free. With just a tilt of your wrist, you can make speedy, secure, and contactless purchases without needing to pull out or bring your wallet.</p> </div> <p>See, e.g., Fitbit Staff, <i>Travel with Ease with Google Maps and Make Payments Seamless with Google Wallet on Sense 2 and Versa 4</i>, Google, https://store.google.com/intl/en/ideas/articles/sense-versa-google-maps-wallet/; <i>What should I know about using by Fitbit device to make contactless payments?</i>, Fitbit Help Center, https://support.google.com/fitbit/answer/14236521.</p> <div data-bbox="422 992 1379 1390">  </div> <p>See, e.g., <i>Google Pay – Pay the Google way</i>, Google, https://pay.google.com/about/; <i>Google Pay – Pay In Store</i>, Google, https://pay.google.com/about/pay-in-store/; <i>Google Wallet</i>, Google, https://wallet.google/.</p>

Claim No.	Accused Products
	<p>In addition, Google has induced and/or contributed to third parties’ use of such devices to practice the accused methods.</p> <p>For example, Google recently announced that “With Google Wallet, we are building a common platform that makes it easier for device makers to provide a digital wallet on every Android device, and developers can enable their users to have quick, convenient access to wallet objects across the Android ecosystem.” – Kevin Flanagan, Partner Engineering Lead, Google Wallet. <i>See, e.g., Google Wallet API tutorial for Google Developers Google I/O 2022</i>, (May 11, 2022), https://www.youtube.com/watch?v=2gTCghy-dU4 at 1:25 (Last visited December 4, 2024).</p> <p>In line with that advertisement, smartphones like the new Motorola Razr Plus 2024 are being sold in the United States with Google Wallet pre-installed on the devices. <i>See, e.g., Motorola RAZR Plus: How to Setup (step by step)</i> (September 22, 2023), https://www.youtube.com/watch?v=hR2Zy0V8Oqw at 3:44 (Last visited December 4, 2024). Google Pay and Google Wallet are also available for download on other electronic devices.</p>
<p>1[a] receiving an input at an electronic device corresponding to a priming operation of the electronic device by an authorized user; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, receives an input at an electronic device corresponding to a priming operation of the electronic device by an authorized user (e.g., authorized by double pressing the digital crown, entering a PIN, pattern, using fingerprint, face unlock, etc.).</p> <h2 data-bbox="422 768 1094 816">Verify it’s you to make a purchase</h2> <p data-bbox="422 833 1381 889">To make payments with Google Wallet, you must have a screen lock set up on your device and verify it’s you for your security.</p> <p data-bbox="422 914 1045 938">You can verify it's you in Google Wallet with several methods:</p> <div data-bbox="422 954 709 1125" style="border: 2px solid red; padding: 5px;"> <ul style="list-style-type: none"> • PIN • Pattern • Password • Class 3 biometric unlock </div> <p data-bbox="422 1133 1367 1190">Tip: Google Wallet doesn't work with Class 1 or Class 2 biometric unlocks or screen locks like Smart Unlock or Knock to Unlock.</p> <p data-bbox="422 1198 1990 1360"><i>See, e.g., Verify it’s you to make a purchase</i>, Google Wallet Help, https://support.google.com/wallet/answer/12059519; <i>Set up screen lock for tap to pay transactions</i>, Google Wallet Help Center (captured Dec. 15, 2023), https://web.archive.org/web/20231215153739/https://support.google.com/wallet/answer/12059519#zippy=%2Cpayment-limits-on-a-locked-device (noting for the United States that “Unlock is required for all transactions except for transit”); <i>Set screen lock on your Pixel phone</i>, Pixel Phone Help, https://support.google.com/pixelphone/answer/2819522.</p>

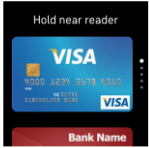
Claim No.	Accused Products
	<p>7.3.10. Biometric Sensors</p> <p>Biometric sensors can be classified as Class 3 (formerly Strong), Class 2 (formerly Weak), or Class 1 (formerly Convenience) based on their spoof and imposter acceptance rates, and on the security of the biometric pipeline. This classification determines the capabilities the biometric sensor has to interface with the platform and with third-party applications. Sensors need to meet additional requirements as detailed below if they wish to be classified as either Class 1, Class 2 or Class 3. Both Class 2 and Class 3 biometrics get additional capabilities as detailed below.</p> <p>See, e.g., Android 15 Compatibility Definition, https://source.android.com/docs/compatibility/15/android-15-cdd.</p> <p>BIOMETRIC_STRONG Added in API level 30</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0; background-color: #f9f9f9;"> <pre>public static final int BIOMETRIC_STRONG</pre> </div> <p>Any biometric (e.g. fingerprint, iris, or face) on the device that meets or exceeds the requirements for Class 3 (formerly Strong), as defined by the Android CDD.</p> <p>This corresponds to <code>KeyProperties.AUTH_BIOMETRIC_STRONG</code> during key generation.</p> <p>See, e.g., BiometricManager.Authenticators , Android Developers, https://developer.android.com/reference/android/hardware/biometrics/BiometricManager.Authenticators#BIOMETRIC_STRONG.</p>

Claim No.	Accused Products
	<p>How to use Google Wallet on Pixel Watch</p> <p>With Screen Lock and Google Wallet set up on Pixel Watch, now it's just a matter of putting the tap-to-pay functionality to use.</p> <ol style="list-style-type: none"> 1. Double-press the crown. 2. Your default card will appear on the screen. 3. If you want to pay with a different card, swipe until you find the card you want to use. 4. Hold your Pixel Watch near the payment terminal. 5. Once the payment has been completed successfully, you will hear a chime and a checkmark appears on your watch. <p><i>See, e.g., How to use Google Wallet on the Pixel Watch, AndroidCentral (Oct. 19, 2022), https://www.androidcentral.com/wearables/how-to-use-google-wallet-pixel-watch.</i></p> <ol style="list-style-type: none"> 1. If prompted enter your 4-digit device PIN code. Your default card appears on the screen. <div data-bbox="470 898 846 1114">  </div> <ol style="list-style-type: none"> 2. To pay with your default card, hold your wrist near the payment terminal. To pay with a different card: <p><i>See, e.g., What should I know about using my Fitbit device to make contactless payments? Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</i></p>

Claim No.	Accused Products
1[b] wherein authorizing of a user of the electronic device comprises recognizing a user input using a human input sensor, and wherein the human input sensor is any one of a touch sensor, a touch-screen display interface, a gesture sensor, a motion sensor, and a biometric sensor; and ¹ ,	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein authorizing of a user of the electronic device comprises recognizing a user input using a human input sensor, and wherein the human input sensor is any one of a touch sensor, a touch-screen display interface (e.g., touchscreen of the smartphone or smartwatch), a gesture sensor, a motion sensor, and a biometric sensor (e.g., face unlock, etc.).</p> <h2>Verify it’s you to make a purchase</h2> <p>To make payments with Google Wallet, you must have a screen lock set up on your device and verify it’s you for your security.</p> <p>You can verify it’s you in Google Wallet with several methods:</p> <ul style="list-style-type: none"> • PIN • Pattern • Password • Class 3 biometric unlock <p>Tip: Google Wallet doesn’t work with Class 1 or Class 2 biometric unlocks or screen locks like Smart Unlock or Knock to Unlock.</p> <p><i>See, e.g., Verify it’s you to make a purchase</i>, Google Wallet Help, https://support.google.com/wallet/answer/12059519; <i>Set up screen lock for tap to pay transactions</i>, Google Wallet Help Center (captured Dec. 15, 2023), https://web.archive.org/web/20231215153739/https://support.google.com/wallet/answer/12059519#zippy=%2Cpayment-limits-on-a-locked-device (noting for the United States that “Unlock is required for all transactions except for transit”); <i>Set screen lock on your Pixel phone</i>, Pixel Phone Help, https://support.google.com/pixelphone/answer/2819522.</p> <h3>7.3.10. Biometric Sensors</h3> <p>Biometric sensors can be classified as Class 3 (formerly Strong), Class 2 (formerly Weak), or Class 1 (formerly Convenience) based on their spoof and imposter acceptance rates, and on the security of the biometric pipeline. This classification determines the capabilities the biometric sensor has to interface with the platform and with third-party applications. Sensors need to meet additional requirements as detailed below if they wish to be classified as either Class 1, Class 2 or Class 3.</p> <p>Both Class 2 and Class 3 biometrics get additional capabilities as detailed below.</p> <p><i>See, e.g., Android 15 Compatibility Definition</i>, https://source.android.com/docs/compatibility/15/android-15-cdd.</p>

¹ See Certificate of Correction issued on May 10, 2022.

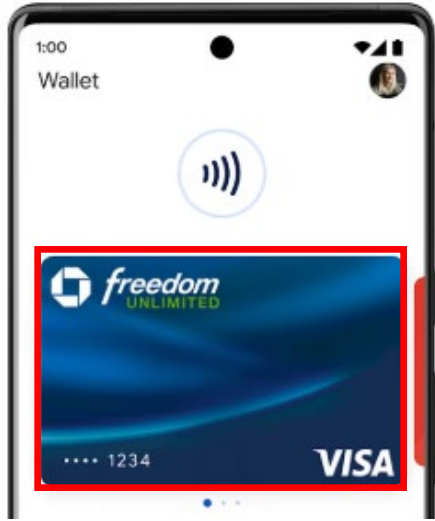
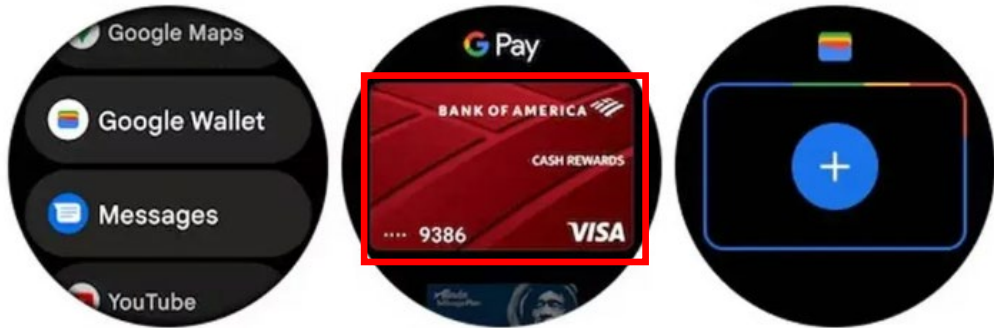
Claim No.	Accused Products
	<p>BIOMETRIC_STRONG Added in API level 30</p> <div> <pre>public static final int BIOMETRIC_STRONG</pre> </div> <p>Any biometric (e.g. fingerprint, iris, or face) on the device that meets or exceeds the requirements for Class 3 (formerly Strong), as defined by the Android CDD.</p> <p>This corresponds to <code>KeyProperties.AUTH_BIOMETRIC_STRONG</code> during key generation.</p> <p>See, e.g., BiometricManager.Authenticators , Android Developers, https://developer.android.com/reference/android/hardware/biometrics/BiometricManager.Authenticators#BIOMETRIC_STRONG.</p> <h3>How to use Google Wallet on Pixel Watch</h3> <p>With Screen Lock and Google Wallet set up on Pixel Watch, now it's just a matter of putting the tap-to-pay functionality to use.</p> <ol style="list-style-type: none"> 1. Double-press the crown. 2. Your default card will appear on the screen. 3. If you want to pay with a different card, swipe until you find the card you want to use. 4. Hold your Pixel Watch near the payment terminal. 5. Once the payment has been completed successfully, you will hear a chime and a checkmark appears on your watch. <p>See, e.g., <i>How to use Google Wallet on the Pixel Watch</i>, AndroidCentral (Oct. 19, 2022), https://www.androidcentral.com/wearables/how-to-use-google-wallet-pixel-watch.</p>

Claim No.	Accused Products
	<p>1. If prompted, enter your 4-digit device PIN code. Your default card appears on the screen.</p> <div style="display: flex; justify-content: space-around; align-items: center;">   </div> <p>2. To pay with your default card, hold your wrist near the payment terminal. To pay with a different card:</p> <p><i>See, e.g., What should I know about using my Fitbit device to make contactless payments?</i> Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</p>
<p>1[c] receiving a request for a transaction payment at said electronic device via an NFC interface of the device; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, receives a request for a transaction payment at said electronic device via the NFC interface of the device (e.g., from a merchant terminal).</p> <p>How does Tap to Pay work?</p> <div style="border: 1px solid red; padding: 10px; margin: 10px 0;"> <p>When you make payment with Tap to Pay on your Android phone, it uses Near Field Communication (NFC) technology to transmit a virtual account number to the retailer’s payment terminal. Tap to Pay operates only within a few inches of the terminal, which helps to keep your Google Pay information private, keeping your actual card number confidential.</p> </div> <p>Here’s how you can start tapping and paying with your Android phone:</p> <ol style="list-style-type: none"> 1. Unlock your device with your passcode or face ID. 2. Hold it near the contactless card reader. 3. Tap and wait for a blue check mark to confirm the payment. <p><i>See, e.g., Make payments effortless with Tap to Pay</i>, Android, https://www.android.com/intl/en_in/articles/what-is-tap-to-pay/.</p>

Claim No.	Accused Products
	<div><div><div><div><div>Host CPU</div><div>NFC Controller</div></div><div>Android device</div></div><div><div>NFC Reader</div></div></div><p>When an NFC card is emulated using host-based card emulation, the data is routed directly to the host CPU instead of being routed to a secure element. Figure 2 illustrates how host-based card emulation works:</p><p>Figure 2. NFC card emulation without a secure element.</p><p>See, e.g., <i>Host-based card emulation overview</i>, Google, https://developer.android.com/develop/connectivity/nfc/hce (last visited December 8, 2024).</p></div>

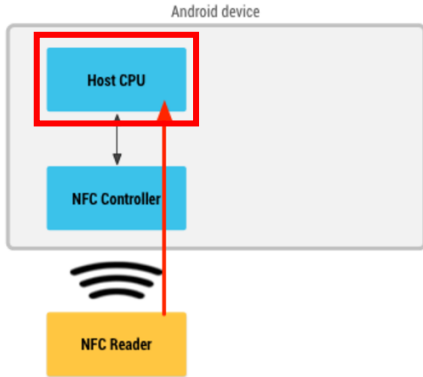
Claim No.	Accused Products
	<div><p>Pixel 9 Pro Fold</p><p>To learn about the features of your Pixel 9 Pro Fold phone, refer to the diagram below:</p><div></div><div><ol style="list-style-type: none">1. Top speaker2. mmWave antenna cover3. Top microphone4. Inner front-facing camera5. Power button/fingerprint sensor6. Volume up/down button7. Rear-facing camera: Ultrawide lens8. Rear-facing camera: 5x Telephoto lens9. Rear-facing camera: Wide lens10. LED flash11. Rear-facing microphone12. Outer front-facing camera13. NFC</div><p>See, e.g., <i>Pixel phone hardware diagram</i>, Pixel Phone Help, https://support.google.com/pixelphone/answer/7157629.</p><p>Make a payment in a store</p><p>Important: For QUICPay and iD, you don't need to open the Google Wallet app to pay. Just hold your watch to the reader.</p><div><ol style="list-style-type: none">1. Open the Google Wallet app 🇸🇬.2. Hold your watch over the contactless payment reader until you hear a sound or feel vibration from your watch.3. If asked, tap Credit regardless of your type of card.4. For debit card transactions, you may have to enter a PIN. Use the PIN that you set up with your bank.</div><div></div><p>See, e.g., <i>Tap to pay with your smartwatch</i>, Google Wallet Help, https://support.google.com/wallet/answer/12059876.</p></div>

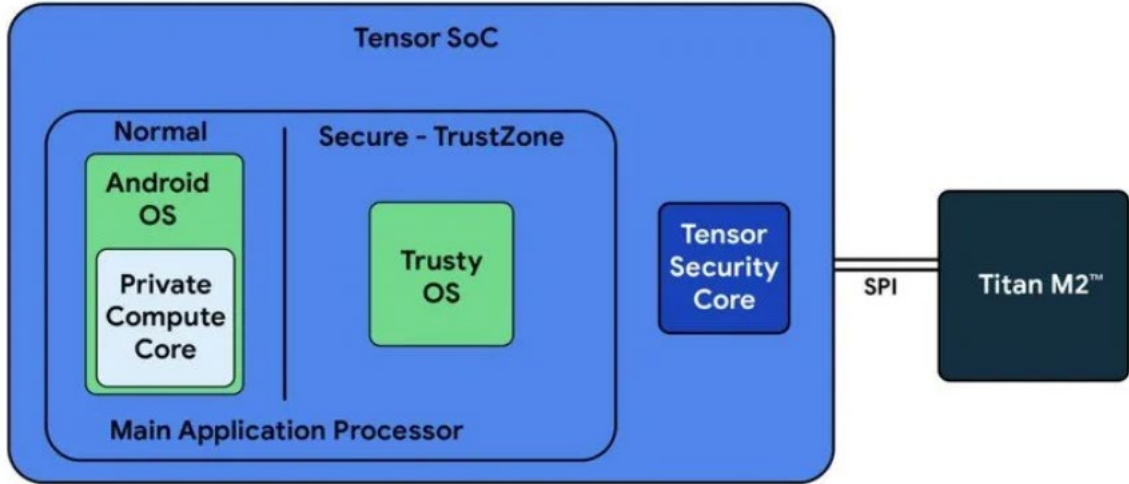
Claim No.	Accused Products
	<p>Google Pixel Watch 3 Specifications ⬆ [. . .]</p> <div> <div>Connectivity</div> <ul style="list-style-type: none"> • 4G LTE and UMTS³ • Bluetooth® 5.3 • Wifi 802.11a/b/g/n/ac/ax 2.4Ghz, 5Ghz • NFC </div> <p>See, e.g., <i>Google Pixel Watch Technical & Device Specifications</i>, Google Pixel Watch Help, https://support.google.com/googlepixelwatch/answer/12651869.</p> <ul style="list-style-type: none"> ● Let's get a sense of what this Fitbit brings to the table: <ul style="list-style-type: none"> ● 1.58 AMOLED screen ● 4 GB internal storage ● A new ECG function as well as a skin temperature sensor, and the standard optical heart rate sensor ● Wi-Fi, NFC, Bluetooth 5.0 and Built-in GPS ● Water resistant up to 50 meters ● Also part of the package are a gyroscope, an altimeter, a 3-axis accelerometer, and an ambient light sensor <p>See, e.g., <i>Fitbit Sense Teardown</i>, https://www.ifixit.com/Teardown/Fitbit+Sense+Teardown/137130 (Last visited December 8, 2024).</p> <p>Which Fitbit devices support contactless payments?</p> <p>Make contactless payments with Fitbit Charge 4, Fitbit Charge 5, Fitbit Charge 6, Fitbit Sense, Fitbit Sense 2, Fitbit Versa 2, Fitbit Versa 3, Fitbit Versa 4, and editions of Fitbit Charge 3 and Fitbit Versa that contain an NFC chip.</p> <p>See, e.g., <i>What should I know about using my Fitbit device to make contactless payments?</i> Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</p>

Claim No.	Accused Products
<p>1[d] displaying, on a display of the device, the request and at least a portion of an original static issuer-supplied payment account information associated with a selected payment method, for a user selection in paying the request; and²,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, displays, on a display of the device, the request and at least a portion of an original static issuer-supplied payment account information associated with a selected payment method (e.g., last four digits of the primary account number (“PAN”)), for a user selection in paying the request.</p>  <p>See, e.g., Molly McHugh-Johnson, <i>Ask a Techspert: How do digital wallets work?</i>, Google – The Keyword (May 11, 2022), https://blog.google/products/android/ask-a-techspert-google-wallet/.</p>  <p>See, e.g., Vinay Patel, <i>The 6 Best Google Pixel Watch features that make you say wow</i> (October 28, 2022), https://www.gizchina.com/2022/10/28/the-6-best-google-pixel-watch-features-that-make-you-say-wow/.</p>

² *Id.*

Claim No.	Accused Products
<p>1[e] retrieving from a memory attached to a processor of the device, a device-specific static limited-use payment information, associated with said selected payment method; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, retrieves from a memory (e.g., a system memory, memory of secure element, or combination of the same) attached to a processor of the device (e.g., a processor or coprocessor, processor of secure element, processor of a SIM/eSIM, or combination of the same), a device-specific static limited-use payment information (e.g., device-specific number/ “device token”/ payment token/ dynamic primary account number (“DPAN”)), associated with said selected payment method.</p> <h2 data-bbox="447 440 940 488">What device tokens are</h2> <p data-bbox="447 529 1409 727">When you pay for something with a physical card — credit, debit or prepaid — the merchant usually charges you through the printed number on the front of your card, known as the Funding Primary Account Number (FPAN). Every time this happens, you provide that number to the merchant, and that number is then sent along to a handful of other parties like the merchant’s bank, the card network (an organization that facilitates transactions between banks and merchants), the payment service provider and more.</p> <p data-bbox="447 748 1409 878">In contrast, Google Wallet creates a device-specific virtual account number, or device token, for each payment method you add, so your real card number isn’t stored on your device or shared with merchants. Thanks to this tokenization, the only parties who have your actual FPAN when you make a purchase are the bank that issued the card and the card network.</p> <p data-bbox="422 889 1980 951"><i>See, e.g., How device tokens keep your payment cards safe in Google Wallet, https://blog.google/products/google-pay/device-tokens-google-wallet.</i></p>

Claim No.	Accused Products
	<p>Host-based card emulation</p> <p>When an NFC card is emulated using host-based card emulation, the data is routed directly to the host CPU instead of being routed to a secure element. Figure 2 illustrates how host-based card emulation works:</p>  <p>The diagram shows an Android device with a Host CPU and an NFC Controller. The Host CPU is highlighted with a red box. An NFC Reader is shown below the device, connected to the Host CPU via a red arrow. The NFC Controller is connected to the Host CPU via a black arrow. The NFC Reader is connected to the NFC Controller via a black arrow. The Host CPU is connected to the NFC Controller via a black arrow.</p> <p>Figure 2. NFC card emulation without a secure element.</p> <p>See, e.g., <i>Host-based card emulation overview</i>, Google, https://developer.android.com/develop/connectivity/nfc/hce (last visited December 8, 2024).</p> <ul style="list-style-type: none"> Google Pay on Fitbit is the extension of Google Pay wallet to Secure Element technology, under Google Pay Wallet ID and a different Token Requestor ID (TRID) for Google Pay SE versus Google Pay HCE. <p>See, e.g., <i>Fitbit Pay FAQ</i>, https://developers.google.com/pay/issuers/support/fitbit-faq.</p> <p>Best answer: Titan is Google's branding for hardware-based security products, and with the Pixel 6 series, it's now a two-part setup. The Titan M2 is a discrete RISC-V security chip fully designed and developed by Google. It communicates with the new Google Tensor security core, which is a custom-designed security subsystem. Together they are dedicated to the preservation of user privacy.</p>

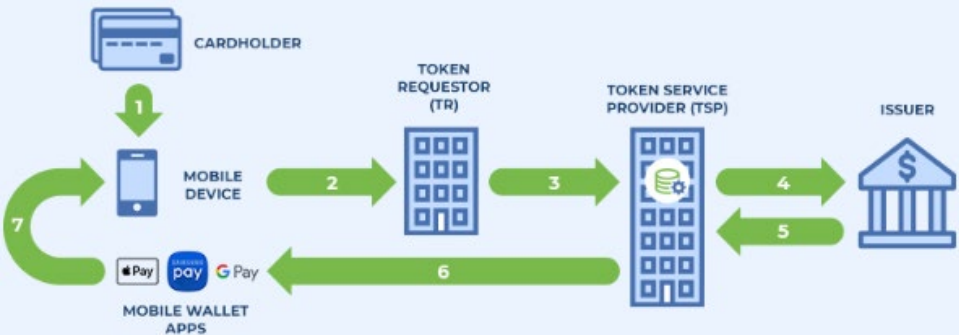
Claim No.	Accused Products
	 <p>The diagram illustrates the architecture of a Tensor SoC. It is divided into three main sections: a 'Normal' section containing 'Android OS' and a 'Private Compute Core'; a 'Secure - TrustZone' section containing 'Trusty OS'; and a 'Tensor Security Core'. These three sections are part of a 'Main Application Processor'. The 'Tensor Security Core' is connected to a separate 'Titan M2' component via an 'SPI' (Serial Peripheral Interface) bus.</p> <p>See, e.g., <i>How does the Google Titan M2 and Tensor security core work?</i> https://www.androidcentral.com/how-does-google-titan-m2-and-tensor-security-core-work.</p> <h4>4.2.1 HCE with Virtual Cloud-Based SE</h4> <p>Android Pay uses HCE instead of the SE in a mobile phone and stores a master domain key representing the PAN in the cloud. Payment tokens and limited-use or single-use token keys (LUKs) generated by the master domain key in the cloud are stored in a secure area of the mobile OS, which uses software-based security, such as white box cryptography, to obfuscate the key. LUKs generate cryptograms that are passed with the EMV payment token for each transaction. The keys are refreshed each time the user connects to a network, which enables transactions to be completed without network connectivity. Rather than requesting a token from the cloud each time it is needed to make a payment, solutions using LUKs address the possibility that an Internet connection might not be available to download a token. LUKs also are restricted and expire quickly, to minimize their value to fraudsters.</p> <p>See, e.g., <i>U.S. Payments Forum, Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions, Version 1.0, January 2018</i>, https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf.</p>

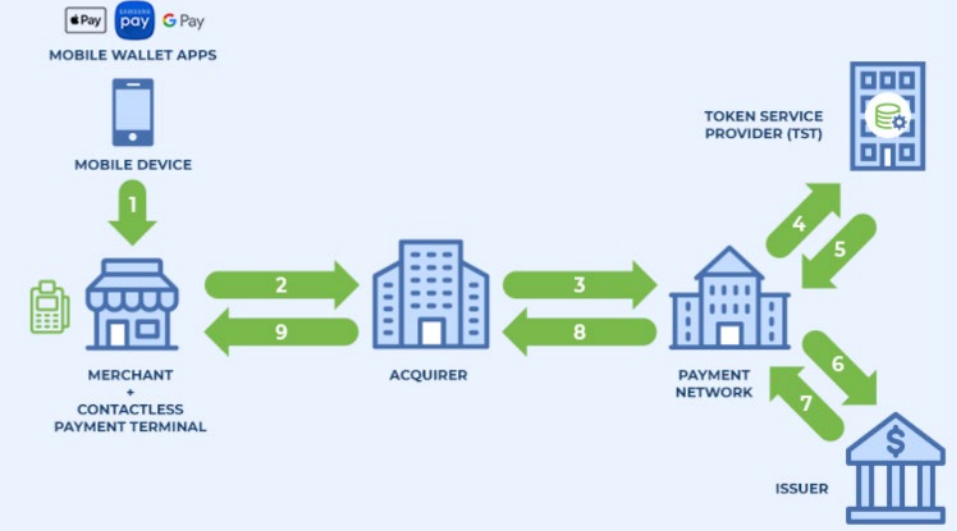
Claim No.	Accused Products
	<p>The following flow diagrams show how the cardholder's device, Google's servers, the TSP, and the card issuing bank's systems interact to provision a token.</p> <pre>sequenceDiagram participant User participant Google participant TSP participant Issuer User->>Google: User enters card details activate Google Google->>User: User accepts Google Pay ToS deactivate Google activate User User->>Google: Present issuer ToS deactivate User activate Google Google->>TSP: checkEligibility() deactivate Google activate TSP TSP->>Issuer: checkEligibility() deactivate TSP activate Issuer Issuer-->>TSP: Success deactivate Issuer TSP-->>Google: Success (card metadata, Issuer ToS, card art) deactivate TSP activate Google Google->>User: ToS accpeted deactivate Google activate User User->>Google: tokenize(risk signals, provisioning data) deactivate User activate Google Google->>TSP: tokenize(risk signals, provisioning data) deactivate Google activate TSP TSP->>Issuer: idvOutcome(approved, declined, challenge) deactivate TSP activate Issuer Issuer-->>TSP: idvOutcome(approved, declined, challenge) deactivate Issuer TSP-->>Google: idvOutcome(approved, declined, challenge) deactivate TSP activate Google Google->>User: idvOutcome(approved, declined, challenge) deactivate Google deactivate User Note over User, Google, TSP, Issuer: If ID&V outcome="green", flow complete, active token. Note over User, Google, TSP, Issuer: If ID&V outcome="red", flow complete, no token. Note over User, Google, TSP, Issuer: If ID&V outcome="yellow", proceed to ID&V. SMS example below.</pre> <p>See, e.g., <i>Google Pay – Device Tokenization – TSP Integration – Overview</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview; <i>Google Pay FAQ</i>, Aerospace Federal Credit Union, https://www.aerofcu.org/Services/Digital-Wallet/Google-Pay-FAQ (“[Google Pay] requires an active Internet connection when adding or removing a payment card or to download transaction history. You can connect via a Wi-Fi network or using your mobile data connection.”).</p>

Claim No.	Accused Products
	<div data-bbox="449 261 816 345" data-label="Image"> </div> <div data-bbox="842 261 1421 344" data-label="Section-Header"> <h2>EMVCo Security Evaluation Certificate Mobile Application</h2> </div> <div data-bbox="466 376 1386 425" data-label="Text"> <p>Please accept this document as confirmation of the EMVCo Software-Based Mobile Payments Security Evaluation Process.</p> </div> <div data-bbox="436 470 930 498" data-label="Text"> <p>Evaluation Certificate Number: SECN0069.03</p> </div> <div data-bbox="436 511 753 540" data-label="Text"> <p>Date SECN Issued: 22 Apr 2021</p> </div> <div data-bbox="1003 511 1392 540" data-label="Text"> <p>Next security review due: 22 Apr 2025</p> </div> <div data-bbox="436 555 749 583" data-label="Text"> <p>Company Name: Google, LLC</p> </div> <div data-bbox="436 584 1161 641" data-label="Text"> <p>Address: 1600 Amphitheatre Pkwy Mountain View, CA 94043 United States of America</p> </div> <div data-bbox="436 652 745 682" data-label="Text"> <p>Product Name: Google Wallet</p> </div> <div data-bbox="413 682 1593 750" data-label="Text"> <p>See, e.g., <i>EMVCo Security Evaluation Certificate Mobile Application</i>, https://www.emvco.com/wp-content/uploads/loa/EMVCo_SECN0069.03_N_08_2024-15.pdf (Last visited December 4, 2024).</p> </div> <div data-bbox="417 782 1344 855" data-label="Section-Header"> <h3>3.1 In-Store EMV Contactless Payments with Device-Centric Digital Wallets</h3> </div> <div data-bbox="417 873 1451 1019" data-label="Text"> <p>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.</p> </div> <div data-bbox="422 1032 1253 1075" data-label="Section-Header"> <h2>5. End-to-End EMV Payment Tokenization Flows</h2> </div> <div data-bbox="422 1091 1444 1151" data-label="Text"> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> </div> <div data-bbox="464 1167 1457 1229" data-label="List-Group"> <ul style="list-style-type: none"> • In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) </div>

Claim No.	Accused Products
	<p>Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet</p> <p>^aID&V methods includes text or email or call. OTP is an example. ^bIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.</p>
	<p>Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet</p> <p>^aIn some implementations, the last four digits, instead of the PAN, are passed back in the authorization response ^bLast 4 digits of the PAN may not always be returned to the merchant.</p>

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 No.	Accused Products
	<p>In general terms, the process for registering a card in a mobile wallet is as follows: [...]</p> <ol style="list-style-type: none"> <li data-bbox="432 277 1365 456">5. If everything is correct, the TSP registers the PAN and links it to a new token in a secure database (<i>Token Vault</i>). Along with the TR identifier, the token expiration date, and a number of additional security features called <i>Token Domain</i>, including restrictions on the use of the new token on certain channels, use by a particular merchant, limitation on the number of permitted uses, and verification of the cryptogram. <li data-bbox="432 488 1094 513">6. The TSP notifies the application of the newly generated token. <li data-bbox="432 545 1360 646">7. The application stores the generated token (<i>Device Account Number</i> (DAN) for Apple Pay or Digitized PAN (DPAN) for Samsung Pay) in a secure location (Secure Element (SE) or Host Card Emulation (HCE)).  <p>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:</p> <ol style="list-style-type: none"> <li data-bbox="432 1114 1360 1341">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: <ul style="list-style-type: none"> • 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. <li data-bbox="432 1357 1241 1382">2. The merchant sends the token and dynamic cryptogram data to the acquirer. [...]

Claim No.	Accused Products
	 <p>The diagram illustrates the mobile payment tokenization process. It shows a Mobile Device (with Apple Pay, Google Pay, and Samsung Pay logos) interacting with a Merchant's Contactless Payment Terminal. The process involves a Token Service Provider (TSP) and an Issuer. The steps are numbered 1 through 9, showing the flow of data and tokens between the device, merchant, acquirer, payment network, and issuer.</p> <p>See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details.</p> <p>5.1.3.2 Token Generation</p> <p>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.</p> <p>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.</p> <p>5.1.3.3 Token Issuance</p> <p>Token Issuance is the process of issuing a Payment Token and related data in preparation for Token Provisioning.</p> <p>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</p>

Claim No.	Accused Products
	<p>Tokens SHALL only be issued through the response to a Token Request from a registered Token Requestor with a valid Token Requestor ID.</p> <p>5.1.3.4 Token Provisioning</p> <p>Token Provisioning is the process of delivering a Payment Token and related data to the Token Location.</p> <p>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.</p> <p><i>See, e.g., EMVCo, EMV® Payment Tokenisation Specification – Technical Framework v2.1 at 35–36 (Jun. 14, 2019), available at https://www.emvco.com/emv-technologies/payment-tokenisation/.</i></p>
<p>1[f] dynamically generating, by a processor of the device, device-specific limited-use payment information, for said selected payment method; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, dynamically generates, by a processor of the device, device-specific limited-use payment information (e.g., a application cryptogram/ transaction cryptogram/ token cryptogram/ payment cryptogram (“dynamic cryptogram”)), for said selected payment method.</p> <p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant’s acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay’s security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token’s DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder’s mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p><i>See, e.g., Google Pay – Device Tokenization – Security, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; Google Pay – Device Tokenization – TSP Integration, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</i></p>

Claim No.	Accused Products		
	<p>5.0 Secure Limited-Use Key Storage</p> <p>5.1 Context</p> <p>Conventional provisioning of credit card information to a device (whether tokenized or not) involves storing a Master Key on a trusted piece of hardware like a Secure Element. For the purpose of this document, it will be called Card Master Key (CMK). CMK is synonymous with Master Derivation Key (MDK).</p> <p>The CMK serves as a long-term secret used to compute cryptographic dynamic verification codes (CVC3) are generated for MSD transactions and ARQC (Online Authorization Request) cryptograms are generated for EMV transactions. These are verified by the issuer during issuer authorization.</p> <p>See, e.g., Google, <i>Google Pay Security Paper</i> (Ver. 2.4, Jan. 2022) available at https://developers.google.com/wallet/access/campus-id/resources/Google_Pay_Security_Paper_2.4.pdf; <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Payment data cryptography for merchants</i>, Google Pay for Payments (Oct. 28, 2024), https://developers.google.com/pay/api/android/guides/resources/payment-data-cryptography.</p> <p>3. Tokenization Use Case Scenarios</p> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p>	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.
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.		

Claim No.	Accused Products
	 <p>EMVCo Security Evaluation Certificate Mobile Application</p> <p>Please accept this document as confirmation of the EMVCo Software-Based Mobile Payments Security Evaluation Process.</p> <p>Evaluation Certificate Number: SECN0069.03</p> <p>Date SECN Issued: 22 Apr 2021 Next security review due: 22 Apr 2025</p> <p>Company Name: Google, LLC Address: 1600 Amphitheatre Pkwy Mountain View, CA 94043 United States of America</p> <p>Product Name: Google Wallet</p> <p>See, e.g., <i>EMVCo Security Evaluation Certificate Mobile Application</i>, https://www.emvco.com/wp-content/uploads/loa/EMVCo_SECN0069.03_N_08_2024-15.pdf (Last visited December 4, 2024).</p> <p>5.0 Secure Limited-Use Key Storage</p> <p>5.1 Context</p> <p>Conventional provisioning of credit card information to a device (whether tokenized or not) involves storing a Master Key on a trusted piece of hardware like a Secure Element. For the purpose of this document, it will be called Card Master Key (CMK). CMK is synonymous with Master Derivation Key (MDK).</p> <p>The CMK serves as a long-term secret used to compute cryptographic dynamic verification codes (CVC3) are generated for MSD transactions and ARQC (Online Authorization Request) cryptograms are generated for EMV transactions. These are verified by the issuer during issuer authorization.</p> <p>See, e.g., Google, <i>Google Pay Security Paper</i> (Ver. 2.4, Jan. 2022) available at https://developers.google.com/wallet/access/campus-id/resources/Google_Pay_Security_Paper_2.4.pdf; <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Payment data cryptography for merchants</i>, Google Pay for Payments (Oct. 28, 2024), https://developers.google.com/pay/api/android/guides/resources/payment-data-cryptography.</p>
1[g] using said limited-use payment informations in place of at least a portion of said selected original issuer-supplied payment	A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartwatch or smartphone, uses said limited-use payment informations (e.g., DPAN, dynamic cryptogram or combinations thereof) in place of at least a portion of said selected original issuer-supplied payment information (e.g., PAN or associated expiration date or card security code/ card identification number/ card validation value (“CVV”)) for the transaction.

Claim No.	Accused Products
information for the transaction; and ³ ,	<h2 data-bbox="447 240 940 289">What device tokens are</h2> <p data-bbox="447 329 1409 524">When you pay for something with a physical card — credit, debit or prepaid — the merchant usually charges you through the printed number on the front of your card, known as the Funding Primary Account Number (FPAN). Every time this happens, you provide that number to the merchant, and that number is then sent along to a handful of other parties like the merchant’s bank, the card network (an organization that facilitates transactions between banks and merchants), the payment service provider and more.</p> <p data-bbox="447 548 1409 678">In contrast, Google Wallet creates a device-specific virtual account number, or device token, for each payment method you add, so your real card number isn’t stored on your device or shared with merchants. Thanks to this tokenization, the only parties who have your actual FPAN when you make a purchase are the bank that issued the card and the card network.</p> <p data-bbox="426 686 1976 751"><i>See, e.g., How device tokens keep your payment cards safe in Google Wallet</i>, https://blog.google/products/google-pay/device-tokens-google-wallet.</p> <h2 data-bbox="426 784 787 816">Tokens and cards-on-file</h2> <p data-bbox="426 857 1197 881">When a user adds their card to Google Pay, they get one or more of the following:</p> <ul data-bbox="464 914 993 1036" style="list-style-type: none"> • Device token (DPANs) • Card-on-file (PAN/FPAN, expiry, and cardholder name) • Cloud token (tokenized version of a card-on-file) <p data-bbox="426 1060 1465 1255">Device tokens, cards on file, and cloud tokens are used in different scenarios. Device tokens are device bound and can be used for in-store NFC transactions and online transactions. Cards on file and cloud tokens are stored at the account level, rather than on the device, and can be used for peer-to-peer and online transactions. When tokenizing a card, the user’s card information may be stored as a card on file and can potentially incur a small, temporary charge. This charge is refunded once the account has been verified. More information can be found on the Google charge support page </p> <p data-bbox="426 1263 1976 1393"><i>See, e.g., Google Pay – Device Tokenization – Overview</i>, Google (Oct. 16, 2024), https://developers.google.com/pay/issuers; <i>Google Pay – Device Tokenization – TSP Integration</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview; <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security.</p>

³ *Id.*

Claim No.	Accused Products
	<p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant’s acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay’s security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token’s DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder’s mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p><i>See, e.g., Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Google Pay – Device Tokenization – TSP Integration</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</p> <p>Device tokenization</p> <p>When a user successfully adds their card to Google Pay, Google Pay stores a uniquely generated token on the device that has its own value. This new number, called a dynamic primary account number (DPAN) or device token, is similar to a credit card number.</p> <p>A DPAN improves account security because Google Pay passes it to a terminal during payment instead of the actual card number. In Google Pay, DPAN is referred as a ‘virtual account number’. Users can only see the last four digits of this number, which are visible on the card details view in the Google Wallet app.</p> <p><i>See, e.g., Enabling Google Pay device tokenization</i>, Google Pay, https://developers.google.com/pay/issuers/tsp-integration/overview.</p>

Claim No.	Accused Products
	<div data-bbox="451 261 816 345">  </div> <div data-bbox="852 261 1419 345"> <p>EMVCo Security Evaluation Certificate Mobile Application</p> </div> <div data-bbox="474 378 1383 425"> <p>Please accept this document as confirmation of the EMVCo Software-Based Mobile Payments Security Evaluation Process.</p> </div> <div data-bbox="445 472 928 498"> <p>Evaluation Certificate Number: SECN0069.03</p> </div> <div data-bbox="445 513 751 539"> <p>Date SECN Issued: 22 Apr 2021</p> </div> <div data-bbox="1014 513 1392 539"> <p>Next security review due: 22 Apr 2025</p> </div> <div data-bbox="445 557 747 583"> <p>Company Name: Google, LLC</p> </div> <div data-bbox="445 586 1159 641"> <p>Address: 1600 Amphitheatre Pkwy Mountain View, CA 94043 United States of America</p> </div> <div data-bbox="445 654 743 680"> <p>Product Name: Google Wallet</p> </div> <div data-bbox="420 683 1591 750"> <p>See, e.g., <i>EMVCo Security Evaluation Certificate Mobile Application</i>, https://www.emvco.com/wp-content/uploads/loa/EMVCo_SECN0069.03_N_08_2024-15.pdf (Last visited December 4, 2024).</p> </div> <div data-bbox="445 794 976 826"> <p>An HCE transaction takes place as follows:</p> </div> <div data-bbox="493 847 1743 1099"> <ol style="list-style-type: none"> 1. To initiate an HCE mobile payment, a customer taps the mobile phone at the POS contactless reader. 2. HCE enables the NFC controller in the mobile phone to route communications from the POS reader to the mobile wallet app to request access to the payment token. 3. The payment token and accompanying dynamic cryptogram are passed to the POS to complete the transaction. </div> <div data-bbox="420 1118 1915 1185"> <p>See, e.g., <i>Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions</i>, https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf, pp. 14.</p> </div> <div data-bbox="428 1229 1251 1269"> <h3>5. End-to-End EMV Payment Tokenization Flows</h3> </div> <div data-bbox="428 1289 1442 1347"> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> </div> <div data-bbox="470 1364 1455 1424"> <ul style="list-style-type: none"> • In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) </div>

Claim No.	Accused Products
	<p>Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 24 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf; <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details.</p>
1[h] combining said dynamically-generated limited-use payment information with said static limited-use payment information, to generate a complete device payment information; and ⁴ ,	A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]) combines said dynamically-generated limited-use payment information (e.g., dynamic cryptogram) with said static limited-use payment information (e.g., DPAN), to generate a complete device payment information.

⁴ *Id.*

Claim No.	Accused Products
	<p>Tokens and cards-on-file</p> <p>When a user adds their card to Google Pay, they get one or more of the following:</p> <ul style="list-style-type: none"> • Device token (DPANs) • Card-on-file (PAN/FPAN, expiry, and cardholder name) • Cloud token (tokenized version of a card-on-file) <p>Device tokens, cards on file, and cloud tokens are used in different scenarios. Device tokens are device bound and can be used for in-store NFC transactions and online transactions. Cards on file and cloud tokens are stored at the account level, rather than on the device, and can be used for peer-to-peer and online transactions. When tokenizing a card, the user's card information may be stored as a card on file and can potentially incur a small, temporary charge. This charge is refunded once the account has been verified. More information can be found on the Google charge support page </p> <p><i>See, e.g., Google Pay – Device Tokenization – Overview</i>, Google (Oct. 16, 2024), https://developers.google.com/pay/issuers; <i>Google Pay – Device Tokenization – TSP Integration</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview; <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security.</p> <p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant's acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay's security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token's DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder's mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p><i>See, e.g., Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Payment data cryptography for merchants</i>, Google Pay for Payments – Android (Oct. 28, 2024), https://developers.google.com/pay/api/android/guides/resources/payment-data-cryptography.</p>

Claim No.	Accused Products
	<p>5.0 Secure Limited-Use Key Storage</p> <p>5.1 Context</p> <p>Conventional provisioning of credit card information to a device (whether tokenized or not) involves storing a Master Key on a trusted piece of hardware like a Secure Element. For the purpose of this document, it will be called Card Master Key (CMK). CMK is synonymous with Master Derivation Key (MDK).</p> <p>The CMK serves as a long-term secret used to compute cryptographic dynamic verification codes (CVC3) are generated for MSD transactions and ARQC (Online Authorization Request) cryptograms are generated for EMV transactions. These are verified by the issuer during issuer authorization.</p> <p>See, e.g., Google, <i>Google Pay Security Paper</i> (Ver. 2.4, Jan. 2022) available at https://developers.google.com/wallet/access/campus-id/resources/Google_Pay_Security_Paper_2.4.pdf; <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Payment data cryptography for merchants</i>, Google Pay for Payments (Oct. 28, 2024), https://developers.google.com/pay/api/android/guides/resources/payment-data-cryptography.</p> <p>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:</p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> EMV Contactless: If the Point of Sale (POS) terminal supports contactless payments via NFC (Near Field Communication), the EMV contactless specification is used to perform the data transfer. The merchant sends the token and dynamic cryptogram data to the acquirer. <p>[...]</p>

Claim No.	Accused Products
	<div><p>The diagram illustrates the EMV payment tokenization process. It shows a flow from a Mobile Device (with Mobile Wallet Apps like Apple Pay, Samsung Pay, and Google Pay) to a Merchant + Contactless Payment Terminal. The process involves an Acquirer and a Payment Network, which interacts with an Issuer and a Token Service Provider (TST). The flow is numbered 1 through 9, indicating the sequence of steps in the transaction.</p></div> <p>See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details (captured May 9, 2024).</p> <h3>5. End-to-End EMV Payment Tokenization Flows</h3> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> <ul style="list-style-type: none">• In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)

Claim No.	Accused Products
	<p>Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 24-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <p>An HCE transaction takes place as follows:</p> <ol style="list-style-type: none"> 1. To initiate an HCE mobile payment, a customer taps the mobile phone at the POS contactless reader. 2. HCE enables the NFC controller in the mobile phone to route communications from the POS reader to the mobile wallet app to request access to the payment token. 3. The payment token and accompanying dynamic cryptogram are passed to the POS to complete the transaction. <p>See, e.g., <i>Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions</i>, https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf, pp. 14.</p>

Claim No.	Accused Products
1[i] transmitting said complete device payment information from said electronic device to a recipient reader via said NFC interface to the recipient NFC reader for a processing of the payment transaction; and,	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]) transmits said complete device payment information (e.g., as identified above) from said electronic device to a recipient reader via said NFC interface to the recipient NFC reader (e.g., merchant reader) for a processing of the payment transaction.</p> <p>Pay in a shop</p> <p>Step 1: Wake up and unlock your phone</p> <p>Important: For users with a Pixel 7 or Pixel 7 Pro, Face Unlock is currently not supported for contactless transactions.</p> <p>Turn on your screen, then unlock your phone. You don't need to open the Google Wallet app.</p> <p>Step 2: Hold the back of your phone to the payment reader</p> <p>When you're done paying, a blue tick will appear on the screen.</p> <p>See, e.g., <i>Pay contactless with your phone</i>, Google, https://support.google.com/wallet/answer/12060043 (Last visited December 8, 2024).</p> <p>Make a payment in a store</p> <p>Important: For QUICPay and iD, you don't need to open the Google Wallet app to pay. Just hold your watch to the reader.</p> <ol style="list-style-type: none"> 1. Open the Google Wallet app 🇪🇺. 2. Hold your watch over the contactless payment reader until you hear a sound or feel vibration from your watch. 3. If asked, tap Credit regardless of your type of card. 4. For debit card transactions, you may have to enter a PIN. Use the PIN that you set up with your bank. <p>See, e.g., <i>Tap to pay with your smartwatch</i>, Google Wallet Help, https://support.google.com/wallet/answer/12059876.</p> 

Claim No.	Accused Products
	<p>2. To pay with your default card, hold your wrist near the payment terminal. To pay with a different card:</p> <ul style="list-style-type: none">• Charge 3 and Charge 4—Tap the screen to find the card you want to use, and then hold your wrist near the payment terminal.• Charge 5 and Charge 6—Swipe to find the card you want to use, and hold your wrist near the payment terminal.• Sense 2, Versa, Versa 2, and Versa 4—Swipe up to find the card you want to use, and then hold your wrist near the payment terminal.• Sense and Versa 3—Swipe up to find the card you want to use, and tap it. Then hold your wrist near the payment terminal. <p><i>See, e.g., What should I know about using my Fitbit device to make contactless payments?</i> Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</p> <p>5. End-to-End EMV Payment Tokenization Flows</p> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> <ul style="list-style-type: none">• In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)

Claim No.	Accused Products
	<div><p>Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet</p><p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 24 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf; <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), 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).</p><p>An HCE transaction takes place as follows:</p><ol style="list-style-type: none">1. To initiate an HCE mobile payment, a customer taps the mobile phone at the POS contactless reader.2. HCE enables the NFC controller in the mobile phone to route communications from the POS reader to the mobile wallet app to request access to the payment token.3. The payment token and accompanying dynamic cryptogram are passed to the POS to complete the transaction.<p>See, e.g., <i>Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions</i>, https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf, pp. 14.</p></div>

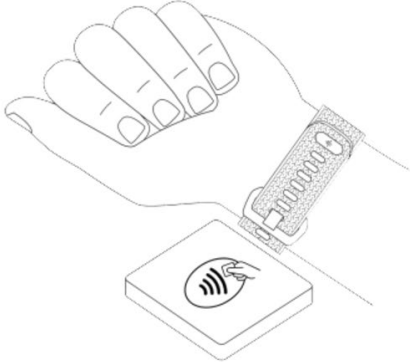
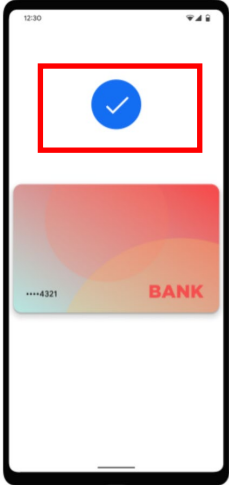
Claim No.	Accused Products
1[j] receiving information at said electronic device corresponding to a transaction status of the payment transaction, wherein such transaction status is at least partly dependent on validation of the complete device payment information by a payment processor authority and a payment issuer authority; and ⁵ ,	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, receives information (e.g., confirmation message) at said electronic device corresponding to a transaction status of the payment transaction, wherein such transaction status is at least partly dependent on validation of the complete device payment information by a payment processor authority (e.g., a payment processor, token service provider (“TSP”), and/or payment network) and a payment issuer authority (e.g., a bank).</p> <p>Pay in a shop</p> <p>Step 1: Wake up and unlock your phone</p> <p>Important: For users with a Pixel 7 or Pixel 7 Pro, Face Unlock is currently not supported for contactless transactions.</p> <p>Turn on your screen, then unlock your phone. You don't need to open the Google Wallet app.</p> <p>Step 2: Hold the back of your phone to the payment reader</p> <p>When you're done paying, a blue tick will appear on the screen.</p> <p>See, e.g., <i>Pay contactless with your phone</i>, Google, https://support.google.com/wallet/answer/12060043 (Last visited December 8, 2024).</p> <p>Make a payment in a store</p> <p>Important: For QUICPay and iD, you don't need to open the Google Wallet app to pay. Just hold your watch to the reader.</p> <ol style="list-style-type: none"> 1. Open the Google Wallet app 🇬🇧. 2. Hold your watch over the contactless payment reader until you hear a sound or feel vibration from your watch. 3. If asked, tap Credit regardless of your type of card. 4. For debit card transactions, you may have to enter a PIN. Use the PIN that you set up with your bank. <p>See, e.g., <i>Tap to pay with your smartwatch</i>, Google Wallet Help, https://support.google.com/wallet/answer/12059876.</p> 

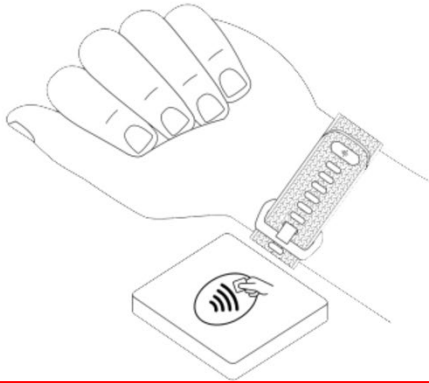
⁵ Id.

Claim No.	Accused Products
	<p>2. To pay with your default card, hold your wrist near the payment terminal. To pay with a different card:</p> <ul style="list-style-type: none"> • Charge 3 and Charge 4—Tap the screen to find the card you want to use, and then hold your wrist near the payment terminal. • Charge 5 and Charge 6—Swipe to find the card you want to use, and hold your wrist near the payment terminal. • Sense 2, Versa, Versa 2, and Versa 4—Swipe up to find the card you want to use, and then hold your wrist near the payment terminal. • Sense and Versa 3—Swipe up to find the card you want to use, and tap it. Then hold your wrist near the payment terminal. <p><i>See, e.g., What should I know about using my Fitbit device to make contactless payments?</i> Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</p> <p>5. End-to-End EMV Payment Tokenization Flows</p> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> <ul style="list-style-type: none"> • In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)

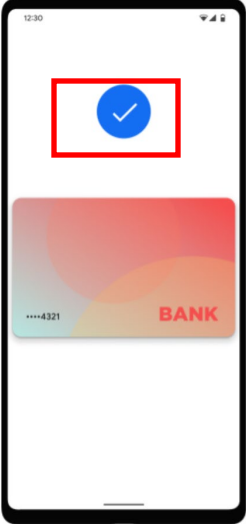
Claim No.	Accused Products
	<div><p>^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response ^b Last 4 digits of the PAN may not always be returned to the merchant.</p><p>Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 24 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf; <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), 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).</p><p>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: [. . .]</p><ol style="list-style-type: none">4. The payment network determines that it is a token and not a PAN, as the token has a specific BIN. It thereby routes the transaction to the related Token Service Provider (TSP).5. The TSP validates the token, the related cryptogram, the Token Requestor (TR) identifier and the Token Domain usage restrictions. If everything is correct, proceed with de-tokenization and sends the original PAN data to the payment network.<p>See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details.</p></div>

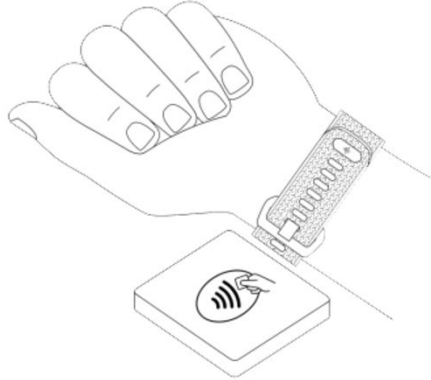
Claim No.	Accused Products
1[k] visually conveying the transaction payment authorization status via a user-interface displayed on said display.	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, visually conveys the transaction payment authorization status via a user-interface displayed on said display (e.g., by displaying a blue tick).</p> <div data-bbox="424 328 669 854" data-label="Image"> </div> <p>Step 2: Hold the back of your phone to the payment reader</p> <p>When you're done paying, a blue tick will appear on the screen.</p> <p>NFC Tap (success)</p> <p>See, e.g., <i>Google Pay – Device Tokenization – TSP Integration – Google Pay Flows</i>, Google (May 2, 2024), https://developers.google.com/pay/issuers/tsp-integration/gpay-flows; <i>Pay contactless with your phone</i>, Google, https://support.google.com/wallet/answer/12060043 (Last visited December 8, 2024).</p> <div data-bbox="424 1047 997 1372" data-label="Image"> </div> <p>See, e.g., <i>Made by Google, How to Use Google Wallet on Your Google Pixel Watch</i>, YouTube (Apr. 11, 2023), https://www.youtube.com/watch?v=Sa6ULG8MNUA; <i>Tap to pay with your smartwatch</i>, Google Wallet Help, https://support.google.com/wallet/answer/12059876.</p>

Claim No.	Accused Products
	 <p>When the payment succeeds, your device vibrates and you’ll receive a confirmation on the screen.</p> <p>See, e.g., <i>What should I know about using my Fitbit device to make contactless payments?</i> Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</p>
<p>2. The method of claim 1, further comprising receiving confirmation via said NFC interface of the validity of said complete device payment information from an NFC payment reader facility.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, receives confirmation via said NFC interface of the validity of said complete device payment information from an NFC payment reader facility.</p>  <p>Step 2: Hold the back of your phone to the payment reader</p> <p>When you're done paying a blue tick will appear on the screen.</p> <p>NFC Tap (success)</p> <p>See, e.g., <i>Google Pay – Device Tokenization – TSP Integration – Google Pay Flows</i>, Google (May 2, 2024), https://developers.google.com/pay/issuers/tsp-integration/gpay-flows; <i>Pay contactless with your phone</i>, Google, https://support.google.com/wallet/answer/12060043 (Last visited December 8, 2024).</p>

Claim No.	Accused Products
	<div data-bbox="426 228 999 548">  </div> <p data-bbox="426 553 1724 651">See, e.g., Made by Google, <i>How to Use Google Wallet on Your Google Pixel Watch</i>, YouTube (Apr. 11, 2023), https://www.youtube.com/watch?v=Sa6ULG8MNUA; <i>Tap to pay with your smartwatch</i>, Google Wallet Help, https://support.google.com/wallet/answer/12059876.</p> <div data-bbox="501 656 926 1036">  </div> <div data-bbox="426 1062 1299 1122" style="border: 2px solid red; padding: 5px;"> <p>When the payment succeeds, your device vibrates and you'll receive a confirmation on the screen.</p> </div> <p data-bbox="426 1133 1577 1193">See, e.g., <i>What should I know about using my Fitbit device to make contactless payments?</i> Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</p>
<p>3. The method of claim 1, further comprising receiving said confirmation result of said complete device payment information authentication status from a payment</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, receives said confirmation result of said complete device payment information authentication status from a payment processing authority (e.g., payment processor, token service provider) via at least one interface of a set of interfaces comprising: said device NFC interface (e.g., NFC chip on the device), a wireless interface (e.g., Wifi chip) of said device.</p>

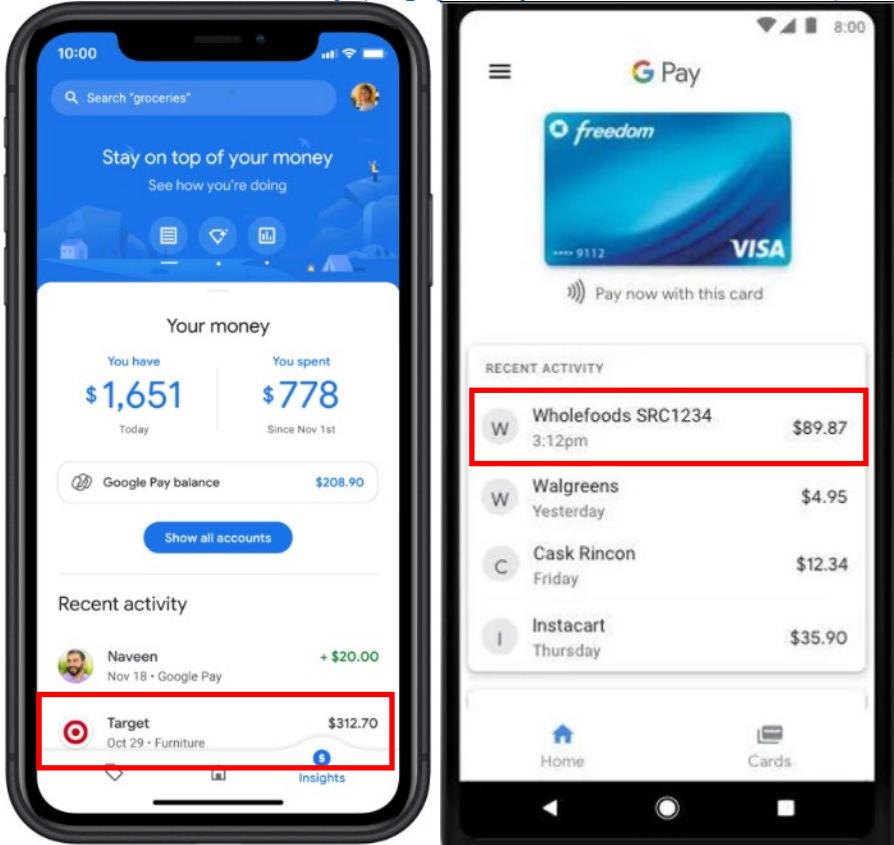
Claim No.	Accused Products
<p>processing authority via at least one interface of a set of interfaces comprising: said device NFC interface, a wireless interface of said device.</p>	<div data-bbox="422 225 1978 951"> <h3>5. End-to-End EMV Payment Tokenization Flows</h3> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> <ul style="list-style-type: none"> In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>The diagram illustrates the flow of a contactless EMV transaction using an NFC-enabled device-centric digital wallet. The process involves several entities: an NFC-Enabled Mobile Phone with a Device-Centric Wallet, a Merchant Contactless-Enabled POS Reader, a Merchant Acquirer/Processor, a Payment Network, an Issuer Processor, and an Issuer. The flow is numbered 1 through 11. A Confirmation Message (12) is sent from the Token Service Provider back to the mobile phone. The flow starts with the mobile phone sending a Payment Token (1) to the POS reader. The POS reader sends a Payment Token + Cryptogram (2) to the Merchant Acquirer/Processor. The Merchant Acquirer/Processor sends a Payment Token + Cryptogram (3) to the Payment Network. The Payment Network sends a Payment Token (4) to the Issuer Processor. The Issuer Processor sends a Payment Token (5) to the Issuer. The Issuer sends a PAN (6) to the Issuer Processor. The Issuer Processor sends a PAN (7) to the Payment Network. The Payment Network sends a PAN (8) to the Merchant Acquirer/Processor. The Merchant Acquirer/Processor sends a Payment Token + Last 4 (9) to the POS reader. The POS reader sends a Payment Token (10) to the mobile phone. The mobile phone sends a Payment Token (11) to the Token Service Provider. The Token Service Provider sends a Confirmation Message (12) back to the mobile phone.</p> <p>^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response</p> <p>^b Last 4 digits of the PAN may not always be returned to the merchant.</p> </div> <div data-bbox="422 971 1978 1164"> <p>Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet</p> <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 24 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf; <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), 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).</p> </div>

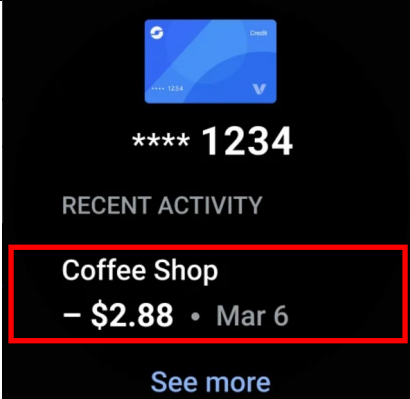
Claim No.	Accused Products
	<div><p>Step 2: Hold the back of your phone to the payment reader</p><p>When you're done paying, a blue tick will appear on the screen.</p><p>NFC Tap (success)</p><p>See, e.g., <i>Google Pay – Device Tokenization – TSP Integration – Google Pay Flows</i>, Google (May 2, 2024), https://developers.google.com/pay/issuers/tsp-integration/gpay-flows; <i>Pay contactless with your phone</i>, Google, https://support.google.com/wallet/answer/12060043 (Last visited December 8, 2024).</p></div> <div><p>See, e.g., <i>Made by Google, How to Use Google Wallet on Your Google Pixel Watch</i>, YouTube (Apr. 11, 2023), https://www.youtube.com/watch?v=Sa6ULG8MNUA; <i>Tap to pay with your smartwatch</i>, Google Wallet Help, https://support.google.com/wallet/answer/12059876.</p></div>

Claim No.	Accused Products
	 <p>When the payment succeeds, your device vibrates and you'll receive a confirmation on the screen.</p> <p><i>See, e.g., What should I know about using my Fitbit device to make contactless payments?</i> Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</p>
<p>4[a] The method of claim 3, wherein the generating the limited-use payment information utilizes a unique device generated information limited-in-use to said selected issuer-payment method, in payment transactions performed by said device, in place of said selected issuer-payment information; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]) generates the limited-use payment information (e.g., as identified above) utilizing a unique device generated information limited-in-use to said selected issuer-payment method (e.g., dynamic cryptogram), in payment transactions performed by said device, in place of said selected issuer-payment information (e.g., PAN or associated expiration date or CVV).</p> <p><i>See supra</i> limitation 1[f].</p> <p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant’s acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay’s security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token’s DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder’s mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p><i>See, e.g., Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Google Pay – Device Tokenization – TSP Integration</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</p>

Claim No.	Accused Products
<p>4[b] wherein said device account information will be rejected as invalid when not including a valid device generated limited-use information.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein said device account information will be rejected as invalid when not including a valid device generated limited-use information.</p> <p><i>See supra</i> limitation 1[i].</p> <p>4.2.4 Token Cryptogram and Key Management</p> <p>One primary function of the TSP is to act as the TSM and deliver tokens and associated EMV-based payment applications to token requestors. The delivery and coordination of the keys with the token requestor (either a mobile device manufacturer or a merchant for an online payment) ensures that an EMV-compliant set of transaction data is generated. Transactions are routed to the TSP providing the validation service to validate the cryptogram before going to the issuer for authorization. Depending on the options selected by the issuer, the TSP may reject the transaction if cryptogram validation fails.</p> <p><i>See, e.g.,</i> US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 24-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>
<p>5[a] The method of claim 3, wherein the generating of the limited-use payment information utilizes a secure combination of a device transaction sequence counter count, a device account number, a device-unique information, and a payment processing authority recognizable information; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein generating of the limited-use payment information (e.g., as identified above) utilizes a secure combination of a device transaction sequence counter count (e.g., transaction-unique value), a device account number (e.g., upon information and belief, a DPAN), a device-unique information (e.g., on information and belief, DPAN), and a payment processing authority recognizable information (e.g., limited-use key).</p> <p><i>See supra</i> limitation 1[f].</p> <p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant’s acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay’s security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token’s DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder’s mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device.

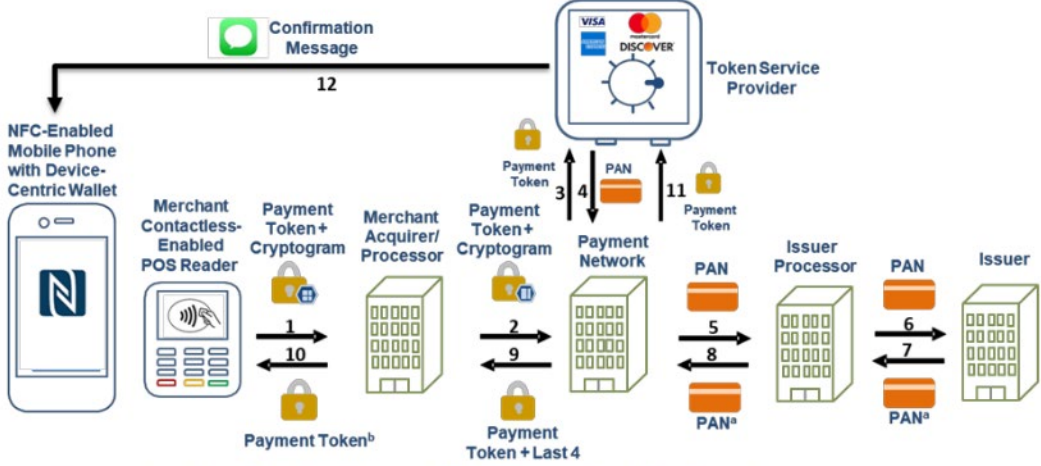
Claim No.	Accused Products		
	<p>See, e.g., <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Google Pay – Device Tokenization – TSP Integration</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</p> <p>3. Tokenization Use Case Scenarios</p> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p> <div>  <p>EMVCo Security Evaluation Certificate Mobile Application</p> <p>Please accept this document as confirmation of the EMVCo Software-Based Mobile Payments Security Evaluation Process.</p> <p>Evaluation Certificate Number: SECN0069.03</p> <p>Date SECN Issued: 22 Apr 2021 Next security review due: 22 Apr 2025</p> <p>Company Name: Google, LLC Address: 1600 Amphitheatre Pkwy Mountain View, CA 94043 United States of America</p> <p>Product Name: Google Wallet</p> <p>See, e.g., <i>EMVCo Security Evaluation Certificate Mobile Application</i>, https://www.emvco.com/wp-content/uploads/loa/EMVCo_SECN0069.03_N_08_2024-15.pdf (Last visited December 4, 2024).</p> </div>	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.
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.		

Claim No.	Accused Products
	<p>How is this an issue specific to EMV? When a merchant stores and forwards EMV chip or tokenized mobile wallet transactions, the Application Transaction Counter (ATC) that provides a sequential reference to each transaction becomes be out of sync and Issuers decline the transaction. An ATC does not come into play with magnetic strip transactions. The ATC is a sequence number that is tracked like a counter on each EMV chip card/mobile wallet transaction. Issuers use the ATC number as a fraud detection tool and an out of sequence can indicate a potentially fraudulent transaction. For example, in a SAF scenario the issuer sees transactions 1, 2, 4, 5 followed by a 3. The transaction with the 3 (which was stored and forwarded once available) is declined by the issuer since it is expecting a 6.</p> <p>See, e.g., Evolution in Payments: EMV is Not the Only Three Letter Word in This Story (MAG Quarterly- Volume Five, Issue Three), https://www.merchantadvisorygroup.org/news/mag-insights/article/2020/11/10/evolution-in-payments-emv-is-not-the-only-three-letter-word-in-this-story-(mag-quarterly--volume-five-issue-three).</p>  <p>See, e.g., Google Pay reimaged: pay, save, manage expenses and more, Google Pay, https://blog.google/products/google-pay/reimagined-pay-save-manage-expenses-and-more/; 6 things you should know about the new Google Pay app, CNET, https://www.cnet.com/tech/services-and-software/things-you-should-know-about-the-new-google-pay-app/.</p>

Claim No.	Accused Products		
	 <p>See, e.g., Google Play, Google Wallet, https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfc&hl=en_US.</p>		
5[b] wherein said generating of said limited-use payment information, is authorizable for a payment, for the singular counted transaction, for said selected payment method, by said device, in said transaction; and,	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein said generating of said limited-use payment information, is authorizable for a payment, for the singular counted transaction (e.g., based on a transaction-unique value), for said selected payment method, by said device, in said transaction.</p> <p>See <i>supra</i> limitation 1[f].</p> <h3>3. Tokenization Use Case Scenarios</h3> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p>	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.
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.		

Claim No.	Accused Products
	<div data-bbox="451 261 816 345">  </div> <div data-bbox="852 261 1419 345"> <p>EMVCo Security Evaluation Certificate Mobile Application</p> </div> <div data-bbox="474 378 1383 427"> <p>Please accept this document as confirmation of the EMVCo Software-Based Mobile Payments Security Evaluation Process.</p> </div> <div data-bbox="445 472 928 500"> <p>Evaluation Certificate Number: SECN0069.03</p> </div> <div data-bbox="445 513 753 540"> <p>Date SECN Issued: 22 Apr 2021</p> </div> <div data-bbox="1014 513 1392 540"> <p>Next security review due: 22 Apr 2025</p> </div> <div data-bbox="445 557 747 584"> <p>Company Name: Google, LLC</p> </div> <div data-bbox="445 586 1159 643"> <p>Address: 1600 Amphitheatre Pkwy Mountain View, CA 94043 United States of America</p> </div> <div data-bbox="445 654 743 682"> <p>Product Name: Google Wallet</p> </div> <div data-bbox="420 683 1593 751"> <p>See, e.g., <i>EMVCo Security Evaluation Certificate Mobile Application</i>, https://www.emvco.com/wp-content/uploads/loa/EMVCo_SECN0069.03_N_08_2024-15.pdf (Last visited December 4, 2024).</p> </div> <div data-bbox="432 790 1866 992"> <p>How is this an issue specific to EMV? When a merchant stores and forwards EMV chip or tokenized mobile wallet transactions, the Application Transaction Counter (ATC) that provides a sequential reference to each transaction becomes be out of sync and Issuers decline the transaction. An ATC does not come into play with magnetic strip transactions. The ATC is a sequence number that is tracked like a counter on each EMV chip card/mobile wallet transaction. Issuers use the ATC number as a fraud detection tool and an out of sequence can indicate a potentially fraudulent transaction. For example, in a SAF scenario the issuer sees transactions 1, 2, 4, 5 followed by a 3. The transaction with the 3 (which was stored and forwarded once available) is declined by the issuer since it is expecting a 6.</p> </div> <div data-bbox="420 1006 1988 1109"> <p>See, e.g., <i>Evolution in Payments: EMV is Not the Only Three Letter Word in This Story</i> (MAG Quarterly- Volume Five, Issue Three), https://www.merchantadvisorygroup.org/news/mag-insights/article/2020/11/10/evolution-in-payments-emv-is-not-the-only-three-letter-word-in-this-story-(mag-quarterly--volume-five-issue-three).</p> </div>
<p>5[c] wherein an authorizing by said payment processing authority, is a comparing of said device-generated limited-use payment information, to a valid transaction payment information generated by said payment</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein an authorizing by said payment processing authority (e.g., payment processor or TSP), is a comparing of said device-generated limited-use payment information, to a valid transaction payment information generated by said payment processing authority using same secure combination method, and same information elements of a valid payment transaction by said device.</p> <p>See <i>supra</i> limitation 1[j].</p> <div data-bbox="445 1352 1436 1430"> <p>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: [. . .]</p> </div>

Claim No.	Accused Products
<p>processing authority using same secure combination method, and same information elements of a valid payment transaction by said device; and,</p>	<p>4. The payment network determines that it is a token and not a PAN, as the token has a specific BIN. It thereby routes the transaction to the related Token Service Provider (TSP).</p> <p>5. The TSP validates the token, the related cryptogram, the Token Requestor (TR) identifier and the Token Domain usage restrictions. If everything is correct, proceed with de-tokenization and sends the original PAN data to the payment network.</p> <div data-bbox="422 532 1360 1073"> </div> <p>See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details.</p> <h3>5. End-to-End EMV Payment Tokenization Flows</h3> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> <ul style="list-style-type: none"> In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)

Claim No.	Accused Products
	 <p>^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response ^b Last 4 digits of the PAN may not always be returned to the merchant.</p> <p>Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 24-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>
5[d] a generating at said valid payment information at a payment processing authority includes a processing authority storing of expected device transaction sequence counter count, expected issuer payment information, an expected a device user information, and the device account number; and,	A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein generating said valid payment information at a payment processing authority includes a processing authority (e.g., TSP) storing of expected device transaction sequence counter count (e.g., transaction-unique value), expected issuer payment information (e.g., limited-use keys), an expected a device user information (e.g., on information and belief account information, phone number, serial number, IMEI), and the device account number (e.g., upon information and belief, a DPAN). See <i>supra</i> limitations 1[j], 5[b]. 5[c].

Claim No.	Accused Products
	<p data-bbox="426 232 947 266">5.0 Secure Limited-Use Key Storage</p> <p data-bbox="426 293 569 321">5.1 Context</p> <div data-bbox="426 345 1335 480" style="border: 2px solid red; padding: 5px;"> <p data-bbox="426 345 1335 464">Conventional provisioning of credit card information to a device (whether tokenized or not) involves storing a Master Key on a trusted piece of hardware like a Secure Element. For the purpose of this document, it will be called Card Master Key (CMK). CMK is synonymous with Master Derivation Key (MDK).</p> </div> <p data-bbox="426 492 1356 605">The CMK serves as a long-term secret used to compute cryptographic dynamic verification codes (CVC3) are generated for MSD transactions and ARQC (Online Authorization Request) cryptograms are generated for EMV transactions. These are verified by the issuer during issuer authorization.</p> <p data-bbox="426 610 1959 740"><i>See, e.g.,</i> Google, <i>Google Pay Security Paper</i> (Ver. 2.4, Jan. 2022) available at https://developers.google.com/wallet/access/campus-id/resources/Google_Pay_Security_Paper_2.4.pdf; <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Payment data cryptography for merchants</i>, Google Pay for Payments (Oct. 28, 2024), https://developers.google.com/pay/api/android/guides/resources/payment-data-cryptography.</p> <p data-bbox="447 784 1089 818">4.2.1 HCE with Virtual Cloud-Based SE</p> <p data-bbox="447 849 1871 1211">Android Pay uses HCE instead of the SE in a mobile phone and stores a master domain key representing the PAN in the cloud. Payment tokens and limited-use or single-use token keys (LUKs) generated by the master domain key in the cloud are stored in a secure area of the mobile OS, which uses software-based security, such as white box cryptography, to obfuscate the key. LUKs generate cryptograms that are passed with the EMV payment token for each transaction. The keys are refreshed each time the user connects to a network, which enables transactions to be completed without network connectivity. Rather than requesting a token from the cloud each time it is needed to make a payment, solutions using LUKs address the possibility that an Internet connection might not be available to download a token. LUKs also are restricted and expire quickly, to minimize their value to fraudsters.</p> <p data-bbox="426 1243 1953 1341"><i>See, e.g.,</i> U.S. Payments Forum, <i>Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions</i>, Version 1.0, January 2018, https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf</p>

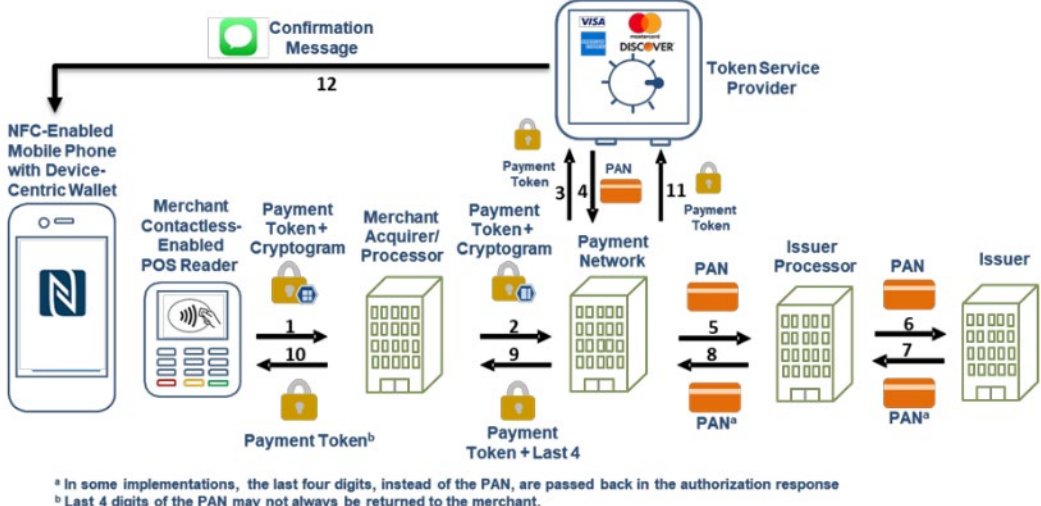
Claim No.	Accused Products		
	<p>The original PAN of the card is never stored on the end user's device. Instead, the payment token with which subsequent transactions are made is securely stored. Let's walk through this: [. . .]</p> <p>4. The payment network determines that it is a token and not a PAN, as the token has a specific BIN. It thereby routes the transaction to the related Token Service Provider (TSP).</p> <p>5. The TSP validates the token, the related cryptogram, the Token Requestor (TR) identifier and the Token Domain usage restrictions. If everything is correct, proceed with de-tokenization and sends the original PAN data to the payment network.</p> <p><i>See, e.g., Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details.</p>		
5[e] an adjusting of said transaction sequence counter count on a per transaction basis; and,	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, adjusts said transaction sequence counter count (e.g., transaction-unique value) on a per transaction basis (e.g., to ensure that the transaction-unique value is unique to a transaction).</p> <p>3. Tokenization Use Case Scenarios</p> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p><i>See, e.g., US Payments Forum, EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p><i>See, e.g., EMVCo, EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p>	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.
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.		

Claim No.	Accused Products
	<p>How is this an issue specific to EMV? When a merchant stores and forwards EMV chip or tokenized mobile wallet transactions, the Application Transaction Counter (ATC) that provides a sequential reference to each transaction becomes be out of sync and Issuers decline the transaction. An ATC does not come into play with magnetic strip transactions. The ATC is a sequence number that is tracked like a counter on each EMV chip card/mobile wallet transaction. Issuers use the ATC number as a fraud detection tool and an out of sequence can indicate a potentially fraudulent transaction. For example, in a SAF scenario the issuer sees transactions 1, 2, 4, 5 followed by a 3. The transaction with the 3 (which was stored and forwarded once available) is declined by the issuer since it is expecting a 6.</p> <p>See, e.g., Evolution in Payments: EMV is Not the Only Three Letter Word in This Story (MAG Quarterly- Volume Five, Issue Three), https://www.merchantadvisorygroup.org/news/mag-insights/article/2020/11/10/evolution-in-payments-emv-is-not-the-only-three-letter-word-in-this-story-(mag-quarterly--volume-five-issue-three).</p>
<p>5[f] an authorizing of a payment information as valid when said processing authority is verifying the limited-use transaction payment information generated by the device, and the processing authority generated valid limited-use payment transaction information, are matching.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein authorizing of a payment information as valid when said processing authority is verifying the limited-use transaction payment information generated by the device, and the processing authority (e.g., TSP) generated valid limited-use payment transaction information, are matching.</p> <p>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: [. . .]</p> <ol style="list-style-type: none"> 4. The payment network determines that it is a token and not a PAN, as the token has a specific BIN. It thereby routes the transaction to the related Token Service Provider (TSP). 5. The TSP validates the token, the related cryptogram, the Token Requestor (TR) identifier and the Token Domain usage restrictions. If everything is correct, proceed with de-tokenization and sends the original PAN data to the payment network. <p>See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details.</p>
<p>6[a] The method of claim 3, wherein the generating the limited-use payment information further utilizes a secure combination of said</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein generating the limited-use payment information further utilizes a secure combination of said information with a device account number (e.g., upon information and belief, a DPAN), a device sequence counter count (e.g., transaction-unique value), device-specific information (e.g., serial number, IMEI, etc.), payment processing authority specific information.</p>

Claim No.	Accused Products
<p>information with a device account number, a device sequence counter count, device-specific information, payment processing authority specific information; and,</p>	<p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant's acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay's security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token's DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder's mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p><i>See, e.g., Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Payment data cryptography for merchants</i>, Google Pay for Payments – Android (Oct. 28, 2024), https://developers.google.com/pay/api/android/guides/resources/payment-data-cryptography.</p> <p>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:</p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> • 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. <p><i>See, e.g., Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details.</p>

Claim No.	Accused Products		
	<p>Device tokenization</p> <p>When a user successfully adds their card to Google Pay, Google Pay stores a uniquely generated token on the device that has its own value. This new number, called a dynamic primary account number (DPAN) or device token, is similar to a credit card number.</p> <p>A DPAN improves account security because Google Pay passes it to a terminal during payment instead of the actual card number. In Google Pay, DPAN is referred as a 'virtual account number'. Users can only see the last four digits of this number, which are visible on the card details view in the Google Wallet app.</p> <p>See, e.g., <i>Enabling Google Pay device tokenization</i>, Google Pay, https://developers.google.com/pay/issuers/tsp-integration/overview.</p> <p>3. Tokenization Use Case Scenarios</p> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p> <p>How is this an issue specific to EMV? When a merchant stores and forwards EMV chip or tokenized mobile wallet transactions, the Application Transaction Counter (ATC) that provides a sequential reference to each transaction becomes out of sync and Issuers decline the transaction. An ATC does not come into play with magnetic strip transactions. The ATC is a sequence number that is tracked like a counter on each EMV chip card/mobile wallet transaction. Issuers use the ATC number as a fraud detection tool and an out of sequence can indicate a potentially fraudulent transaction. For example, in a SAF scenario the issuer sees transactions 1, 2, 4, 5 followed by a 3. The transaction with the 3 (which was stored and forwarded once available) is declined by the issuer since it is expecting a 6.</p> <p>See, e.g., <i>Evolution in Payments: EMV is Not the Only Three Letter Word in This Story</i> (MAG Quarterly- Volume Five, Issue Three), https://www.merchantadvisorygroup.org/news/mag-insights/article/2020/11/10/evolution-in-payments-emv-is-not-the-only-three-letter-word-in-this-story-(mag-quarterly--volume-five-issue-three).</p>	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.
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.		

Claim No.	Accused Products
6[b] a verifying of said combination by a payment processing authority, performing same secure combination of same information as retained at the authority; and,	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method comprising verifying of said combination by a payment processing authority (e.g., token service provider), performing same secure combination of same information as retained at the authority.</p> <ol style="list-style-type: none"> 3. The acquirer routes the transaction to the payment network in the same way as a normal transaction would proceed. 4. The payment network determines that it is a token and not a PAN, as the token has a specific BIN. It thereby routes the transaction to the related Token Service Provider (TSP). 5. The TSP validates the token, the related cryptogram, the Token Requestor (TR) identifier and the Token Domain usage restrictions. If everything is correct, proceed with de-tokenization and sends the original PAN data to the payment network. <p><i>See, e.g., Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details.</i></p> <p>5. End-to-End EMV Payment Tokenization Flows</p> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> <ul style="list-style-type: none"> • In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)

Claim No.	Accused Products
	 <p>Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 24-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>
<p>6[c] a payment processing authority comparing said device generated payment information, and said payment processing authority generated payment information, for a verifying of a limited-use payment as valid; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method comprising a payment processing authority (e.g., token service provider) comparing said device generated payment information, and said payment processing authority generated payment information, for a verifying of a limited-use payment as valid (e.g., “if everything is correct”).</p>

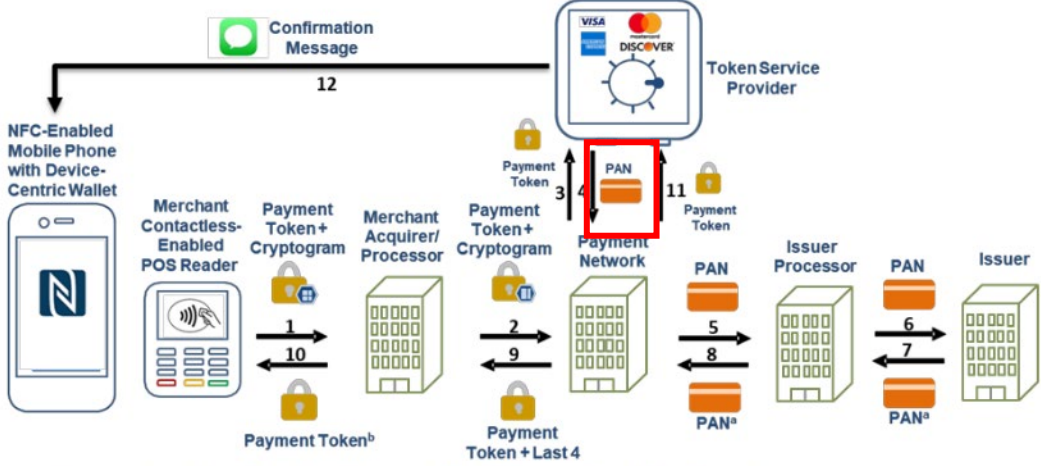
Claim No.	Accused Products
	<p>3. The acquirer routes the transaction to the payment network in the same way as a normal transaction would proceed.</p> <p>4. The payment network determines that it is a token and not a PAN, as the token has a specific BIN. It thereby routes the transaction to the related Token Service Provider (TSP).</p> <p>5. The TSP validates the token, the related cryptogram, the Token Requestor (TR) identifier and the Token Domain usage restrictions. If everything is correct, proceed with de-tokenization and sends the original PAN data to the payment network.</p> <p><i>See, e.g., Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details.</i></p> <p>5. End-to-End EMV Payment Tokenization Flows</p> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> <ul style="list-style-type: none">• In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)

<p>Claim No.</p>	<p>Accused Products</p> <p>Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet</p> <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 24-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>
<p>6[d] a conveying of said validation result as a declining or accepting of said transaction payment; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method comprising conveying of said validation result as a declining or accepting of said transaction payment (e.g., issuer validates the transaction and sends the response to the payment network).</p>

Claim No.	Accused Products
	<p>5. The TSP validates the token, the related cryptogram, the Token Requestor (TR) identifier and the Token Domain usage restrictions. If everything is correct, proceed with de-tokenization and sends the original PAN data to the payment network.</p> <p>6. The payment network sends the original PAN data to the sender.</p> <p>7. The issuer validates the transaction with the original PAN data and sends the response to the payment network.</p> <p>8. The payment network replaces the original PAN with the payment token initially received and sends it to the acquirer.</p> <p>9. The acquirer notifies the merchant of the result of the transaction.</p> <p><i>See, e.g., Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details.</p> <p>5. End-to-End EMV Payment Tokenization Flows</p> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> <ul style="list-style-type: none"> In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)

Claim No.	Accused Products
	<p>Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 24-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>
6[e] upon a proper validating of said result, a conveying of original issuer payment information to an original payment method issuer, for a settlement of said transaction.	A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method comprising upon a proper validating of said result, a conveying of original issuer payment information to an original payment method issuer, for a settlement of said transaction (e.g., acquirer notifies the merchant of the result of the transaction).

Claim No.	Accused Products
	<p>5. The TSP validates the token, the related cryptogram, the Token Requestor (TR) identifier and the Token Domain usage restrictions. If everything is correct, proceed with de-tokenization and sends the original PAN data to the payment network.</p> <p>6. The payment network sends the original PAN data to the sender.</p> <p>7. The issuer validates the transaction with the original PAN data and sends the response to the payment network.</p> <p>8. The payment network replaces the original PAN with the payment token initially received and sends it to the acquirer.</p> <p>9. The acquirer notifies the merchant of the result of the transaction.</p> <p><i>See, e.g., Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details.</p> <p>5. End-to-End EMV Payment Tokenization Flows</p> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> <ul style="list-style-type: none"> In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)

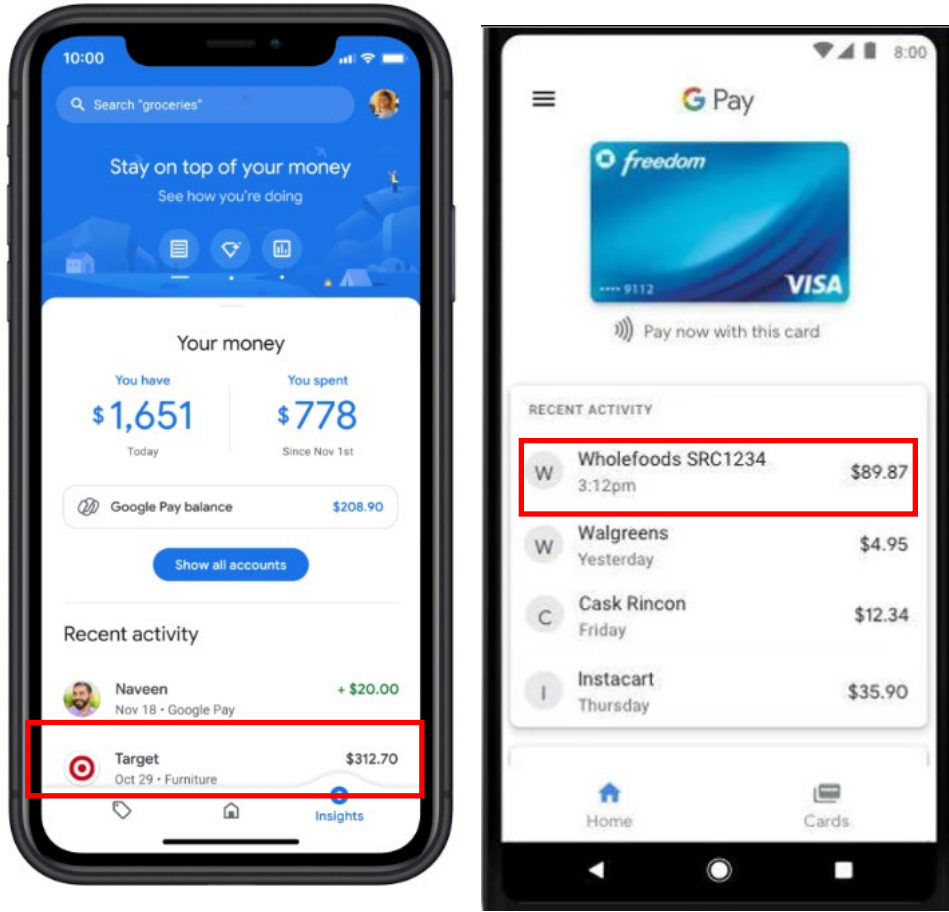
Claim No.	Accused Products
	 <p>^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response ^b Last 4 digits of the PAN may not always be returned to the merchant.</p> <p>Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 24-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>
<p>7. The method of claim 3, wherein the visual conveying of the transaction status is further comprising at least one, of a set of visual information including:</p> <p>a confirmation result of payment authority authenticating said device-transmitted limited-use payment information,</p> <p>a confirmation result of payment authority authenticating said</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein the visual conveying of the transaction status is further comprising at least one, of a set of visual information including: a confirmation result of payment authority authenticating said device-transmitted limited-use payment information, a confirmation result of payment authority authenticating said device-transmitted complete device payment information, an NFC transaction status (e.g., NFC tap success), a transaction payment amount, a payment facility wherein the transaction was performed, a merchant information, an original issuer payment account information, an original payment issuer information, a request for an authorized-user approval of the transaction, a payment processing status, an issuer payment approval status, and a payment completion status (e.g., blue tick).</p>

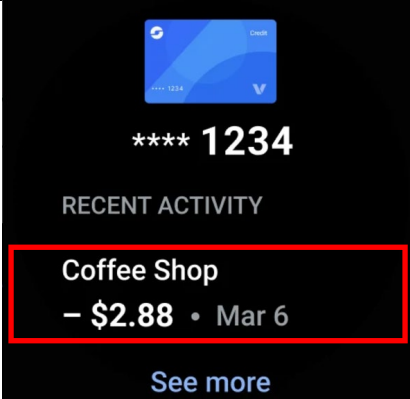
Claim No.	Accused Products
device-transmitted complete device payment information, an NFC transaction status, a transaction payment amount, a payment facility wherein the transaction was performed, a merchant information, an original issuer payment account information, an original payment issuer information, a request for an authorized-user approval of the transaction, a payment processing status, an issuer payment approval status, and a payment completion status.	<div data-bbox="426 228 688 794" data-label="Image"> </div> <p>Step 2: Hold the back of your phone to the payment reader</p> <p>When you're done paying a blue tick will appear on the screen.</p> <p>NFC Tap (success)</p> <p>See, e.g., <i>Google Pay – Device Tokenization – TSP Integration – Google Pay Flows</i>, Google (May 2, 2024), https://developers.google.com/pay/issuers/tsp-integration/gpay-flows; <i>Pay contactless with your phone</i>, Google, https://support.google.com/wallet/answer/12060043 (Last visited December 8, 2024).</p> <div data-bbox="426 993 997 1317" data-label="Image"> </div> <p>See, e.g., <i>Made by Google, How to Use Google Wallet on Your Google Pixel Watch</i>, YouTube (Apr. 11, 2023), https://www.youtube.com/watch?v=Sa6ULG8MNUA; <i>Tap to pay with your smartwatch</i>, Google Wallet Help, https://support.google.com/wallet/answer/12059876.</p>

Claim No.	Accused Products
	<p>When the payment succeeds, your device vibrates and you'll receive a confirmation on the screen.</p> <p>See, e.g., <i>What should I know about using my Fitbit device to make contactless payments?</i> Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</p>
8[a] The method of claim 1, wherein the generating the limited-use payment information is comprising: a device-specific account number; and,	See Claims 1[e], 5[a]. Specifically, the Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, generates the limited-use payment information (e.g., the dynamic cryptogram) using a device-specific account number (e.g., upon information and belief, a DPAN).
8[b] a device-internal transaction sequence counter count; and,	See Claim 5[a]. Specifically, the Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, generates the limited-use payment information (e.g., the dynamic cryptogram) using a device-internal transaction sequence counter count (e.g., transaction-unique value).
8[c] an information unique to the user and device which does not pass in the transaction; and,	See Claim 5[a]. Specifically, the Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, generates the limited-use payment information (e.g., the dynamic cryptogram) using, on information and belief, information unique to the user and device (e.g., serial number, IMEI, etc.). On information and belief, such information does not pass in the transaction because the TSP stores such information.

Claim No.	Accused Products
	<p>4.2.5 Lifecycle Management</p> <p>Once a token is created, any changes to the PAN, token, device, or cardholder need to be controlled and updates sent through the tokenization ecosystem. The TSP makes access to the token lifecycle available to the issuer and token requestor and is responsible for notifying all parties of lifecycle changes. The token lifecycle is represented by different states. The TSP decides what activities are permitted in each state of a token’s lifecycle, and the lifecycle state may be subject to some level of token domain control.</p> <p>The token lifecycle and its expiration do not have to mirror the lifecycle and expiration of the PAN that token represents. A token can be suspended while the PAN is active. A PAN can expire but still be tokenized with an expiration date in the future.</p> <p><i>EMV Payment Tokenization Primer and Lessons Learned</i>, US Payments Forum at 17 (June 2019, version 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>
<p>8[d] at least one payment authority-supplied information which does not pass in the transaction, wherein the complete device payment information is only valid for use in place of an issuer payment method in authorizable payments when comprising all valid device generated limited-use information elements, and</p>	<p><i>See</i> Claim 5[a]. Specifically, the Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein at least one payment authority-supplied information (e.g., limited-use keys) which does not pass in the transaction, wherein the complete device payment information is only valid for use in place of an issuer payment method in authorizable payments when comprising all valid device generated limited-use information elements. On information and belief, such information does not pass in the transaction because the payment network generates and stores such information.</p> <p>4.2.1 HCE with Virtual Cloud-Based SE</p> <p>Android Pay uses HCE instead of the SE in a mobile phone and stores a master domain key representing the PAN in the cloud. Payment tokens and limited-use or single-use token keys (LUKs) generated by the master domain key in the cloud are stored in a secure area of the mobile OS, which uses software-based security, such as white box cryptography, to obfuscate the key. LUKs generate cryptograms that are passed with the EMV payment token for each transaction. The keys are refreshed each time the user connects to a network, which enables transactions to be completed without network connectivity. Rather than requesting a token from the cloud each time it is needed to make a payment, solutions using LUKs address the possibility that an Internet connection might not be available to download a token. LUKs also are restricted and expire quickly, to minimize their value to fraudsters.</p> <p><i>See, e.g., U.S. Payments Forum</i>, Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions, Version 1.0, January 2018, https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf</p>

Claim No.	Accused Products
	<p>4.2.5 Lifecycle Management</p> <p>Once a token is created, any changes to the PAN, token, device, or cardholder need to be controlled and updates sent through the tokenization ecosystem. The TSP makes access to the token lifecycle available to the issuer and token requestor and is responsible for notifying all parties of lifecycle changes. The token lifecycle is represented by different states. The TSP decides what activities are permitted in each state of a token’s lifecycle, and the lifecycle state may be subject to some level of token domain control.</p> <p>The token lifecycle and its expiration do not have to mirror the lifecycle and expiration of the PAN that token represents. A token can be suspended while the PAN is active. A PAN can expire but still be tokenized with an expiration date in the future.</p> <p><i>EMV Payment Tokenization Primer and Lessons Learned</i>, US Payments Forum at 17 (June 2019, version 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>
<p>8[e] wherein said generating is limiting in-scope-of-use said generated payment information, for said user-selected issuer payment method option, to a unique-per-device unique-per-use one-time transacting by said combining device; by combining said information elements including: said transaction-specific sequence count information, said device-specific information, said user-specific information, and said authority-specific information.</p>	<p><i>See</i> Claims 8[a], 8[b], 8[c], and 8[d]. Specifically, the generated payment information (<i>e.g.</i>, the dynamic cryptogram) is unique-per-device and unique-per-use because it is generated using transaction-specific sequence count information (<i>e.g.</i>, transaction-unique value), device-specific information (<i>e.g.</i>, the digital token), authority-specific information (<i>e.g.</i>, the limited-use key), and, on information and belief, user-specific information (<i>e.g.</i>, serial number, IMEI, etc.).</p>

Claim No.	Accused Products
9. The method of claim 8, wherein the generating the limited-use payment information further utilizes a secure combining of said information, by at least one processor of the device, into a singular cryptogram number, capable of passing in at least a portion of the device transaction payment information.	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein the generating the limited-use payment information further utilizes a secure combining of said information, by at least one processor of the device, into a singular cryptogram number (e.g., dynamic cryptogram), capable of passing in at least a portion of the device transaction payment information (e.g., transaction data).</p> <div>  <p>The image displays two smartphone screens side-by-side, both showing the Google Pay application interface. The left screen, titled 'Your money', shows a balance of \$1,651 and a recent transaction at Target for \$312.70, which is highlighted with a red rectangular box. The right screen, titled 'G Pay', shows a Visa card and a list of recent transactions, with the first transaction at Wholefoods for \$89.87 highlighted with a red rectangular box. Both screens have a bottom navigation bar with icons for Home and Cards.</p> <p><i>See, e.g., Google Pay reimaged: pay, save, manage expenses and more, Google Pay, https://blog.google/products/google-pay/reimagined-pay-save-manage-expenses-and-more/; 6 things you should know about the new Google Pay app, CNET, https://www.cnet.com/tech/services-and-software/things-you-should-know-about-the-new-google-pay-app/.</i></p> </div>

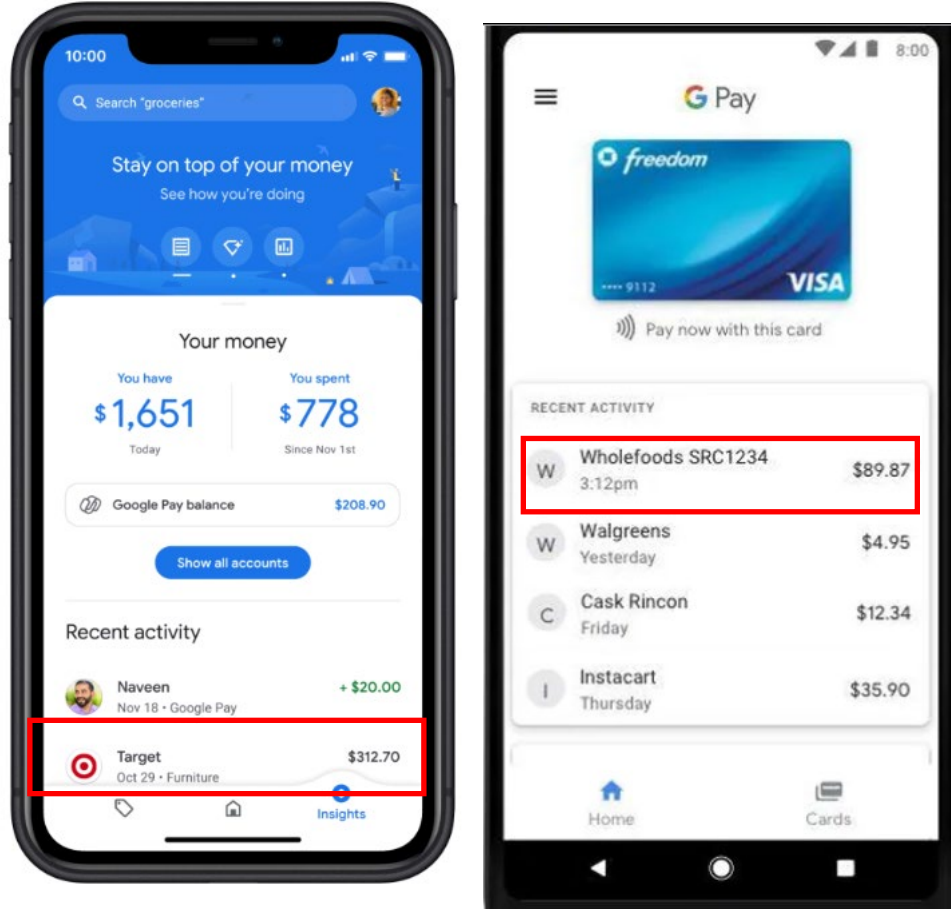
Claim No.	Accused Products		
	 <p>See, e.g., Google Play, Google Wallet, https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfcrel&hl=en_US.</p> <h3>3. Tokenization Use Case Scenarios</h3> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p>	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.
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.		
10. The method of claim 9, wherein the generating the limited-use payment information further utilizes a secure combination with a	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone or smartwatch, performs a method wherein the generating the limited-use payment information further utilizes a secure combination with a device key (e.g., limited-use keys), and a payment issuer secret (e.g., issuer secrets, keys).		

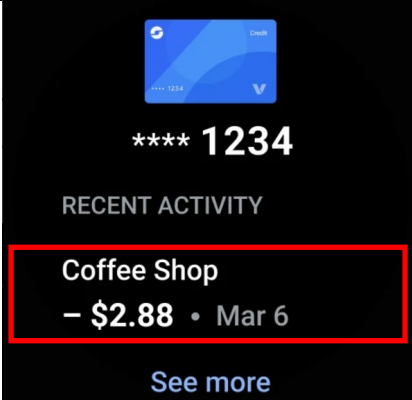
Claim No.	Accused Products
device key, and a payment issuer secret.	<p data-bbox="426 232 947 264">5.0 Secure Limited-Use Key Storage</p> <p data-bbox="426 293 569 318">5.1 Context</p> <div data-bbox="426 345 1335 480" style="border: 2px solid red; padding: 5px;"> <p data-bbox="426 345 1335 464">Conventional provisioning of credit card information to a device (whether tokenized or not) involves storing a Master Key on a trusted piece of hardware like a Secure Element. For the purpose of this document, it will be called Card Master Key (CMK). CMK is synonymous with Master Derivation Key (MDK).</p> </div> <p data-bbox="426 492 1356 602">The CMK serves as a long-term secret used to compute cryptographic dynamic verification codes (CVC3) are generated for MSD transactions and ARQC (Online Authorization Request) cryptograms are generated for EMV transactions. These are verified by the issuer during issuer authorization.</p> <p data-bbox="426 610 1961 737"><i>See, e.g., Google, Google Pay Security Paper (Ver. 2.4, Jan. 2022) available at https://developers.google.com/wallet/access/campus-id/resources/Google_Pay_Security_Paper_2.4.pdf; Google Pay – Device Tokenization – Security, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; Payment data cryptography for merchants, Google Pay for Payments (Oct. 28, 2024), https://developers.google.com/pay/api/android/guides/resources/payment-data-cryptography.</i></p> <p data-bbox="447 784 1089 816">4.2.1 HCE with Virtual Cloud-Based SE</p> <div data-bbox="447 846 1875 1045" style="border: 2px solid red; padding: 5px;"> <p data-bbox="447 846 1875 1045">Android Pay uses HCE instead of the SE in a mobile phone and stores a master domain key representing the PAN in the cloud. Payment tokens and limited-use or single-use token keys (LUKs) generated by the master domain key in the cloud are stored in a secure area of the mobile OS, which uses software-based security, such as white box cryptography, to obfuscate the key. LUKs generate cryptograms that are passed with the EMV payment token for each transaction. The keys are refreshed each time the user connects to a network, which enables transactions to be completed without network connectivity.</p> </div> <p data-bbox="447 1097 1808 1208">Rather than requesting a token from the cloud each time it is needed to make a payment, solutions using LUKs address the possibility that an Internet connection might not be available to download a token. LUKs also are restricted and expire quickly, to minimize their value to fraudsters.</p> <p data-bbox="426 1243 1955 1338"><i>See, e.g., U.S. Payments Forum, Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions, Version 1.0, January 2018, https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf</i></p>

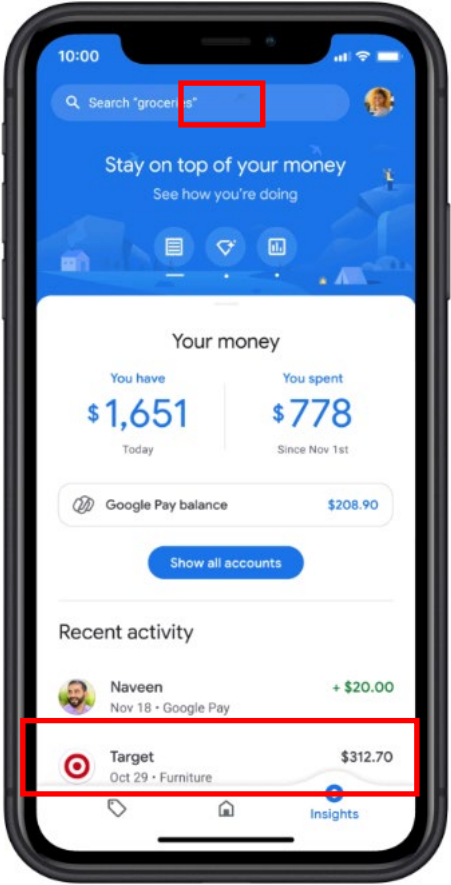
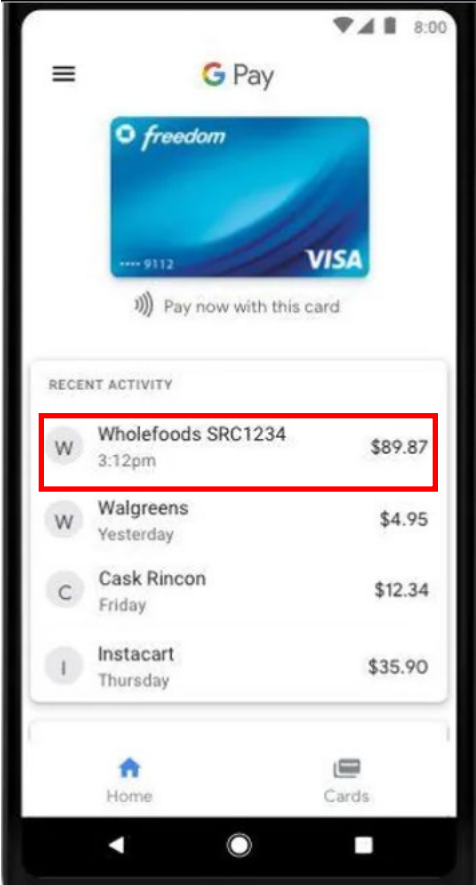
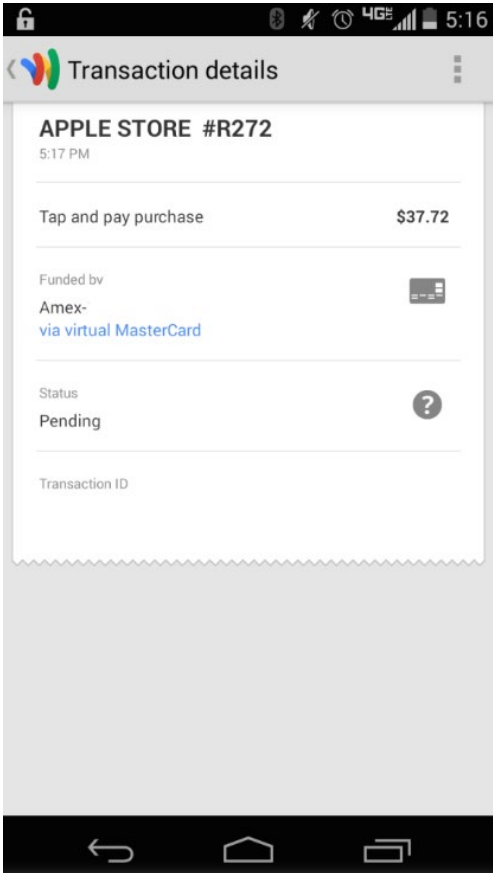
Claim No.	Accused Products		
11[a] The method of claim 1, wherein the generating the limited-use payment information further comprises securely combining by at least one processor of the device of: a device payment transaction sequence counter count, and	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein the generating the limited-use payment information further comprises securely combining by at least one processor of the device of: a device payment transaction sequence counter count (e.g., transaction-unique value).</p> <p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant’s acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay’s security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token’s DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder’s mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p>See, e.g., <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Google Pay – Device Tokenization – TSP Integration</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</p> <h3>3. Tokenization Use Case Scenarios</h3> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> • In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p>	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.
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.		

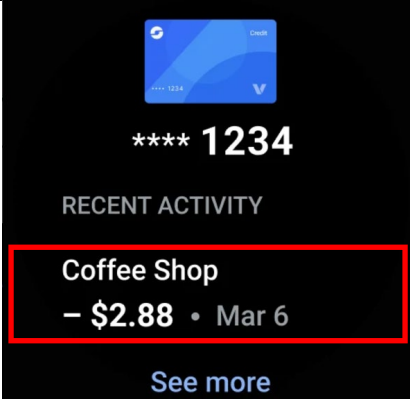
Claim No.	Accused Products
	<p>How is this an issue specific to EMV? When a merchant stores and forwards EMV chip or tokenized mobile wallet transactions, the Application Transaction Counter (ATC) that provides a sequential reference to each transaction becomes out of sync and Issuers decline the transaction. An ATC does not come into play with magnetic strip transactions. The ATC is a sequence number that is tracked like a counter on each EMV chip card/mobile wallet transaction. Issuers use the ATC number as a fraud detection tool and an out of sequence can indicate a potentially fraudulent transaction. For example, in a SAF scenario the issuer sees transactions 1, 2, 4, 5 followed by a 3. The transaction with the 3 (which was stored and forwarded once available) is declined by the issuer since it is expecting a 6.</p> <p>See, e.g., Evolution in Payments: EMV is Not the Only Three Letter Word in This Story (MAG Quarterly- Volume Five, Issue Three), https://www.merchantadvisorygroup.org/news/mag-insights/article/2020/11/10/evolution-in-payments-emv-is-not-the-only-three-letter-word-in-this-story-(mag-quarterly--volume-five-issue-three).</p>
<p>11[b] at least one of a set comprising: a device-specific internal information associated with said device and also known to a payment processing authority; and, at least one payment processing authority-specific information provided by a payment processing authority; and, a payment issuer specific information provided by a payment issuer.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone or smartwatch, performs a method wherein the generating the limited-use payment information further comprises securely combining by at least one processor of the device of: a device-specific internal information associated with said device and also known to a payment processing authority (e.g., DPAN); and at least one payment processing authority-specific information provided by a payment processing authority (e.g., limited-use keys, DPAN); and, a payment issuer specific information provided by a payment issuer (e.g., limited-use keys).</p> <p>4.2.1 HCE with Virtual Cloud-Based SE</p> <p>Android Pay uses HCE instead of the SE in a mobile phone and stores a master domain key representing the PAN in the cloud. Payment tokens and limited-use or single-use token keys (LUKs) generated by the master domain key in the cloud are stored in a secure area of the mobile OS, which uses software-based security, such as white box cryptography, to obfuscate the key. LUKs generate cryptograms that are passed with the EMV payment token for each transaction. The keys are refreshed each time the user connects to a network, which enables transactions to be completed without network connectivity. Rather than requesting a token from the cloud each time it is needed to make a payment, solutions using LUKs address the possibility that an Internet connection might not be available to download a token. LUKs also are restricted and expire quickly, to minimize their value to fraudsters.</p> <p>See, e.g., <i>U.S. Payments Forum</i>, Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions, Version 1.0, January 2018, https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf</p>

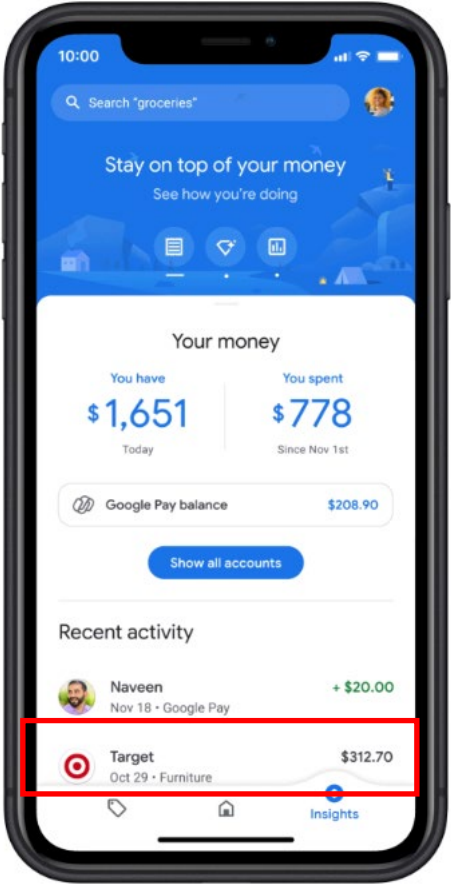
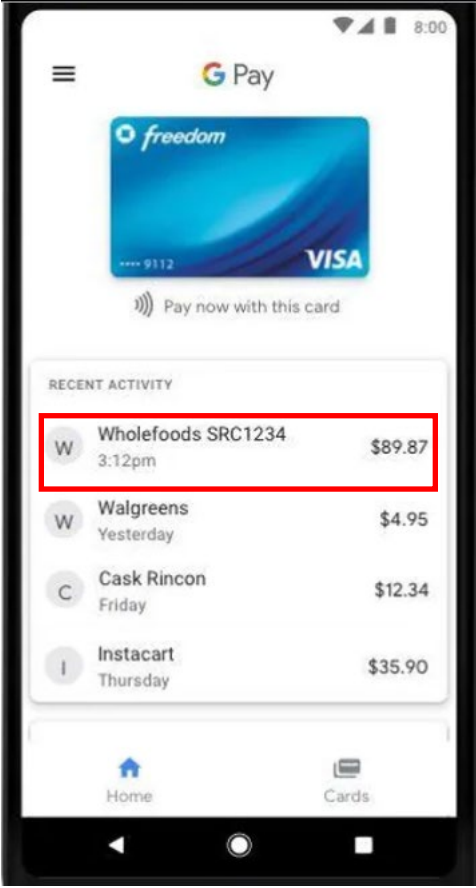
Claim No.	Accused Products
	<p>In general terms, the process for registering a card in a mobile wallet is as follows: [. . .]</p> <ol style="list-style-type: none"> 5. The TSP validates the token, the related cryptogram, the Token Requestor (TR) identifier and the Token Domain usage restrictions. If everything is correct, proceed with de-tokenization and sends the original PAN data to the payment network. 6. The payment network sends the original PAN data to the sender. 7. The issuer validates the transaction with the original PAN data and sends the response to the payment network. 8. The payment network replaces the original PAN with the payment token initially received and sends it to the acquirer. 9. The acquirer notifies the merchant of the result of the transaction. <p><i>See, e.g., Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details.</i></p>
<p>12. The method of claim 1, wherein the generating the limited-use payment information utilizes a recipient NFC facility provided information.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein the generating the limited-use payment information utilizes a recipient NFC facility provided information (e.g., store code, merchant ID).</p> <p>3. Tokenization Use Case Scenarios</p> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> • In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p><i>See, e.g., US Payments Forum, EMV Payment Tokenization Primer and Lessons Learned at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</i></p>

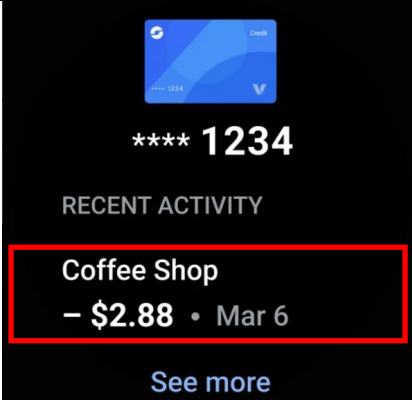
Claim No.	Accused Products
	<div> <div>Token Cryptogram</div> <div>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</div> </div> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p> <div>  <p>The image displays two smartphone screens side-by-side, both showing the Google Pay application interface. The left screen, titled 'Stay on top of your money', shows a summary of 'Your money' with 'You have \$1,651' and 'You spent \$778'. Below this, it lists 'Recent activity' with a transaction from 'Target' on Oct 29 for \$312.70, which is highlighted with a red rectangular box. The right screen shows a 'freedom VISA' card with the text 'Pay now with this card'. Below the card, it displays 'RECENT ACTIVITY' with a list of transactions: 'Wholefoods SRC1234' for \$89.87 (highlighted with a red box), 'Walgreens' for \$4.95, 'Cask Rincon' for \$12.34, and 'Instacart' for \$35.90.</p> </div> <p>See, e.g., <i>Google Pay reimaged: pay, save, manage expenses and more</i>, Google Pay, https://blog.google/products/google-pay/reimagined-pay-save-manage-expenses-and-more/; 6 things you should know about the new Google Pay app, CNET, https://www.cnet.com/tech/services-and-software/things-you-should-know-about-the-new-google-pay-app/.</p>

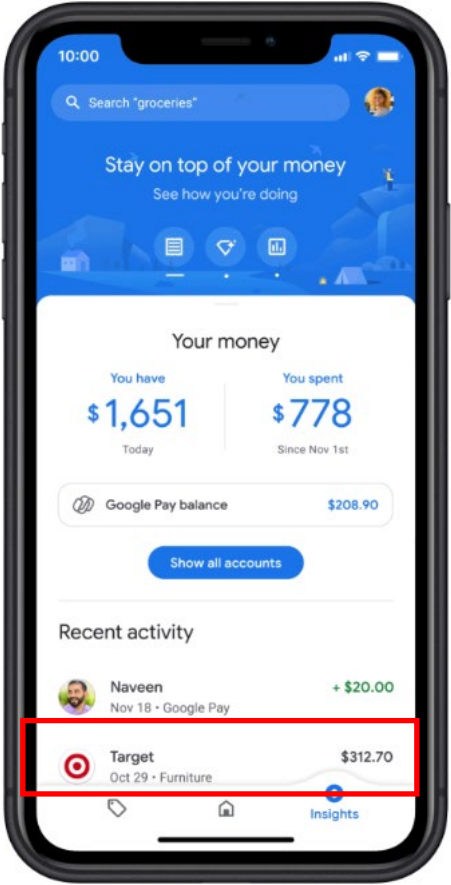
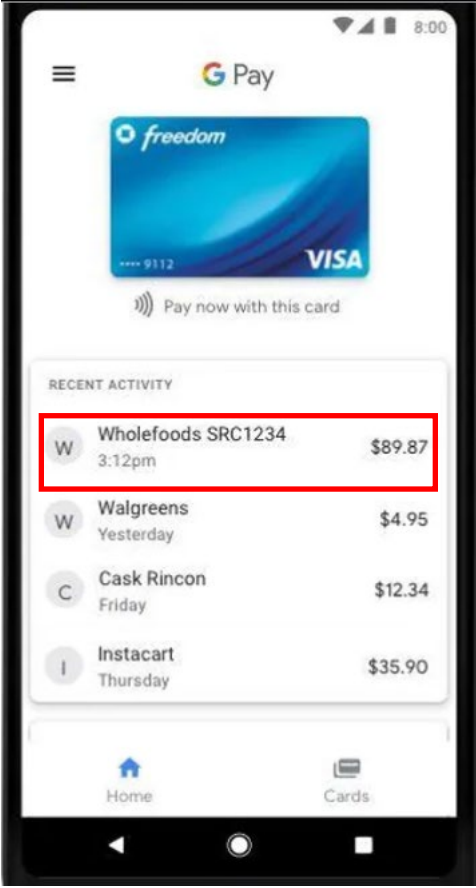
Claim No.	Accused Products		
	 <p>See, e.g., Google Play, Google Wallet, https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfc&hl=en_US.</p>		
13. The method of claim 1, wherein the generating the limited-use payment information utilizes a merchant identifying information.	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein the generating the limited-use payment information utilizes a merchant identifying information (e.g., store name, store code, merchant ID, etc.).</p> <h3>3. Tokenization Use Case Scenarios</h3> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p>	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.
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.		

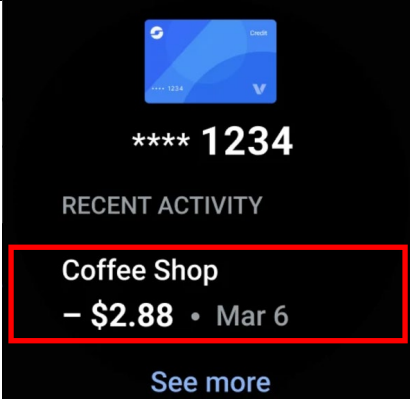
Claim No.	Accused Products
	<div></div> <p>See, e.g., <i>Google Pay reimaged: pay, save, manage expenses and more</i>, Google Pay, https://blog.google/products/google-pay/reimagined-pay-save-manage-expenses-and-more/; 6 things you should know about the new Google Pay app, CNET, https://www.cnet.com/tech/services-and-software/things-you-should-know-about-the-new-google-pay-app/; <i>Another place Google Wallet works alongside Apple Pay? Try the Apple Store</i>, https://phandroid.com/2014/10/29/google-wallet-works-at-the-apple-store/.</p>

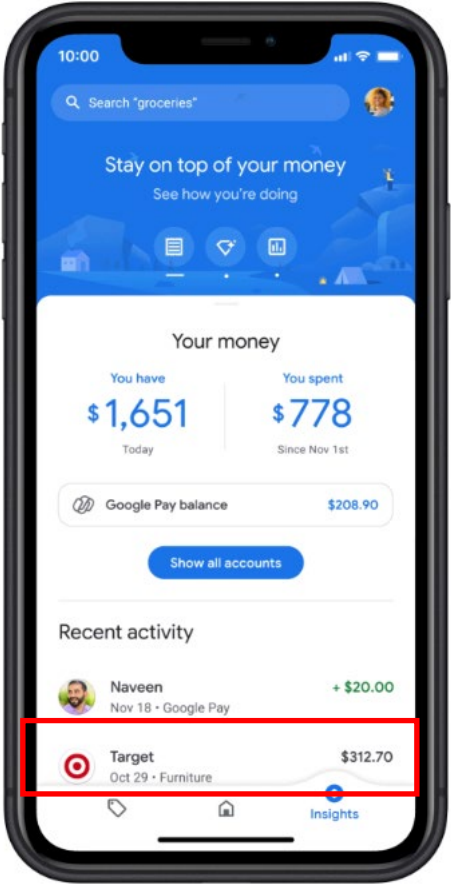
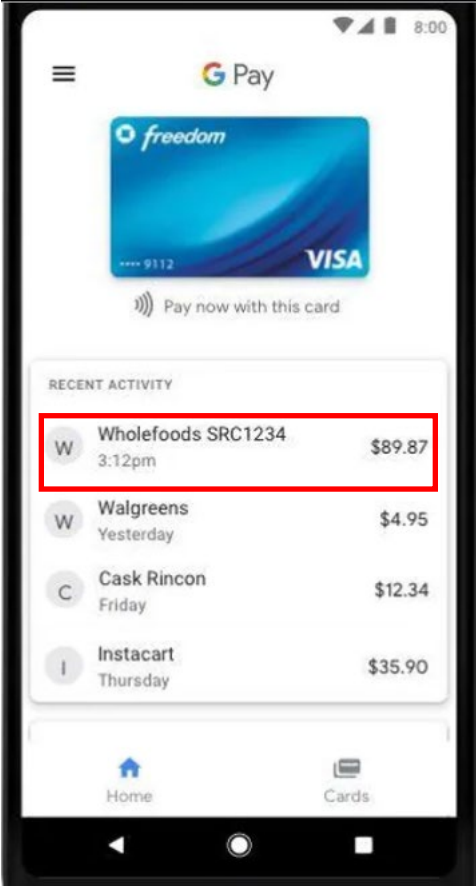
Claim No.	Accused Products		
	 <p>See, e.g., Google Play, Google Wallet, https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfc&hl=en_US.</p>		
14. The method of claim 1, wherein the generating the limited-use payment information utilizes a transaction facility information.	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein the generating the limited-use payment information utilizes a transaction facility information (e.g., store name, store code, merchant ID, etc.).</p> <h3>3. Tokenization Use Case Scenarios</h3> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table border="1" data-bbox="424 1130 1486 1302"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p>	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.
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.		

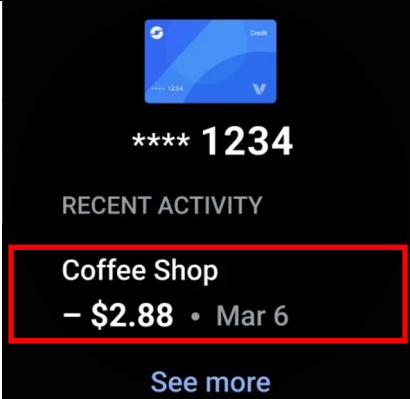
Claim No.	Accused Products
	<div></div> <p><i>See, e.g., Google Pay reimaged: pay, save, manage expenses and more, Google Pay, https://blog.google/products/google-pay/reimagined-pay-save-manage-expenses-and-more/; 6 things you should know about the new Google Pay app, CNET, https://www.cnet.com/tech/services-and-software/things-you-should-know-about-the-new-google-pay-app/.</i></p>

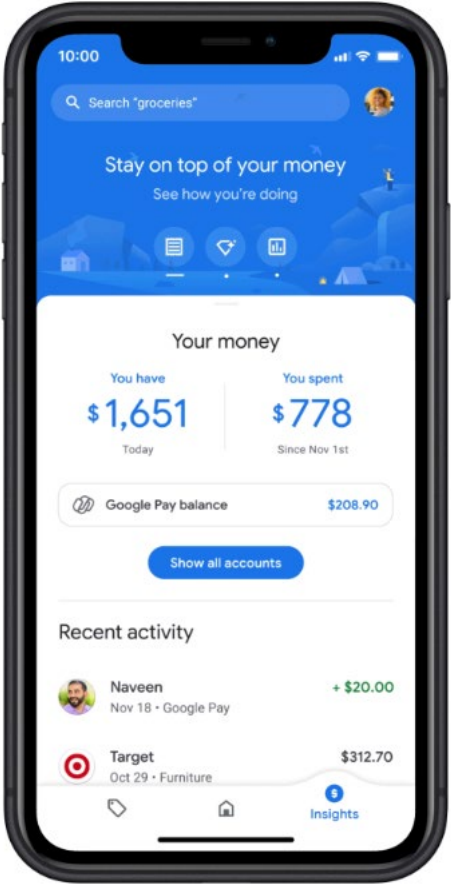
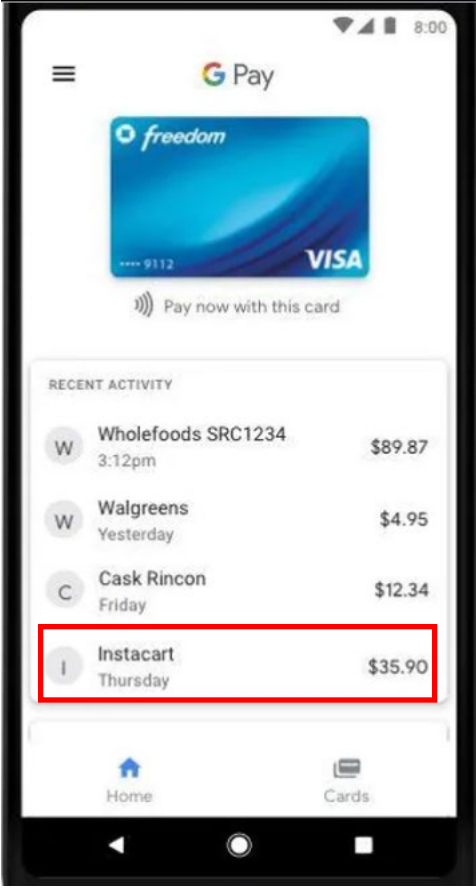
Claim No.	Accused Products		
	 <p>See, e.g., Google Play, Google Wallet, https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfc&hl=en_US.</p>		
15. The method of claim 1, wherein the generating the limited-use payment information utilizes a payment amount.	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre] , such as a smartphone or smartwatch, performs a method wherein the generating the limited-use payment information utilizes a payment amount (e.g., authorized amount).</p> <h3>3. Tokenization Use Case Scenarios</h3> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p>	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.
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.		

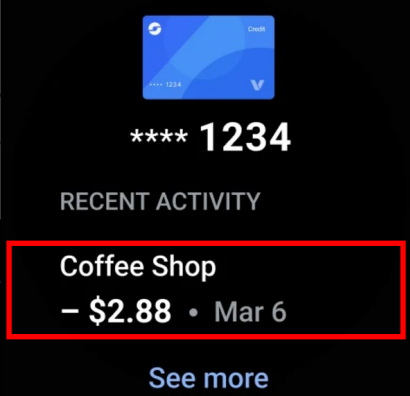
Claim No.	Accused Products
	<div></div> <p><i>See, e.g., Google Pay reimaged: pay, save, manage expenses and more, Google Pay, https://blog.google/products/google-pay/reimagined-pay-save-manage-expenses-and-more/; 6 things you should know about the new Google Pay app, CNET, https://www.cnet.com/tech/services-and-software/things-you-should-know-about-the-new-google-pay-app/.</i></p>

Claim No.	Accused Products		
	 <p>See, e.g., Google Play, Google Wallet, https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfc&hl=en_US.</p>		
16. The method of claim 1, wherein the generating the limited-use payment information utilizes a payment facility type.	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone or smartwatch, performs a method wherein the generating the limited-use payment information utilizes a payment facility type (e.g., retail store (e.g., Target) or grocery store (e.g., Wholefoods), or contactless terminal).</p> <h3>3. Tokenization Use Case Scenarios</h3> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p>	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.
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.		

Claim No.	Accused Products
	<div></div> <p><i>See, e.g., Google Pay reimaged: pay, save, manage expenses and more, Google Pay, https://blog.google/products/google-pay/reimagined-pay-save-manage-expenses-and-more/; 6 things you should know about the new Google Pay app, CNET, https://www.cnet.com/tech/services-and-software/things-you-should-know-about-the-new-google-pay-app/.</i></p>

Claim No.	Accused Products		
	 <p>See, e.g., Google Play, Google Wallet, https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfc&hl=en_US.</p>		
17. The method of claim 1, wherein the generating the limited-use payment information utilizes an online transaction information.	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein the generating the limited-use payment information utilizes an online transaction information (e.g., prior online transaction data (e.g., Instacart)).</p> <h3>3. Tokenization Use Case Scenarios</h3> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p>	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.
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.		

Claim No.	Accused Products
	<div></div> <p><i>See, e.g., Google Pay reimaged: pay, save, manage expenses and more, Google Pay, https://blog.google/products/google-pay/reimagined-pay-save-manage-expenses-and-more/; 6 things you should know about the new Google Pay app, CNET, https://www.cnet.com/tech/services-and-software/things-you-should-know-about-the-new-google-pay-app/.</i></p>

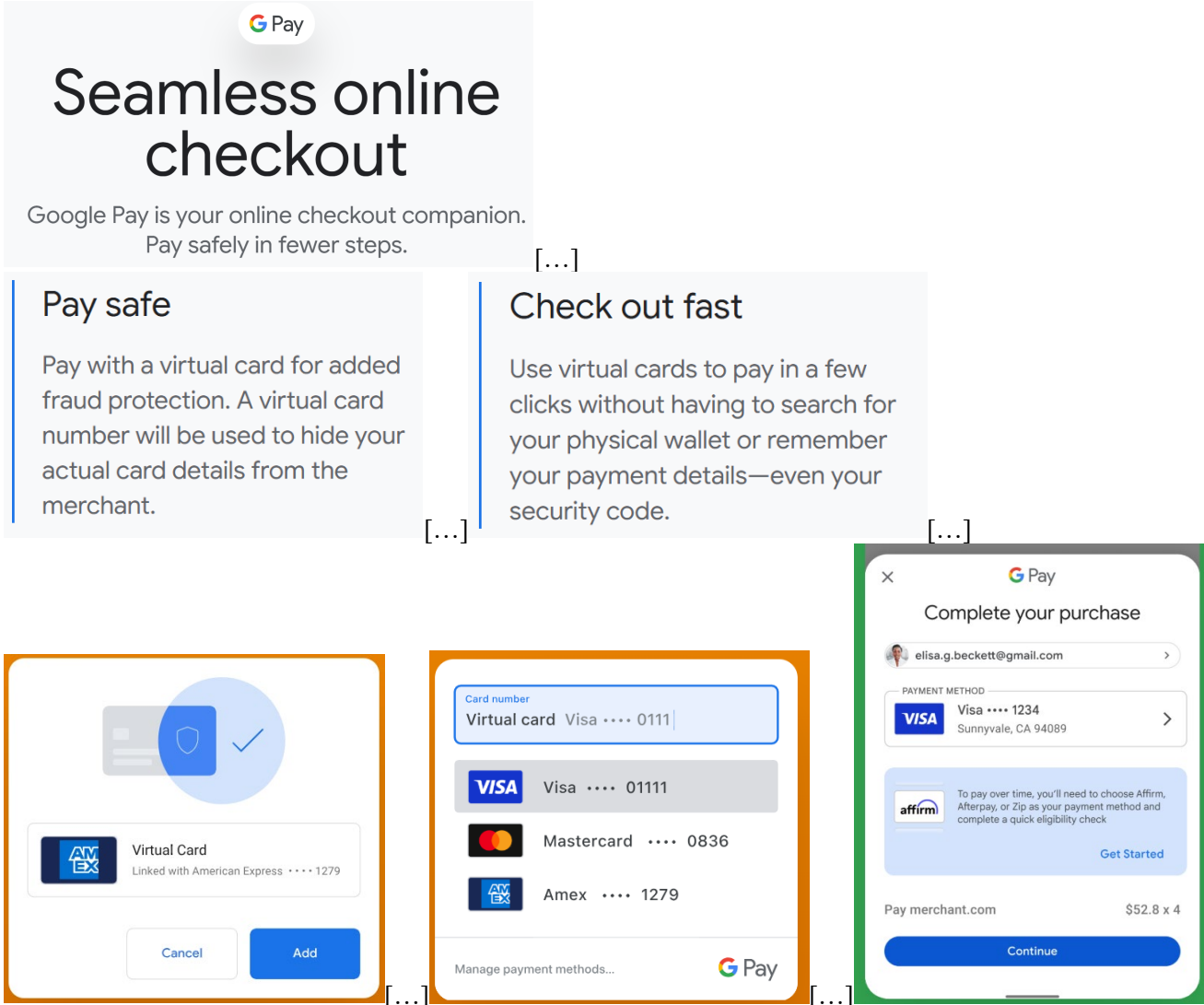
Claim No.	Accused Products
	 <p>See, e.g., Google Play, Google Wallet, https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfcrel&hl=en_US.</p>
<p>18[a] The method of claim 1, further comprising: dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the payment issuer, and wherein the dynamically generating the cryptogram number comprises cryptographically combining a transaction sequence counter count, payment processing authority secrets, and a device account number; and</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method comprising: dynamically generating a cryptogram number (e.g., dynamic cryptogram) for use by the electronic device in place of a card validation value (e.g., CVV) originated from the payment issuer, and wherein the dynamically generating the cryptogram number comprises cryptographically combining a transaction sequence counter count (e.g., transaction-unique value), payment processing authority secrets (e.g., secret key), and a device account number (e.g., upon information and belief, a DPAN).</p> <p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant’s acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay’s security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token’s DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder’s mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p>See, e.g., Google Pay – Device Tokenization – Security, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; Google Pay – Device Tokenization – TSP Integration, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</p>

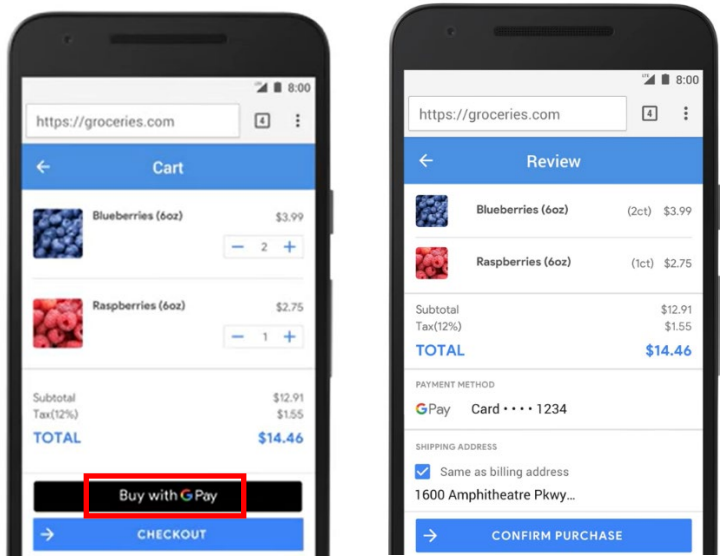
Claim No.	Accused Products
	<p>Device tokenization</p> <p>When a user successfully adds their card to Google Pay, Google Pay stores a uniquely generated token on the device that has its own value. This new number, called a dynamic primary account number (DPAN) or device token, is similar to a credit card number.</p> <p>A DPAN improves account security because Google Pay passes it to a terminal during payment instead of the actual card number. In Google Pay, DPAN is referred as a 'virtual account number'. Users can only see the last four digits of this number, which are visible on the card details view in the Google Wallet app.</p> <p>See, e.g., <i>Enabling Google Pay device tokenization</i>, Google Pay, https://developers.google.com/pay/issuers/tsp-integration/overview.</p> <p>3. Tokenization Use Case Scenarios</p> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> • In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <p>5.0 Secure Limited-Use Key Storage</p> <p>5.1 Context</p> <p>Conventional provisioning of credit card information to a device (whether tokenized or not) involves storing a Master Key on a trusted piece of hardware like a Secure Element. For the purpose of this document, it will be called Card Master Key (CMK). CMK is synonymous with Master Derivation Key (MDK).</p> <p>The CMK serves as a long-term secret used to compute cryptographic dynamic verification codes (CVC3) are generated for MSD transactions and ARQC (Online Authorization Request) cryptograms are generated for EMV transactions. These are verified by the issuer during issuer authorization.</p> <p>See, e.g., Google, <i>Google Pay Security Paper</i> (Ver. 2.4, Jan. 2022) available at https://developers.google.com/wallet/access/campus-id/resources/Google_Pay_Security_Paper_2.4.pdf; <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Payment data cryptography for merchants</i>, Google Pay for Payments (Oct. 28, 2024), https://developers.google.com/pay/api/android/guides/resources/payment-data-cryptography.</p>

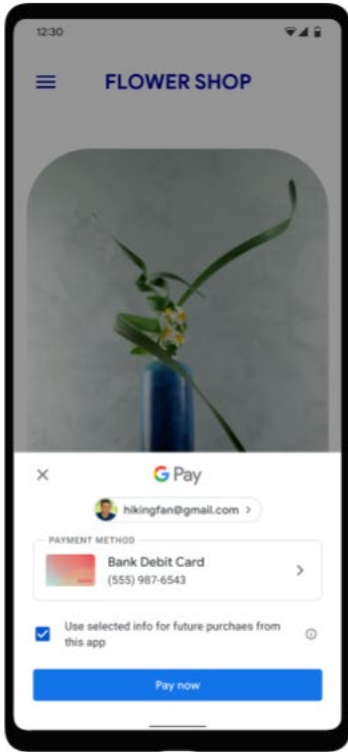
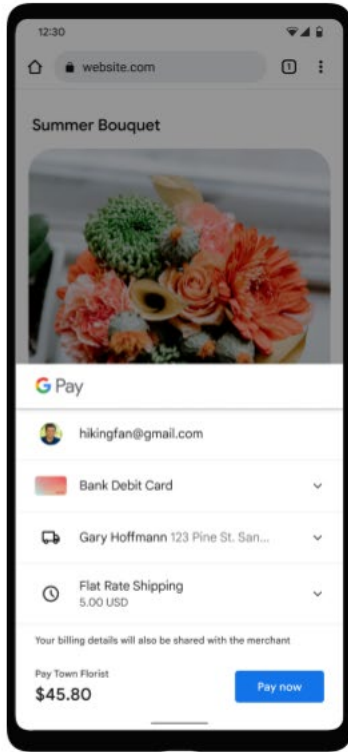
Claim No.	Accused Products		
	<table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p> <p>How is this an issue specific to EMV? When a merchant stores and forwards EMV chip or tokenized mobile wallet transactions, the Application Transaction Counter (ATC) that provides a sequential reference to each transaction becomes out of sync and Issuers decline the transaction. An ATC does not come into play with magnetic strip transactions. The ATC is a sequence number that is tracked like a counter on each EMV chip card/mobile wallet transaction. Issuers use the ATC number as a fraud detection tool and an out of sequence can indicate a potentially fraudulent transaction. For example, in a SAF scenario the issuer sees transactions 1, 2, 4, 5 followed by a 3. The transaction with the 3 (which was stored and forwarded once available) is declined by the issuer since it is expecting a 6.</p> <p>See, e.g., Evolution in Payments: EMV is Not the Only Three Letter Word in This Story (MAG Quarterly- Volume Five, Issue Three), https://www.merchantadvisorygroup.org/news/mag-insights/article/2020/11/10/evolution-in-payments-emv-is-not-the-only-three-letter-word-in-this-story-(mag-quarterly--volume-five-issue-three).</p> <p>6.6.3 Cardholder Verification</p> <p>Issuers may wish to implement host-based PINs for cardholder verification with tokenized card-present transactions. Issuers do not need to check the card security code (e.g., CSC, CVV, CID) but rely on the dynamic cryptogram validation by the TSP.</p> <p>US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 35 (June 2019) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>	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.
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.		
18[b] wherein further, said dynamically generating of said cryptogram results in a one-time limited-use card validation value number, via the incrementing of said transaction sequence counter count on a per-transaction basis, and	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein further, said dynamically generating of said cryptogram results in a one-time limited-use card validation value number (e.g., dynamic cryptogram), via the incrementing of said transaction sequence counter count on a per-transaction basis, and using said updated transaction sequence counter count in said generation of said cryptogram (e.g., using the transaction-unique value).</p> <p>See Claim 5[a], 5[b], 5[e].</p>		

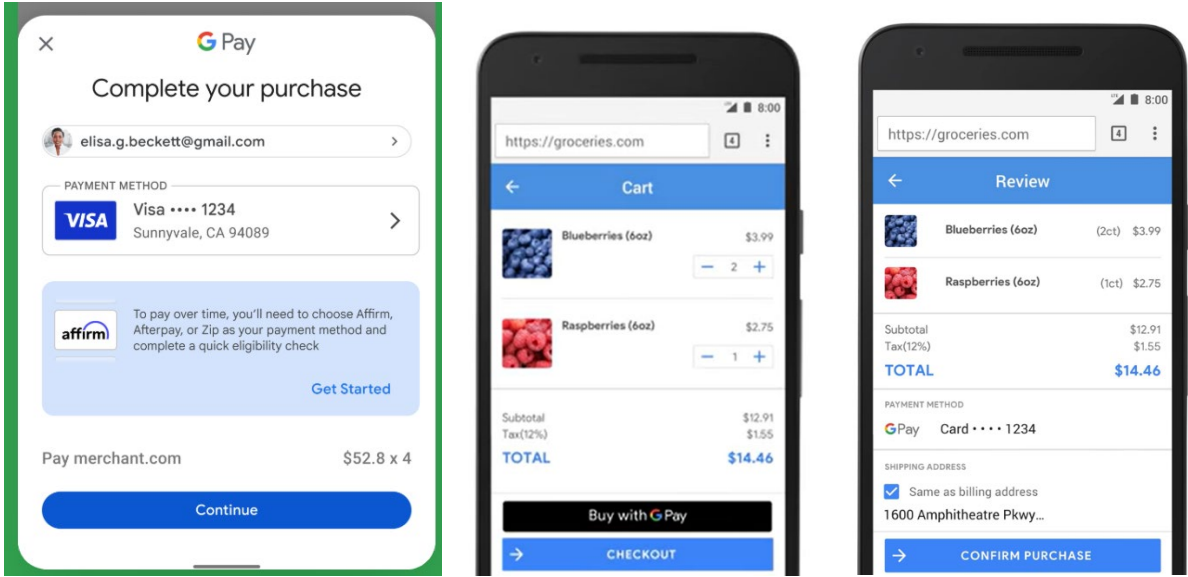
Claim No.	Accused Products
using said updated transaction sequence counter count in said generation of said cryptogram; and,	<p>How is this an issue specific to EMV? When a merchant stores and forwards EMV chip or tokenized mobile wallet transactions, the Application Transaction Counter (ATC) that provides a sequential reference to each transaction becomes out of sync and Issuers decline the transaction. An ATC does not come into play with magnetic strip transactions. The ATC is a sequence number that is tracked like a counter on each EMV chip card/mobile wallet transaction. Issuers use the ATC number as a fraud detection tool and an out of sequence can indicate a potentially fraudulent transaction. For example, in a SAF scenario the issuer sees transactions 1, 2, 4, 5 followed by a 3. The transaction with the 3 (which was stored and forwarded once available) is declined by the issuer since it is expecting a 6.</p> <p>See, e.g., Evolution in Payments: EMV is Not the Only Three Letter Word in This Story (MAG Quarterly- Volume Five, Issue Three), https://www.merchantadvisorygroup.org/news/mag-insights/article/2020/11/10/evolution-in-payments-emv-is-not-the-only-three-letter-word-in-this-story-(mag-quarterly--volume-five-issue-three).</p>
18[c] wherein said cryptogram is used in place of issuer supplied card validation value number, in performing said transaction payment by the device.	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone or smartwatch, performs a method wherein said cryptogram (e.g., dynamic cryptogram) is used in place of issuer supplied card validation value number (e.g., CVV), in performing said transaction payment by the device.</p> <p>See Claim 1[g].</p> <p>6.6.3 Cardholder Verification</p> <p>Issuers may wish to implement host-based PINs for cardholder verification with tokenized card-present transactions. Issuers do not need to check the card security code (e.g., CSC, CVV, CID) but rely on the dynamic cryptogram validation by the TSP.</p> <p>US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 35 (June 2019) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>

II. Claim 19 and Dependent Claims 20–24

Claim No.	Accused Products
19[Pre]: A method of performing an online payment transaction, the method comprising:	<p>To the extent the preamble is limiting, a Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs an online payment transaction. (see 1[pre])</p>  <p>See, e.g., <i>Seamless online checkout</i>, Google, https://pay.google.com/about/pay-online/.</p>

Claim No.	Accused Products
	<p>Just look for Google Pay at checkout in your favorite apps and sites. Finally, confirm your purchase.</p>  <p>See, e.g., <i>How do you pay online with Google Pay?</i>, Google Help, https://www.youtube.com/watch?v=yl5SGXiPnDY.</p> <p>In addition, Google induces other devices, through its Chrome browser, to perform a payment transaction.</p> <h3>Save your payment information in Google Pay</h3> <p>When you’re signed in to Chrome and you enter your payment method into an online form, Chrome may ask if you want to save your payment info in Google Pay. If you accept, your payment information is saved in Google Pay. If Google Pay doesn’t support your payment method, Chrome may offer to save it locally on your device.</p> <p>Payment methods saved in Google Pay show up as suggestions in most online forms.</p> <p>See, e.g., <i>Fill out forms automatically in Chrome</i>, Google, https://support.google.com/googlepay/answer/142893.</p>

Claim No.	Accused Products
	<div><div><p>NFC Tap (success)</p></div><div><p>In-app buy flow</p></div><div><p>Online buy flow</p></div></div> <p>See, e.g., Google Pay Flows, https://developers.google.com/pay/issuers/tsp-integration/gpay-flows.</p>

Claim No.	Accused Products
19[a]: receiving an input signal at an electronic device, the input signal corresponding to a request for payment of an online payment transaction by said electronic device, via a wireless interface of the electronic device;	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone, laptop, tablet, or smartwatch, receives an input signal (e.g., a request for online payment) at an electronic device, the input signal corresponding to a request for payment of an online payment transaction by said electronic device, via a wireless interface (e.g., Wi-Fi, LTE, 5G chip) of the electronic device.</p> <p>Just look for Google Pay at checkout in your favorite apps and sites.</p> <p>Finally, confirm your purchase.</p>  <p>See, e.g., <i>Seamless online checkout</i>, Google, https://pay.google.com/about/pay-online/; <i>How do you pay online with Google Pay?</i>, Google Help, https://www.youtube.com/watch?v=y15SGXiPnDY.</p> <p>Connect to Wi-Fi networks on your Pixel phone</p> <p>To use Wi-Fi the way you want, you can change how and when your device connects.</p> <p>When you have Wi-Fi turned on, your device automatically connects to nearby Wi-Fi networks you've connected to before. You can also set your device to automatically turn on Wi-Fi near saved networks.</p> <p>See, e.g., <i>Connect to Wi-Fi networks on your Pixel phone</i>, Pixel Phone Help, https://support.google.com/pixelphone/answer/2819519.</p>

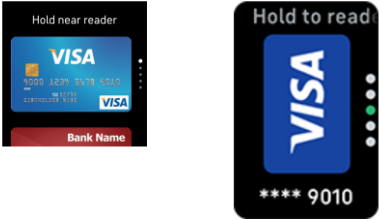
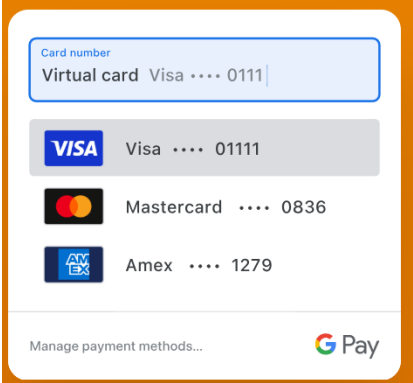
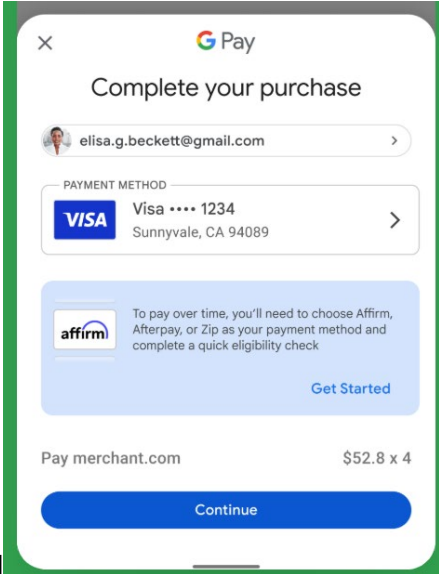
Claim No.	Accused Products
	<p>Connect to Wi-Fi networks on your Pixel Tablet</p> <p>To use Wi-Fi the way you want, you can change how and when your Pixel Tablet connects.</p> <p>When you have Wi-Fi turned on, your tablet automatically connects to nearby Wi-Fi networks you've connected to before. You can also set your tablet to automatically turn on Wi-Fi near saved networks.</p> <p>See, e.g., <i>Connect to Wi-Fi networks on your Pixel Tablet</i>, Google Pixel Tablet Help, https://support.google.com/googlepixelttablet/answer/13591526.</p> <p>Connect to Wi-Fi</p> <p>Your watch can automatically connect to saved Wi-Fi networks when it loses its connection with your phone.</p> <p>Turn on Wi-Fi</p> <ol style="list-style-type: none">1. If your screen is dim, tap it to wake up the watch.2. From the top of the screen, swipe down.3. Tap Settings .• If you don't see it right away, swipe left and tap Settings .4. Tap Connections > Wi-Fi. If Wi-Fi is set to off, tap the Wi-Fi switch to switch it on.• Wear 2: Scroll and tap Connectivity > Wi-Fi. If Wi-Fi is set to off, tap Wi-Fi to switch it to Automatic. <p>See, e.g., <i>Connect to Wi-Fi</i>, Wear OS by Google Help, https://support.google.com/wearos/answer/6207505.</p>

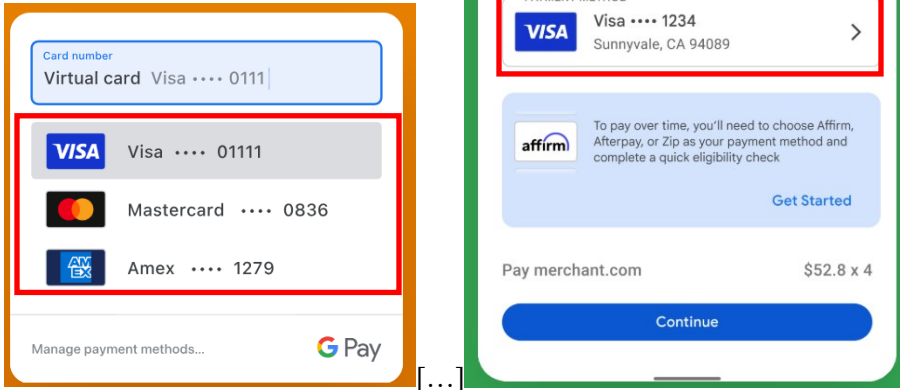
Claim No.	Accused Products
	<p data-bbox="510 237 1398 334">Set up and manage Google Pixel Watch with a cellular plan</p> <div data-bbox="510 386 1035 423" style="border: 2px solid red; padding: 2px;"> <p data-bbox="510 386 1035 423">Google Pixel Watch 4G LTE features</p> </div> <p data-bbox="510 440 787 464">Google Pixel Watch 4G LTE:</p> <ul data-bbox="510 488 1457 691" style="list-style-type: none"> • Has a direct connection to your cellular network/carrier plan. • Shares a number with your phone so notifications and messages are in sync. <ul style="list-style-type: none"> • Note: Google Pixel Watch LTE does not require you to have a new number but you will need to set up a separate line. Your watch will have the same number as your phone once you pair them and activate 4G LTE with a compatible carrier. • Lets you make calls and use apps from your watch without your phone. <p data-bbox="489 703 1627 764">See, e.g., <i>Set up and manage Google Pixel Watch with a cellular plan</i>, Google Pixel Watch Help, https://support.google.com/googlepixelwatch/answer/13541778.</p> <div data-bbox="510 821 1425 859" style="background-color: #e6f2ff; padding: 10px;"> <p data-bbox="510 821 1425 859">Which types of Wi-Fi networks can my Fitbit watch connect to?</p> </div> <p data-bbox="541 911 1860 1328">Your Fitbit watch can connect to open, WEP, WPA personal, and WPA2 personal Wi-Fi networks. Your watch won’t connect to 5GHz, 802.11ac, WPA enterprise, or public Wi-Fi networks that require logins, subscriptions, or profiles. If you see a captive portal when connecting to the Wi-Fi network on a computer, the network isn’t supported. A captive portal opens a web page in your browser and could ask for a username and password, payment, or acceptance of terms. This is commonly found when connecting to Wi-Fi networks in hotels, airports, coffee shops, and other public places. For best results, connect your watch to your home or work Wi-Fi network. Make sure you know the network password before connecting.</p> <p data-bbox="489 1344 1961 1375">See, e.g., <i>How do I connect my Fitbit watch to Wi-Fi?</i>, Fitbit Help Center, https://support.google.com/fitbit/answer/14236812.</p>

Claim No.	Accused Products
	<div data-bbox="489 224 1304 306" style="border: 2px solid red; padding: 5px;"> <p>Connect your Chromebook to Wi-Fi</p> </div> <p>To connect to the Internet, use a compatible Wi-Fi network.</p> <p>Step 1: Turn on Wi-Fi</p> <ol style="list-style-type: none"> 1. At the bottom right, select the time. 2. Select Not Connected . • If you find your Wi-Fi network name and a signal strength, your Chromebook is already connected to Wi-Fi. 3. Turn on Wi-Fi. 4. Your Chromebook will automatically look for available networks and show them to you in a list. <p>See, e.g., <i>Connect your Chromebook to Wi-Fi</i>, Chromebook Help, https://support.google.com/chromebook/answer/1047420.</p>
<p>19[b] a displaying of the payment request notification at a touch-screen display user-interface of the electronic device; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone, laptop, tablet, or smartwatch, displays the payment request notification at a touch-screen display user-interface (e.g., touchscreen) of the electronic device.</p> <p>1. You can pay faster from more browsers and devices</p> <p>We’re starting to roll out Google Pay on the web from desktop and iOS—which means you’ll start seeing it when you’re shopping on browsers like Chrome, Safari, and Firefox, no matter your device. Plus, if you save a card to Google Pay on your Pixelbook, you’ll be able to use it on the web with another device, like an iPhone.</p> <p>See, e.g., <i>5 ways Google Pay can save you time and money at checkout</i>, Google The Keyword, https://blog.google/products/google-pay/5-ways-google-pay-can-save-you-time-and-money/.</p>

Claim No.	Accused Products
	<div data-bbox="940 224 1701 365" data-label="Text"> <p>Just look for Google Pay at checkout in your favorite apps and sites.</p> <p>Finally, confirm your purchase.</p> </div> <div data-bbox="489 365 1675 933" data-label="Image"> </div> <p>See, e.g., <i>Seamless online checkout</i>, Google, https://pay.google.com/about/pay-online/; <i>How do you pay online with Google Pay?</i>, Google Help, https://www.youtube.com/watch?v=y15SGXiPnDY.</p>
<p>19[c]: upon an authorizing of a valid device user, displaying at least one user-selectable payment account option, and requesting a user approval of payment, via the touch-screen display user-interface;</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone, laptop, tablet, or smartwatch, upon an authorizing of a valid device user, displays at least one user-selectable payment account option (e.g., Visa, Mastercard, Amex, etc.), and requesting a user approval of payment, via the touch-screen display user-interface (e.g., touchscreen display).</p> <div data-bbox="506 1169 1215 1247" data-label="Section-Header"> <h3>Unlock your screen faster with a PIN</h3> </div> <p>Before you lock your screen, you can create a PIN to unlock your screen. If you use an account for work or school, your admin might require you to enter your password occasionally. On some Chromebooks, you can also use your PIN instead of your Google Account password to sign in.</p> <p>See, e.g., <i>Lock or unlock your screen</i>, Chromebook Help, https://support.google.com/chromebook/answer/2587994.</p>

Claim No.	Accused Products
	<p>Verify it’s you to make a purchase</p> <p>To make payments with Google Wallet, you must have a screen lock set up on your device and verify it’s you for your security.</p> <p>You can verify it's you in Google Wallet with several methods:</p> <ul style="list-style-type: none">• PIN• Pattern• Password• Class 3 biometric unlock <p>Tip: Google Wallet doesn't work with Class 1 or Class 2 biometric unlocks or screen locks like Smart Unlock or Knock to Unlock.</p> <p>See, e.g., <i>Verify it’s you to make a purchase</i>, Google Wallet Help, https://support.google.com/wallet/answer/12059519; <i>Set up screen lock for tap to pay transactions</i>, Google Wallet Help Center (captured Dec. 15, 2023), https://web.archive.org/web/20231215153739/https://support.google.com/wallet/answer/12059519#zippy=%2Cpayment-limits-on-a-locked-device (noting for the United States that “Unlock is required for all transactions except for transit”); <i>Set screen lock on your Pixel phone</i>, Pixel Phone Help, https://support.google.com/pixelphone/answer/2819522.</p> <p>How to use Google Wallet on Pixel Watch</p> <p>With Screen Lock and Google Wallet set up on Pixel Watch, now it's just a matter of putting the tap-to-pay functionality to use.</p> <ol style="list-style-type: none">1. Double-press the crown.2. Your default card will appear on the screen.3. If you want to pay with a different card, swipe until you find the card you want to use.4. Hold your Pixel Watch near the payment terminal.5. Once the payment has been completed successfully, you will hear a chime and a checkmark appears on your watch. <p>See, e.g., <i>How to use Google Wallet on the Pixel Watch</i>, AndroidCentral (Oct. 19, 2022), https://www.androidcentral.com/wearables/how-to-use-google-wallet-pixel-watch.</p>

Claim No.	Accused Products
	<p>1. If prompted, enter your 4-digit device PIN code Your default card appears on the screen.</p> <div></div> <p>See, e.g., <i>What should I know about using my Fitbit device to make contactless payments?</i> Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</p> <div><div></div><div></div></div> <p>See, e.g., <i>Seamless online checkout</i>, Google, https://pay.google.com/about/pay-online/.</p>

Claim No.	Accused Products
<p>19[d] receiving, from a valid device user, a payment selection and authorization approval input on the electronic device;</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone, laptop, tablet, or smartwatch, receives, from a valid device user, a payment selection and authorization approval input (e.g., selecting one of the plurality of payment methods) on the electronic device.</p> <div data-bbox="489 545 1383 932">  </div> <p>See, e.g., <i>Seamless online checkout</i>, Google, https://pay.google.com/about/pay-online/.</p>
<p>19[e] generating at least one limited-use numbers at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information; and</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (see 1[pre]), such as a smartphone, laptop, tablet, or smartwatch, generates at least one limited-use numbers (e.g., dynamic cryptogram or a combination of one or more of these with a DPAN) at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information (e.g., card number/ personal account number (“PAN”) and associated expiration date and security code/ card verification code “CVV”).</p>

Claim No.	Accused Products
	<p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant’s acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay’s security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token’s DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder’s mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p>See, e.g., <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Google Pay – Device Tokenization – TSP Integration</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</p> <p>Tokens and cards-on-file</p> <p>When a user adds their card to Google Pay, they get one or more of the following:</p> <ul style="list-style-type: none"> • Device token (DPANs) • Card-on-file (PAN/FPAN, expiry, and cardholder name) • Cloud token (tokenized version of a card-on-file) <p>Device tokens, cards on file, and cloud tokens are used in different scenarios. Device tokens are device bound and can be used for in-store NFC transactions and online transactions. Cards on file and cloud tokens are stored at the account level, rather than on the device, and can be used for peer-to-peer and online transactions. When tokenizing a card, the user’s card information may be stored as a card on file and can potentially incur a small, temporary charge. This charge is refunded once the account has been verified. More information can be found on the Google charge support page ↗</p> <p>See, e.g., <i>Device Tokenization</i>, Google Pay, https://developers.google.com/pay/issuers.</p>

Claim No.	Accused Products
	<p>Device tokenization</p> <p>When a user successfully adds their card to Google Pay, Google Pay stores a uniquely generated token on the device that has its own value. This new number, called a dynamic primary account number (DPAN) or device token, is similar to a credit card number.</p> <p>A DPAN improves account security because Google Pay passes it to a terminal during payment instead of the actual card number. In Google Pay, DPAN is referred as a 'virtual account number'. Users can only see the last four digits of this number, which are visible on the card details view in the Google Wallet app.</p> <p>See, e.g., Enabling Google Pay device tokenization, Google Pay, https://developers.google.com/pay/issuers/tsp-integration/overview.</p>  <p>See, e.g., How device tokens keep your payment cards safe in Google Wallet, https://blog.google/products/google-pay/device-tokens-google-wallet.</p>

Claim No.	Accused Products
	<div data-bbox="514 261 882 345" data-label="Image"> </div> <div data-bbox="907 261 1486 344" data-label="Section-Header"> <h2>EMVCo Security Evaluation Certificate Mobile Application</h2> </div> <div data-bbox="531 376 1451 425" data-label="Text"> <p>Please accept this document as confirmation of the EMVCo Software-Based Mobile Payments Security Evaluation Process.</p> </div> <div data-bbox="501 470 995 498" data-label="Text"> <p>Evaluation Certificate Number: SECN0069.03</p> </div> <div data-bbox="501 511 819 539" data-label="Text"> <p>Date SECN Issued: 22 Apr 2021</p> </div> <div data-bbox="1071 511 1457 539" data-label="Text"> <p>Next security review due: 22 Apr 2025</p> </div> <div data-bbox="501 555 812 583" data-label="Text"> <p>Company Name: Google, LLC</p> </div> <div data-bbox="501 584 1224 641" data-label="Text"> <p>Address: 1600 Amphitheatre Pkwy Mountain View, CA 94043 United States of America</p> </div> <div data-bbox="501 652 812 682" data-label="Text"> <p>Product Name: Google Wallet</p> </div> <div data-bbox="478 682 1659 750" data-label="Text"> <p>See, e.g., <i>EMVCo Security Evaluation Certificate Mobile Application</i>, https://www.emvco.com/wp-content/uploads/loa/EMVCo_SECN0069.03_N_08_2024-15.pdf (Last visited December 4, 2024).</p> </div> <div data-bbox="501 794 1098 829" data-label="Text"> <p>An HCE transaction takes place as follows:</p> </div> <div data-bbox="560 852 1957 1130" data-label="List-Group"> <ol style="list-style-type: none"> 1. To initiate an HCE mobile payment, a customer taps the mobile phone at the POS contactless reader. 2. HCE enables the NFC controller in the mobile phone to route communications from the POS reader to the mobile wallet app to request access to the payment token. 3. The payment token and accompanying dynamic cryptogram are passed to the POS to complete the transaction. </div> <div data-bbox="478 1153 1999 1219" data-label="Text"> <p>See, e.g., <i>Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions</i>, https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf, pp. 14.</p> </div>

Claim No.	Accused Products
	<p>5. End-to-End EMV Payment Tokenization Flows</p> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> <ul style="list-style-type: none"> In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>^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.</p> <p>Figure 7. Processing an In-App Transaction Using a Merchant Mobile App with Tokens Provisioned in a Device-Centric Wallet</p> <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 12, 23-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <p>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:</p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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.

[...]

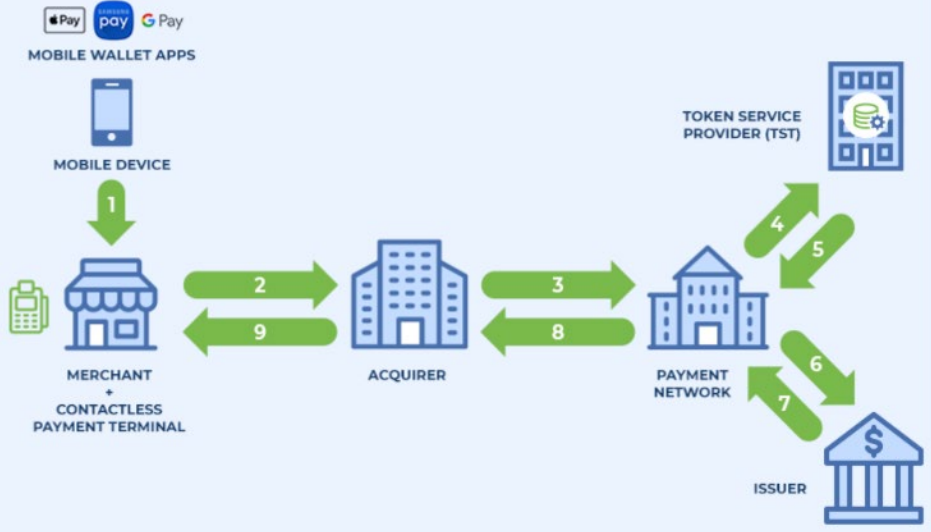
Claim No.	Accused Products
	<div data-bbox="499 240 1455 272" style="border: 2px solid red; padding: 2px;"> <p>2. The merchant sends the token and dynamic cryptogram data to the acquirer.</p> </div> <div data-bbox="499 280 1444 812"> <p>The diagram illustrates the tokenization process for mobile payments. It shows a Mobile Device (with Apple Pay, Samsung Pay, and Google Pay logos) interacting with a Merchant's Contactless Payment Terminal. Step 1 shows the device sending data to the terminal. Step 2 shows the terminal sending token and dynamic cryptogram data to the Acquirer. Step 3 shows the Acquirer sending data to the Payment Network. Step 4 shows the Payment Network sending data to the Token Service Provider (TST). Step 5 shows the TST sending data to the Issuer. Step 6 shows the Issuer sending data to the Payment Network. Step 7 shows the Payment Network sending data to the Acquirer. Step 8 shows the Acquirer sending data to the Merchant's terminal. Step 9 shows the Merchant's terminal sending data to the Mobile Device.</p> </div> <p>See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details (captured May 9, 2024).</p>
<p>19[f] combining said at least one limited-use numbers, with said selected account information, to form a complete payment information; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, combines said at least one limited-use numbers (e.g., dynamic cryptogram), with said selected account information (e.g., DPAN), to form a complete payment information.</p> <p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant’s acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay’s security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token’s DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder’s mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device.

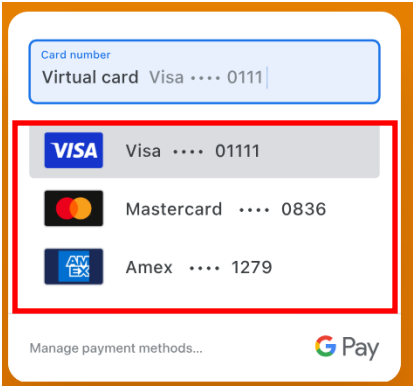
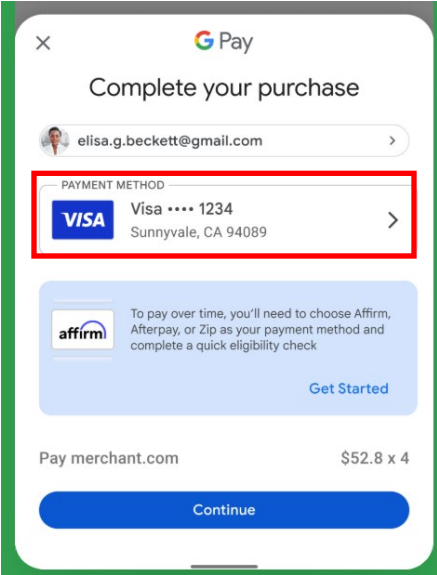
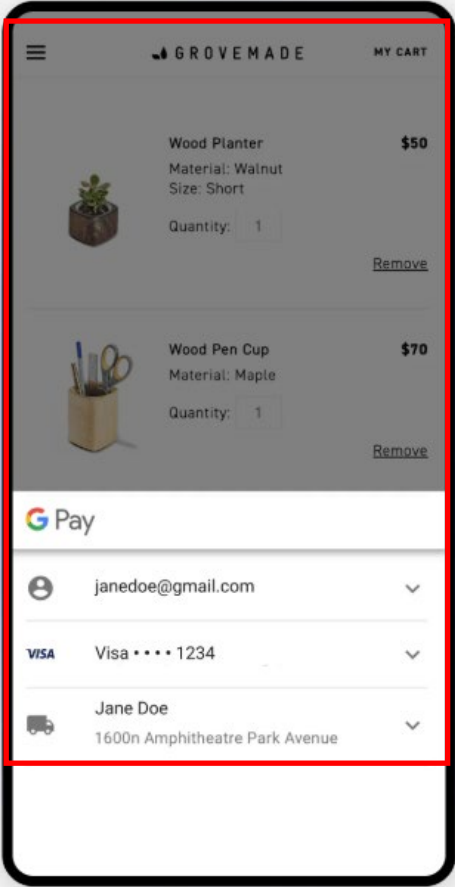
Claim No.	Accused Products		
	<p>See, e.g., <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Google Pay – Device Tokenization – TSP Integration</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</p> <p>The following JSON snippet is an example of the full <code>encryptedMessage</code> for a <code>CARD</code> <code>paymentMethod</code> with a <code>CRYPTOGRAM_3DS</code> <code>authMethod</code>:</p> <pre>{ "paymentMethod": "CARD", "paymentMethodDetails": { "authMethod": "CRYPTOGRAM_3DS", "pan": "1111222233334444", "expirationMonth": 10, "expirationYear": 2025, "cryptogram": "AAAAAA...", "eciIndicator": "eci indicator" }, }</pre> <p>See, e.g., <i>Payment data cryptography for merchants</i>, Google Pay, https://developers.google.com/pay/api/android/guides/resources/payment-data-cryptography.</p> <h3>3. Tokenization Use Case Scenarios</h3> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p>	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.
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.		

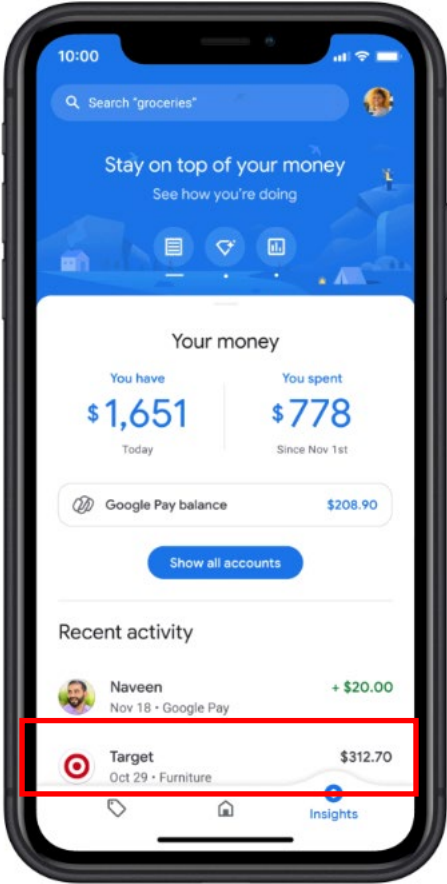
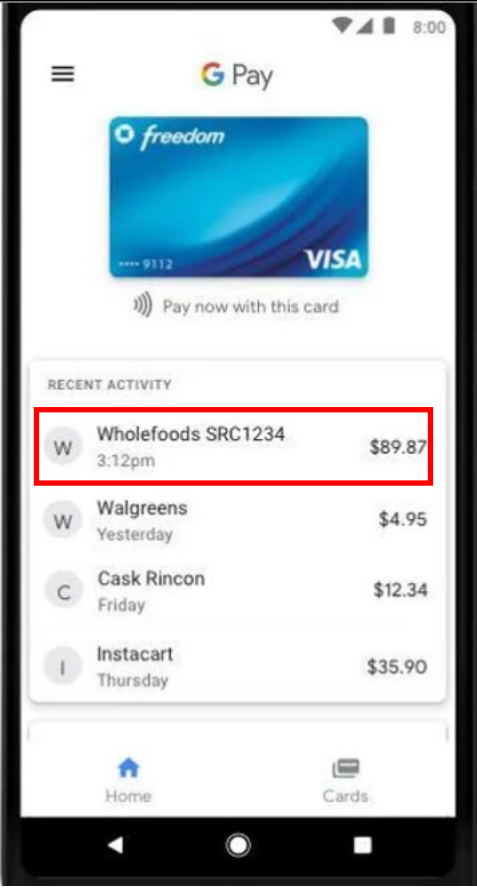
Claim No.	Accused Products
	<div data-bbox="520 261 882 345">  </div> <div data-bbox="919 261 1484 345"> <p>EMVCo Security Evaluation Certificate Mobile Application</p> </div> <div data-bbox="541 378 1451 427"> <p>Please accept this document as confirmation of the EMVCo Software-Based Mobile Payments Security Evaluation Process.</p> </div> <div data-bbox="512 472 995 500"> <p>Evaluation Certificate Number: SECN0069.03</p> </div> <div data-bbox="512 513 819 540"> <p>Date SECN Issued: 22 Apr 2021</p> </div> <div data-bbox="1083 513 1457 540"> <p>Next security review due: 22 Apr 2025</p> </div> <div data-bbox="512 557 814 584"> <p>Company Name: Google, LLC</p> </div> <div data-bbox="512 586 1224 643"> <p>Address: 1600 Amphitheatre Pkwy Mountain View, CA 94043 United States of America</p> </div> <div data-bbox="512 654 812 682"> <p>Product Name: Google Wallet</p> </div> <div data-bbox="491 683 1656 751"> <p>See, e.g., <i>EMVCo Security Evaluation Certificate Mobile Application</i>, https://www.emvco.com/wp-content/uploads/loa/EMVCo_SECN0069.03_N_08_2024-15.pdf (Last visited December 4, 2024).</p> </div> <div data-bbox="512 797 1098 831"> <p>An HCE transaction takes place as follows:</p> </div> <div data-bbox="573 855 1938 1133"> <ol style="list-style-type: none"> 1. To initiate an HCE mobile payment, a customer taps the mobile phone at the POS contactless reader. 2. HCE enables the NFC controller in the mobile phone to route communications from the POS reader to the mobile wallet app to request access to the payment token. 3. The payment token and accompanying dynamic cryptogram are passed to the POS to complete the transaction. </div> <div data-bbox="491 1154 1980 1222"> <p>See, e.g., <i>Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions</i>, https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf, pp. 14.</p> </div>

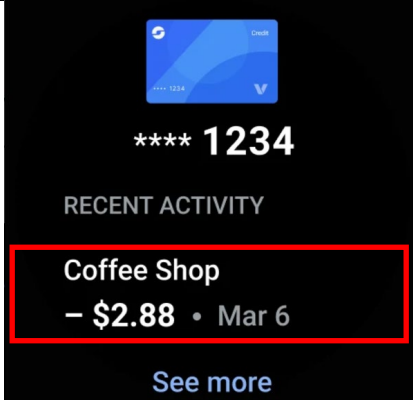
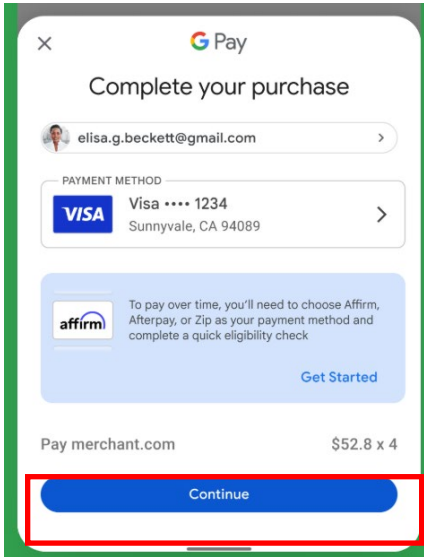
Claim No.	Accused Products
	<div><div><div><h3>5. End-to-End EMV Payment Tokenization Flows</h3><p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p><ul style="list-style-type: none">In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)</div><div><p>The diagram illustrates the flow of an in-app transaction using a merchant mobile app. It involves several entities: Merchant Mobile App, Merchant Acquirer/Processor, Payment Network, Token Service Provider, Issuer Processor, and Issuer. The process is numbered 1 through 10. Step 1 shows the Merchant Mobile App sending a 'Payment Token + Cryptogram' to the Merchant Acquirer/Processor. Step 2 shows the Merchant Acquirer/Processor sending a 'Payment Token + Cryptogram' to the Payment Network. Step 3 shows the Payment Network sending a 'Payment Token + Cryptogram' to the Token Service Provider. Step 4 shows the Token Service Provider sending a 'Payment Token + Cryptogram' to the Payment Network. Step 5 shows the Payment Network sending a 'PAN' to the Issuer Processor. Step 6 shows the Issuer Processor sending a 'PAN' to the Issuer. Step 7 shows the Issuer sending a 'PAN' to the Issuer Processor. Step 8 shows the Issuer Processor sending a 'PAN' to the Payment Network. Step 9 shows the Payment Network sending a 'Payment Token + Last 4' to the Merchant Acquirer/Processor. Step 10 shows the Merchant Acquirer/Processor sending a 'Confirmation Message' to the Merchant Mobile App. A red box highlights step 1.</p></div><div><p>^a Other TSP providers are also possible.</p><p>^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.</p><p>^c The payment network to which the transaction is routed may need to be the payment network that provided the token.</p></div><div><p>Figure 7. Processing an In-App Transaction Using a Merchant Mobile App with Tokens Provisioned in a Device-Centric Wallet</p><p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 12, 23-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p><p>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:</p><ol style="list-style-type: none">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:<ul style="list-style-type: none">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.</div></div></div>

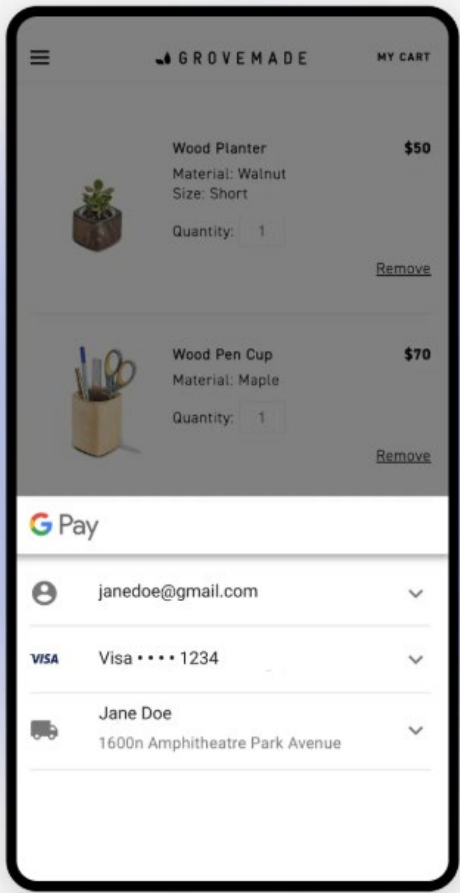
[...]

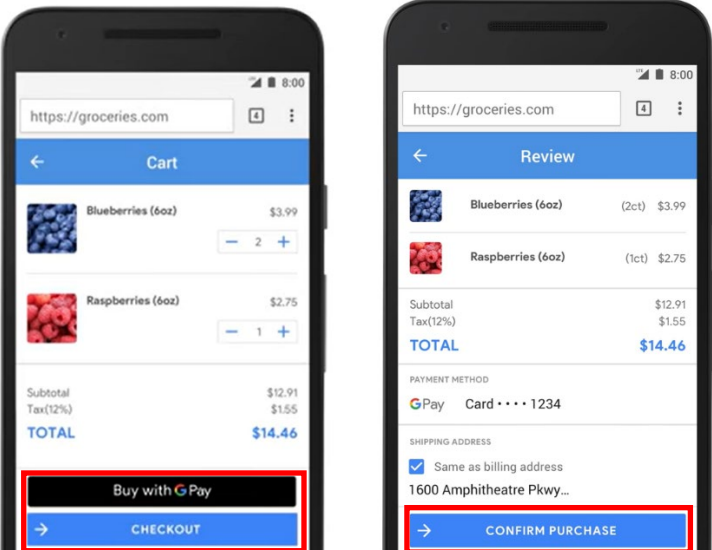
Claim No.	Accused Products
	<div data-bbox="499 240 1455 272" style="border: 2px solid red; padding: 2px;"> <p>2. The merchant sends the token and dynamic cryptogram data to the acquirer.</p> </div>  <p>The diagram illustrates a mobile payment transaction flow involving several entities: MOBILE WALLET APPS (Apple Pay, Samsung Pay, Google Pay), MOBILE DEVICE, MERCHANT + CONTACTLESS PAYMENT TERMINAL, ACQUIRER, PAYMENT NETWORK, TOKEN SERVICE PROVIDER (TST), and ISSUER. The flow is numbered 1 through 9. Step 1 shows the mobile device interacting with the merchant terminal. Step 2 shows the merchant terminal sending data to the acquirer. Step 3 shows the acquirer sending data to the payment network. Step 4 shows the payment network sending data to the token service provider. Step 5 shows the token service provider sending data to the issuer. Step 6 shows the issuer sending data to the payment network. Step 7 shows the payment network sending data to the acquirer. Step 8 shows the acquirer sending data to the merchant terminal. Step 9 shows the merchant terminal sending data to the mobile device.</p> <p>See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details (captured May 9, 2024).</p>
<p>19[g] wherein the receiving of a user payment approval authorization through the user-interface of the electronic device, is comprising a displaying on said display at least a portion of information comprising: the payment request, the merchant, the amount, and the transaction information; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, when receiving a user payment approval authorization through the user-interface, displays on said display at least a portion of information comprising: the payment request, the merchant (e.g., merchant name), the amount (e.g., the payment amount), and the transaction information (e.g., product(s) being bought).</p>

Claim No.	Accused Products
	<div></div> <p>[...]</p> <p>See, e.g., <i>Seamless online checkout</i>, Google, https://pay.google.com/about/pay-online/; <i>Accept Google Pay in your online store, across browsers, and on Android devices</i>, https://www.shopify.com/google-pay.</p>

Claim No.	Accused Products
	<div></div> <div></div> <p><i>See, e.g., Google Pay reimaged: pay, save, manage expenses and more, Google Pay, https://blog.google/products/google-pay/reimaged-pay-save-manage-expenses-and-more/; 6 things you should know about the new Google Pay app, CNET, https://www.cnet.com/tech/services-and-software/things-you-should-know-about-the-new-google-pay-app/.</i></p>

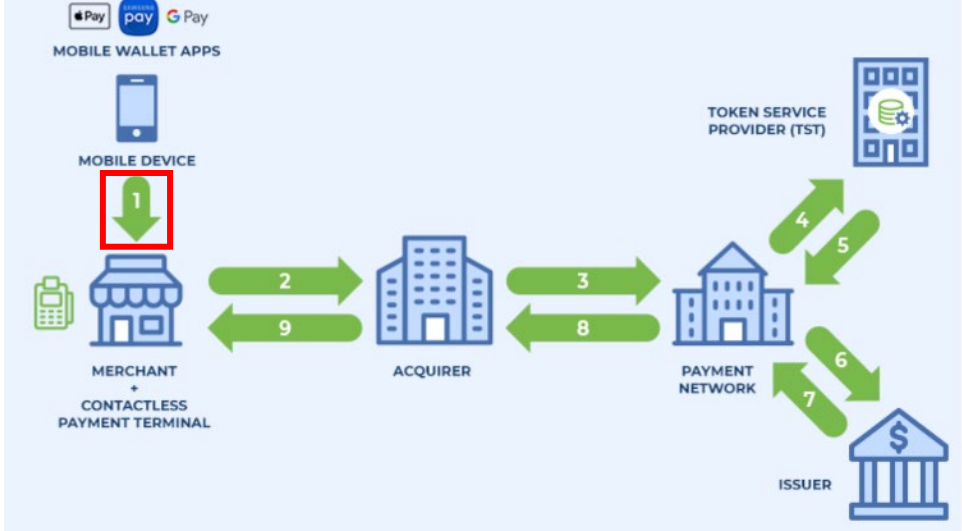
Claim No.	Accused Products
	 <p>See, e.g., Google Play, Google Wallet, https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfc&hl=en_US.</p>
<p>19[h] receiving a user input providing for at least one transaction authorization actions, from a set of actions including: approving a transaction, denying a transaction, selecting a user information, a payment amount adjustment, and selecting a transaction payment method; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, when receiving a user payment approval authorization through the user-interface, receives a user input providing for at least one transaction authorization actions, from a set of actions including: approving a transaction, denying a transaction, selecting a user information, a payment amount adjustment, and selecting a transaction payment method (e.g., selecting one from Visa, Mastercard, and Amex).</p>  <p>See, e.g., Seamless online checkout, Google, https://pay.google.com/about/pay-online/.</p>

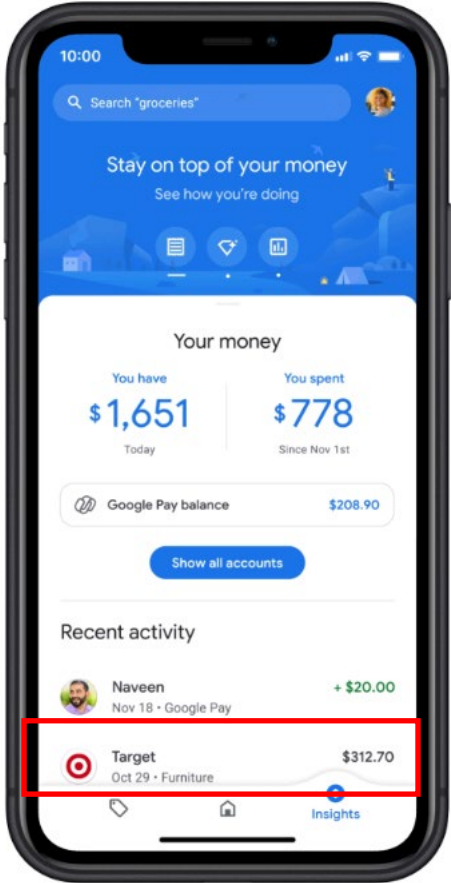
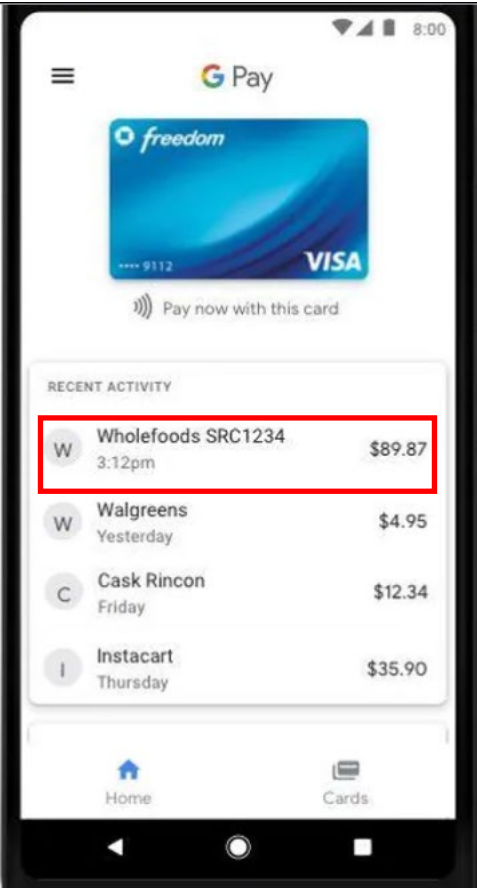
Claim No.	Accused Products
	<div></div> <p>See, e.g., Accept Google Pay in your online store, across browsers, and on Android devices, https://www.shopify.com/google-pay.</p>

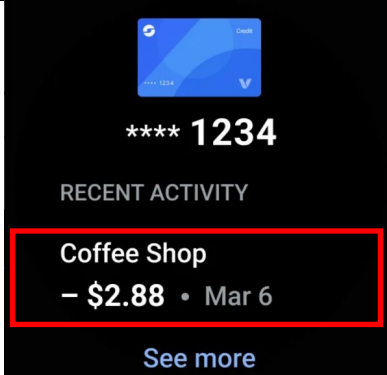
Claim No.	Accused Products
	<div>Just look for Google Pay at checkout in your favorite apps and sites.</div> <div>Finally, confirm your purchase.</div> <div></div> <div>See, e.g., <i>How do you pay online with Google Pay?</i>, Google Help, https://www.youtube.com/watch?v=yl5SGXiPnDY.</div>
19[i] on receiving said user payment approval authorization input, a transmitting by the wireless interface of the approved complete payment information for the online transaction.	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, on receiving said user payment approval authorization input, transmits by the wireless interface (e.g., through a Wi-Fi, LTE, or 5G chipset) of the approved complete payment information for the online transaction.

Claim No.	Accused Products
	<div><div><div><div><div>12:00</div><div>← sportstore.com</div><div></div></div><div>Shopping Cart</div><div><div><div><div>Skateboard</div><div>x1</div></div><div>\$80.00</div></div></div><div><div>Subtotal:</div><div>\$80.00</div></div><div><div>Shipping:</div><div>\$0.00</div></div><div><div>Total:</div><div>\$80.00</div></div><div>Buy with </div></div></div><div>[...]</div><div><div><div><div>12:00</div><div>← sportstore.com</div><div></div></div><div><div>Card number</div><div>..... 0836</div></div><div><div><div>VISA</div><div>Visa 4545</div></div><div><div><div>Mastercard</div><div>.... 0836</div></div></div><div><div><div>Amex</div><div>Amex 1279</div></div></div><div>Manage payment methods...</div><div></div></div></div><div><div><div>12:00</div><div>← sportstore.com</div><div></div></div><div><div><div>Skateboard</div><div></div></div></div><div>Your order has been placed successfully</div><div>Continue shopping</div></div></div><p>See, e.g., <i>Seamless online checkout</i>, Google, https://pay.google.com/about/pay-online/.</p><h3>5. End-to-End EMV Payment Tokenization Flows</h3><p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p><ul style="list-style-type: none">In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)</div>

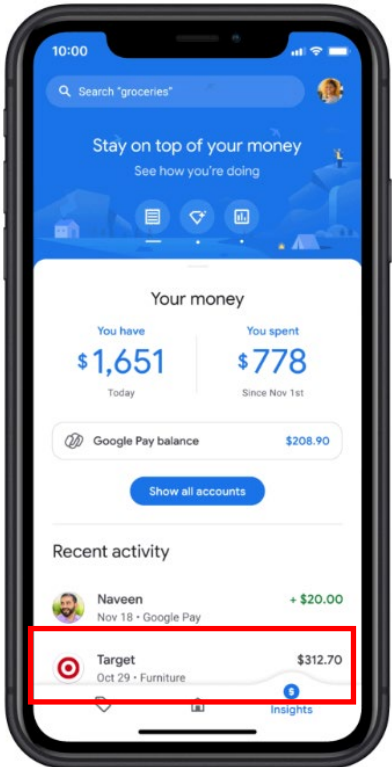
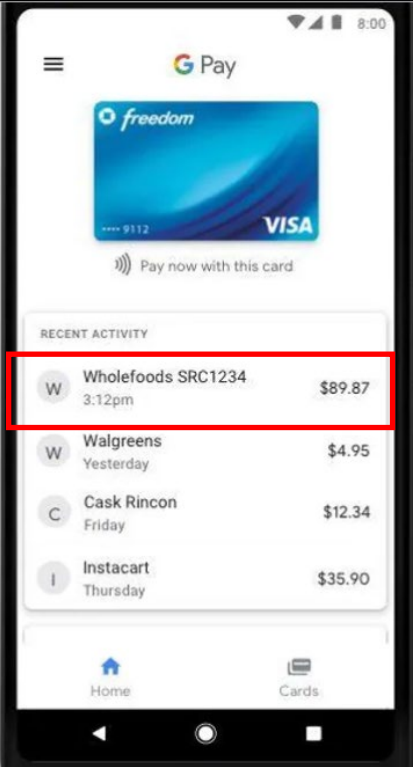
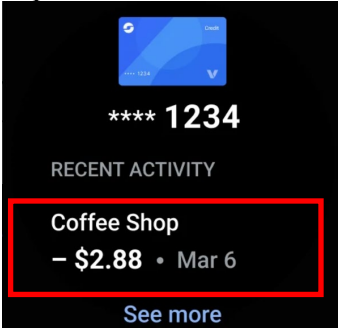
Claim No.	Accused Products
	<div><p>^a Other TSP providers are also possible.</p><p>^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.</p><p>^c The payment network to which the transaction is routed may need to be the payment network that provided the token.</p><p>Figure 7. Processing an In-App Transaction Using a Merchant Mobile App with Tokens Provisioned in a Device-Centric Wallet</p><p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 12, 23-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p><p>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:</p><ol style="list-style-type: none">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:<ul style="list-style-type: none">• 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.</div>

Claim No.	Accused Products
	 <p><i>See, e.g., Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), 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).</p>
<p>20[a] The method of claim 19, further comprising: dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the payment issuing authority, and wherein dynamically generating the cryptogram number comprises cryptographically combining a device transaction sequence counter count, a user information, a payment account number, information and secrets known to a</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, dynamically generates a cryptogram number (e.g., dynamic cryptogram) for use by the electronic device in place of a card validation value originated from the payment issuing authority (e.g., CVV), and wherein dynamically generating the cryptogram number comprises cryptographically combining a device transaction sequence counter count (e.g., transaction-unique value), a user information, a payment account number (e.g., DPAN), information and secrets known to a payment processing authority (e.g., secret keys).</p> <p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant’s acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay’s security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token’s DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder’s mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device.

Claim No.	Accused Products
payment processing authority; and	<p>See, e.g., <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Google Pay – Device Tokenization – TSP Integration</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</p> <div></div> <p>See, e.g., <i>Google Pay reimaged: pay, save, manage expenses and more</i>, Google Pay, https://blog.google/products/google-pay/reimagined-pay-save-manage-expenses-and-more/; 6 things you should know about the new Google Pay app, CNET, https://www.cnet.com/tech/services-and-software/things-you-should-know-about-the-new-google-pay-app/.</p>

Claim No.	Accused Products
	 <p>See, e.g., Google Play, Google Wallet, https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfcrel&hl=en_US.</p> <p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant’s acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay’s security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token’s DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder’s mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p>See, e.g., Google Pay – Device Tokenization – Security, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; Google Pay – Device Tokenization – TSP Integration, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</p> <h3>3. Tokenization Use Case Scenarios</h3> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> • In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>

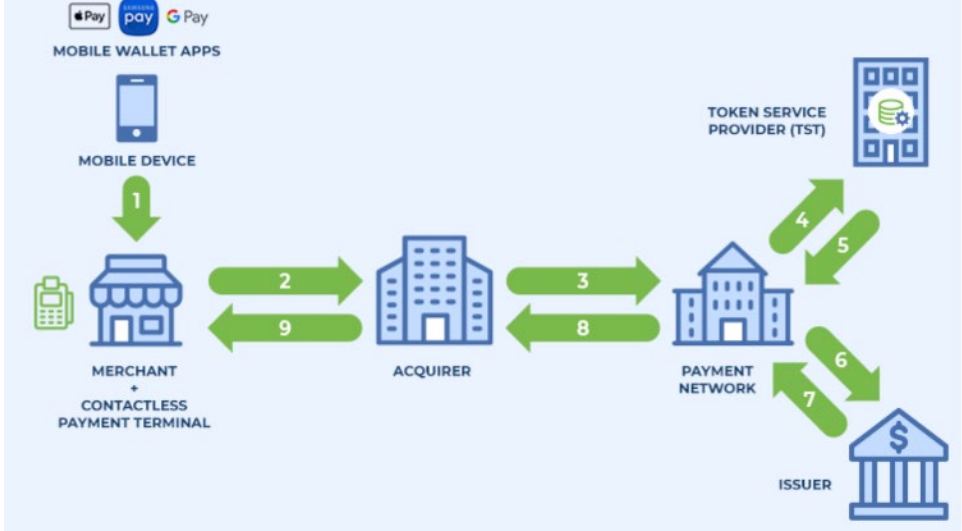
Claim No.	Accused Products		
	<table border="1" data-bbox="499 232 1554 397"> <tr> <td data-bbox="499 232 730 397">Token Cryptogram</td><td data-bbox="730 232 1554 397">A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p data-bbox="489 406 1806 435"><i>See, e.g., EMVCo, EMV Payment Tokenisation Specification – Technical Framework at 10 (June 2019 ver. 2.1).</i></p> <p data-bbox="489 446 1921 641">How is this an issue specific to EMV? When a merchant stores and forwards EMV chip or tokenized mobile wallet transactions, the Application Transaction Counter (ATC) that provides a sequential reference to each transaction becomes out of sync and Issuers decline the transaction. An ATC does not come into play with magnetic strip transactions. The ATC is a sequence number that is tracked like a counter on each EMV chip card/mobile wallet transaction. Issuers use the ATC number as a fraud detection tool and an out of sequence can indicate a potentially fraudulent transaction. For example, in a SAF scenario the issuer sees transactions 1, 2, 4, 5 followed by a 3. The transaction with the 3 (which was stored and forwarded once available) is declined by the issuer since it is expecting a 6.</p> <p data-bbox="489 662 1974 760"><i>See, e.g., Evolution in Payments: EMV is Not the Only Three Letter Word in This Story (MAG Quarterly- Volume Five, Issue Three), https://www.merchantadvisorygroup.org/news/mag-insights/article/2020/11/10/evolution-in-payments-emv-is-not-the-only-three-letter-word-in-this-story-(mag-quarterly--volume-five-issue-three).</i></p>	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.
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.		
<p>20[b] wherein further, said dynamically generating said card validation value number results in a one-time limited-use payment information, on incrementing the device transaction sequence counter count on each transaction payment, and said device combining said current transaction sequence count at the instant of generating said cryptogram number.</p>	<p data-bbox="489 768 1974 930">A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs a method wherein dynamically generating said card validation value number (e.g., dynamic cryptogram) results in a one-time limited-use payment information, on incrementing the device transaction sequence counter (e.g., transaction-unique value) count on each transaction payment, and said device combining said current transaction sequence count at the instant of generating said cryptogram number.</p> <p data-bbox="489 971 1663 1032">Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant’s acquiring bank, and the card issuing bank.</p> <p data-bbox="489 1065 1041 1094">Highlights of Google Pay’s security features include:</p> <ul data-bbox="531 1127 1726 1347" style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token’s DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder’s mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p data-bbox="489 1356 1988 1448"><i>See, e.g., Google Pay – Device Tokenization – Security, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; Google Pay – Device Tokenization – TSP Integration, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</i></p>		

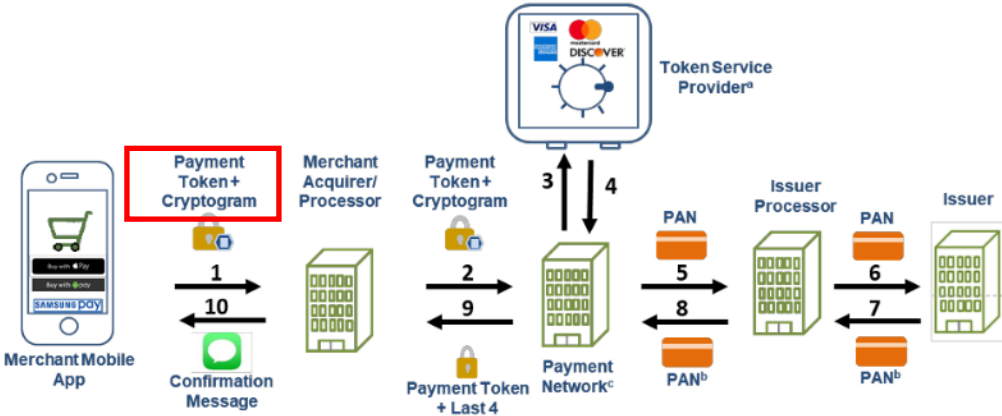
Claim No.	Accused Products
	<div><p>See, e.g., <i>Google Pay reimaged: pay, save, manage expenses and more</i>, Google Pay, https://blog.google/products/google-pay/reimagined-pay-save-manage-expenses-and-more/; 6 things you should know about the new Google Pay app, CNET, https://www.cnet.com/tech/services-and-software/things-you-should-know-about-the-new-google-pay-app/.</p><p>See, e.g., <i>Google Play, Google Wallet</i>, https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfcrel&hl=en_US.</p></div>

Claim No.	Accused Products		
	<p>3. Tokenization Use Case Scenarios</p> <p>Payment tokenization can be implemented in a variety of environments and use cases:</p> <ul style="list-style-type: none"> In-store EMV contactless payments with device-centric³ digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p> <p>How is this an issue specific to EMV? When a merchant stores and forwards EMV chip or tokenized mobile wallet transactions, the Application Transaction Counter (ATC) that provides a sequential reference to each transaction becomes out of sync and Issuers decline the transaction. An ATC does not come into play with magnetic strip transactions. The ATC is a sequence number that is tracked like a counter on each EMV chip card/mobile wallet transaction. Issuers use the ATC number as a fraud detection tool and an out of sequence can indicate a potentially fraudulent transaction. For example, in a SAF scenario the issuer sees transactions 1, 2, 4, 5 followed by a 3. The transaction with the 3 (which was stored and forwarded once available) is declined by the issuer since it is expecting a 6.</p> <p>See, e.g., Evolution in Payments: EMV is Not the Only Three Letter Word in This Story (MAG Quarterly- Volume Five, Issue Three), https://www.merchantadvisorygroup.org/news/mag-insights/article/2020/11/10/evolution-in-payments-emv-is-not-the-only-three-letter-word-in-this-story-(mag-quarterly--volume-five-issue-three).</p>	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.
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.		
21[a] The method of claim 19, wherein at least a portion of said limited-use number comprises a static device account number, and wherein the static device account number is of a limited scope of valid use to a specific device,	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs a method wherein at least a portion of said limited-use number comprises a static device account number (e.g., DPAN), and wherein the static device account number is of a limited scope of valid use to a specific device (e.g., device to which DPAN is assigned).		

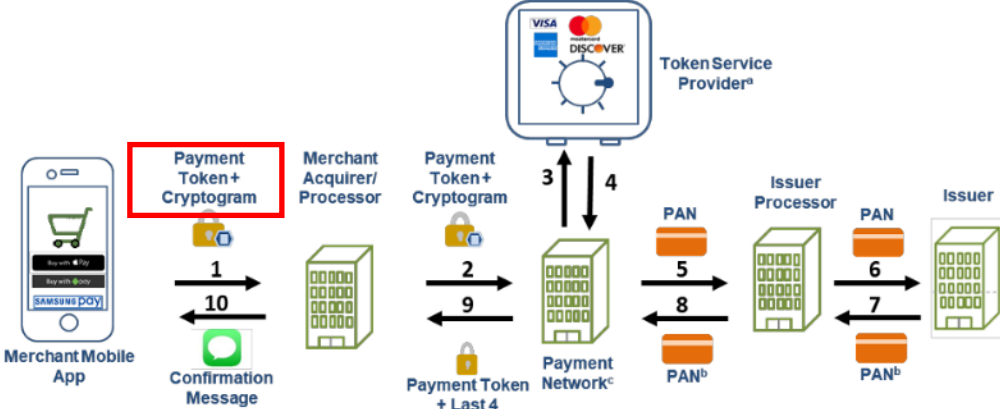
Claim No.	Accused Products
	<p data-bbox="531 237 1062 285">What device tokens are</p> <p data-bbox="531 334 1566 545">When you pay for something with a physical card — credit, debit or prepaid — the merchant usually charges you through the printed number on the front of your card, known as the Funding Primary Account Number (FPAN). Every time this happens, you provide that number to the merchant, and that number is then sent along to a handful of other parties like the merchant’s bank, the card network (an organization that facilitates transactions between banks and merchants), the payment service provider and more.</p> <div data-bbox="489 573 1581 732" style="border: 2px solid red; padding: 5px;"> <p data-bbox="531 581 1566 716">In contrast, Google Wallet creates a device-specific virtual account number, or device token, for each payment method you add, so your real card number isn’t stored on your device or shared with merchants. Thanks to this tokenization, the only parties who have your actual FPAN when you make a purchase are the bank that issued the card and the card network.</p> </div> <p data-bbox="489 737 1566 797"><i>See, e.g., How device tokens keep your payment cards safe in Google Wallet</i>, The Keyword, https://blog.google/products/google-pay/device-tokens-google-wallet.</p>
<p data-bbox="107 808 457 1138">21[b] and wherein further a payment processing authority provides said device account number unique for the specific electronic device, in place of payment issuer information, in performing payment transactions by the electronic device, and further comprising:</p>	<p data-bbox="489 808 1986 935">A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs a method wherein a payment processing authority (e.g., TSP) provides said device account number (e.g., DPAN) unique for the specific electronic device, in place of payment issuer information (e.g., PAN), in performing payment transactions by the electronic device.</p> <p data-bbox="489 979 1314 1019">5. End-to-End EMV Payment Tokenization Flows</p> <p data-bbox="489 1040 1503 1097">This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> <ul data-bbox="531 1117 1524 1170" style="list-style-type: none"> <li data-bbox="531 1117 1524 1170">• In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)

Claim No.	Accused Products
	<div><p>^a Other TSP providers are also possible.</p><p>^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.</p><p>^c The payment network to which the transaction is routed may need to be the payment network that provided the token.</p><p>Figure 7. Processing an In-App Transaction Using a Merchant Mobile App with Tokens Provisioned in a Device-Centric Wallet</p><p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 12, 23-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p><p>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:</p><ol style="list-style-type: none">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:<ul style="list-style-type: none">• EMV Contactless: If the Point of Sale (POS) terminal supports contactless payments via NFC (Near Field Communication), the EMV contactless specification is used to perform the data transfer.The merchant sends the token and dynamic cryptogram data to the acquirer.<p>[...]</p></div>

Claim No.	Accused Products
	 <p><i>See, e.g., Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), 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).</p>
<p>21[c] performing a payment transaction by the electronic device including the dynamically generated limited-use number;</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs a method comprising performing a payment transaction by the electronic device including the dynamically generated limited-use number (e.g., DPAN, dynamic cryptogram, etc.).</p> <p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant’s acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay’s security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token’s DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder’s mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p><i>See, e.g., Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Google Pay – Device Tokenization – TSP Integration</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</p>

Claim No.	Accused Products
	<div data-bbox="499 228 1554 399"> <div>Token Cryptogram</div> <div>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.</div> </div> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p> <h3>5. End-to-End EMV Payment Tokenization Flows</h3> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> <ul style="list-style-type: none"> In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)  <p>^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.</p> <p>Figure 7. Processing an In-App Transaction Using a Merchant Mobile App with Tokens Provisioned in a Device-Centric Wallet</p> <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 12, 23-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>

Claim No.	Accused Products		
21[d] combining the dynamically-generated number and the static device account number within a device-generated complete payment information; and	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs a method comprising combining the dynamically-generated number (e.g., dynamic cryptogram) and the static device account number (e.g., DPAN) within a device-generated complete payment information.</p> <p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant’s acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay’s security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token’s DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder’s mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p>See, e.g., <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Google Pay – Device Tokenization – TSP Integration</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</p> <table border="1"> <tr> <td>Token Cryptogram</td><td>A cryptogram, containing a transaction-unique value, typically generated using the Payment Token, Payment Token related data and transaction data. Cryptogram derivation methods may vary by scenario and may be Payment System-specific.</td></tr> </table> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</p> <p>5. End-to-End EMV Payment Tokenization Flows</p> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> <ul style="list-style-type: none"> • In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) 	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.
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.		

Claim No.	Accused Products
	 <p>^a Other TSP providers are also possible.</p> <p>^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.</p> <p>^c The payment network to which the transaction is routed may need to be the payment network that provided the token.</p> <p>Figure 7. Processing an In-App Transaction Using a Merchant Mobile App with Tokens Provisioned in a Device-Centric Wallet</p> <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 12, 23-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>
<p>21[e] conveying said device-generated complete payment information, in place of a selected payment issuer information, when the device is performing payment transactions; and</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs a method comprising conveying said device-generated complete payment information (e.g., as identified above), in place of a selected payment issuer information (e.g., PAN or associated expiration date or CVV), when the device is performing payment transactions.</p> <p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant’s acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay’s security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token’s DPAN rather than the FPAN of the card. This “tokenization” provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder’s mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device.

Claim No.	Accused Products
	<p>See, e.g., <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Google Pay – Device Tokenization – TSP Integration</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</p> <p>3.1 In-Store EMV Contactless Payments with Device-Centric Digital Wallets</p> <p>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.</p> <p>5. End-to-End EMV Payment Tokenization Flows</p> <p>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</p> <ul style="list-style-type: none"> In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay) <p>Figure 7. Processing an In-App Transaction Using a Merchant Mobile App with Tokens Provisioned in a Device-Centric Wallet</p> <p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 12, 23-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>

Claim No.	Accused Products
21[f] wherein a using of said static device account number without a valid dynamically generated limited-use number, shall be deniable as invalid, and outside a valid scope of device-limited usage.	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs a method wherein a using of said static device account number without a valid dynamically generated limited-use number, shall be deniable as invalid, and outside a valid scope of device-limited usage (e.g., dynamic cryptogram validation fails).</p> <p>4.2.4 Token Cryptogram and Key Management</p> <p>One primary function of the TSP is to act as the TSM and deliver tokens and associated EMV-based payment applications to token requestors. The delivery and coordination of the keys with the token requestor (either a mobile device manufacturer or a merchant for an online payment) ensures that an EMV-compliant set of transaction data is generated. Transactions are routed to the TSP providing the validation service to validate the cryptogram before going to the issuer for authorization. Depending on the options selected by the issuer, the TSP may reject the transaction if cryptogram validation fails.</p> <p><i>See, e.g., US Payments Forum, EMV Payment Tokenization Primer and Lessons Learned at 24-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</i></p>
22[a] The method of claim 19, further comprising: generating a limited-use security code number for use in place of a card issuer card security code, by cryptographically combining information from at least one of a set of information comprising: a device transaction sequence counter; a device account number; a payment account information, device secrets; payment processing authority secrets; and	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs a method comprising: generating a limited-use security code number (e.g., dynamic cryptogram) for use in place of a card issuer card security code (e.g., CVV), by cryptographically combining information from at least one of a set of information comprising: a device transaction sequence counter (e.g., transaction-unique value); a device account number (e.g., upon information and belief, a DPAN); a payment account information, device secrets (e.g., secret keys); payment processing authority secrets.</p> <p><i>See, e.g., Claim 5[a].</i></p>
22[b] displaying the limited-use security code number on the user-interface of the device display.	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs a method comprising: displaying the limited-use security code number on the user-interface of the device display.</p>

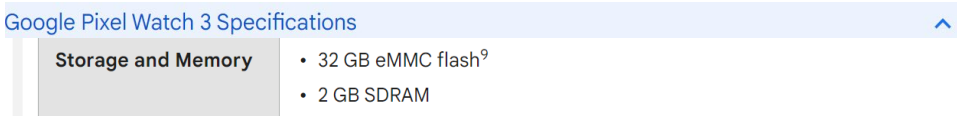
Claim No.	Accused Products
	<p>When you use a virtual card, not only is your actual card information not shared, but it will also change something else about the card in addition to the number. For example, some cards will change the virtual card number for each merchant you shop at, while others will change the CVC or CID, the three- or four-digit security code, in addition to the virtual card number.</p> <p><i>See, e.g., Ask a Techspert: How do virtual cards work for online shopping?</i> https://blog.google/products/google-pay/what-is-a-virtual-card/.</p> <div data-bbox="514 537 1732 628"> <h3>Step 4: View Your Card Details</h3> </div> <p>Tap on the card again to view the full card number.</p> <p>The app will display the full card number, expiration date, and CVV. Please note that for security reasons, you should never share these details with anyone.</p> <p><i>See, e.g., How to See Full Card Number on Google Pay: A Step-by-Step Guide</i>, https://www.live2tech.com/how-to-see-full-card-number-on-google-pay-a-step-by-step-guide/.</p>
<p>23[a] The method of claim 19, wherein a payment processing authority verifying and authorizing a transmitted limited-use number based on a time of use, and cryptographically combining a transaction sequence count information; a device account number; a user account information; a payment issuer information; a payment processing authority secrets; a transaction information; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs a method wherein a payment processing authority (e.g., TSP) verifying and authorizing a transmitted limited-use number (e.g., dynamic cryptogram) based on a time of use, and cryptographically combining a transaction sequence count information (e.g., transaction-unique value); a device account number (e.g., upon information and belief, a DPAN); a user account information; a payment issuer information; a payment processing authority secrets; (e.g., secret keys) a transaction information.</p> <p><i>See, e.g., Claim 5[a], 5[c].</i></p>
<p>23[b] further comprising: receiving an authorization of</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs a method comprising receiving an authorization of said transaction (e.g., transaction approval), responsive to verifying a valid</p>

Claim No.	Accused Products
said transaction, responsive to verifying a valid limited-use number appearing in a transaction information in place of the payment issuer information; and	limited-use number (e.g., dynamic token) appearing in a transaction information in place of the payment issuer information (e.g., CVV). See, e.g., 5[f].
23[c] a rejecting by the payment processing authority, on a detecting as invalid at least one verification test, from a set of tests comprising: a mis-matching of the transacted limited-use number, and the authority cryptographically-combined number; a transactional use of a device account number outside of its limited scope of valid payment reader facility use; a transactional use outside of a valid time window; a transactional re-use of a number limited to a one-time use; and, a transactional use of an expired number outside of a limited time-of-use.	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs a method comprising rejecting by the payment processing authority, on a detecting as invalid at least one verification test, from a set of tests comprising: a mis-matching of the transacted limited-use number, and the authority cryptographically-combined number; a transactional use of a device account number outside of its limited scope of valid payment reader facility use; a transactional use outside of a valid time window; a transactional re-use of a number limited to a one-time use; and, a transactional use of an expired number outside of a limited time-of-use (e.g., if dynamic cryptogram validation fails). See, e.g., 4[b]. 4.2.4 Token Cryptogram and Key Management One primary function of the TSP is to act as the TSM and deliver tokens and associated EMV-based payment applications to token requestors. The delivery and coordination of the keys with the token requestor (either a mobile device manufacturer or a merchant for an online payment) ensures that an EMV-compliant set of transaction data is generated. Transactions are routed to the TSP providing the validation service to validate the cryptogram before going to the issuer for authorization. Depending on the options selected by the issuer, the TSP may reject the transaction if cryptogram validation fails. See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 24-26 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf .
24. The method of claim 19, wherein the user selecting of a payment method at an electronic device comprises receiving a user touch input selection, via the user interface, of a displayed payment method option, on the device touch-screen display interface.	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs a method comprising wherein the user selecting of a payment method at an electronic device comprises receiving a user touch input selection, via the user interface, of a displayed payment method option (e.g., one or more card options), on the device touch-screen display interface. See, e.g., 19[c], 19[d].

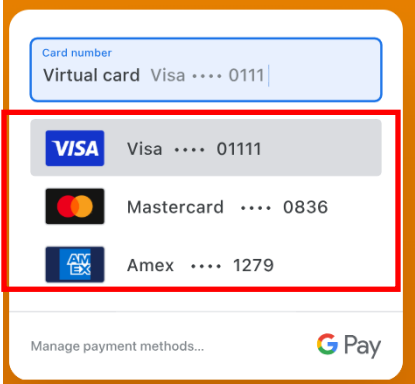
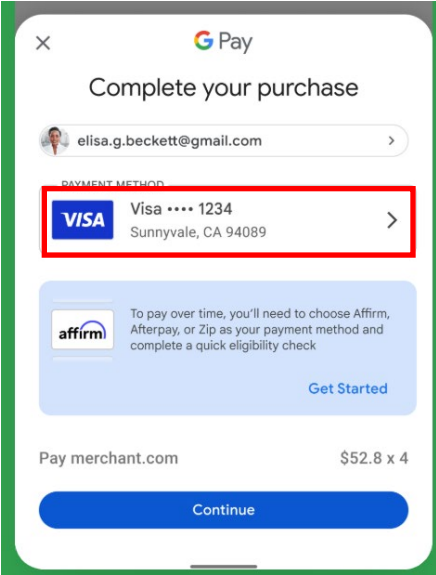
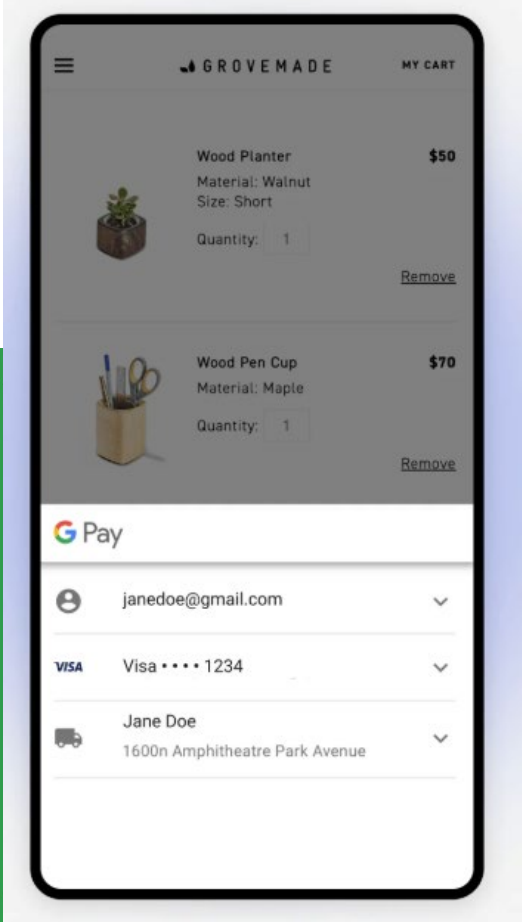
III. Claim 25 and Dependent Claims 26–30

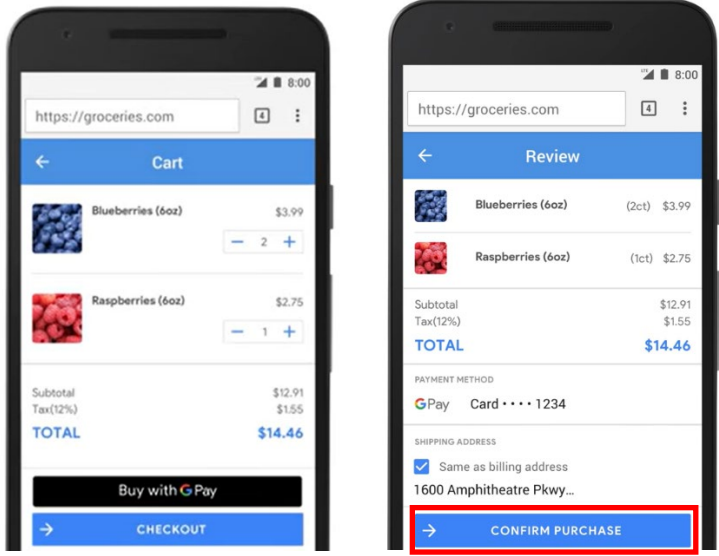
Claim No.	Accused Products				
25[Pre] A non-transitory, computer-readable medium storing computer executable instructions that when executed by one or more processors, cause the one or more processors to:	<p>To the extent the preamble is limiting, a Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, smartwatch, tablet, or laptop, includes a non-transitory, computer readable medium storing instructions (e.g., memory, flash, memory in a SIM/eSIM, or combination of the same) executable by a processor (e.g., a processor, coprocessor, secure element, or any combination of the same).</p> <p><i>See supra</i> limitation 19[pre].</p>  <p><i>See, e.g., Building with Google Pay, https://android-developers.googleblog.com/2018/05/building-with-google-pay.html.</i></p> <p>Pixel Tablet Overview Tech specs</p> <table border="0"> <tr> <td>Memory and storage</td><td>Processor</td></tr> <tr> <td>8 GB LPDDR5 RAM · 128 & 256 GB UFS 3.1 storage</td><td>Google Tensor G2 · Titan M2 security coprocessor</td></tr> </table> <p><i>See, e.g., Pixel Tablet, Tech Specs, https://store.google.com/product/pixel_tablet_specs.</i></p> <p>Samsung Galaxy Chromebook Plus</p> <div>Intel® Core™ 3 CPU, 8 GB RAM, 256 GB storage</div> <p><i>See, e.g., Chromebook, Samsung Galaxy Chromebook Plus, https://www.google.com/chromebook/discover/pdp-samsung-galaxy-chromebook-plus/sku-samsung-galaxy-chromebook-plus-8gb-256gb/.</i></p>	Memory and storage	Processor	8 GB LPDDR5 RAM · 128 & 256 GB UFS 3.1 storage	Google Tensor G2 · Titan M2 security coprocessor
Memory and storage	Processor				
8 GB LPDDR5 RAM · 128 & 256 GB UFS 3.1 storage	Google Tensor G2 · Titan M2 security coprocessor				

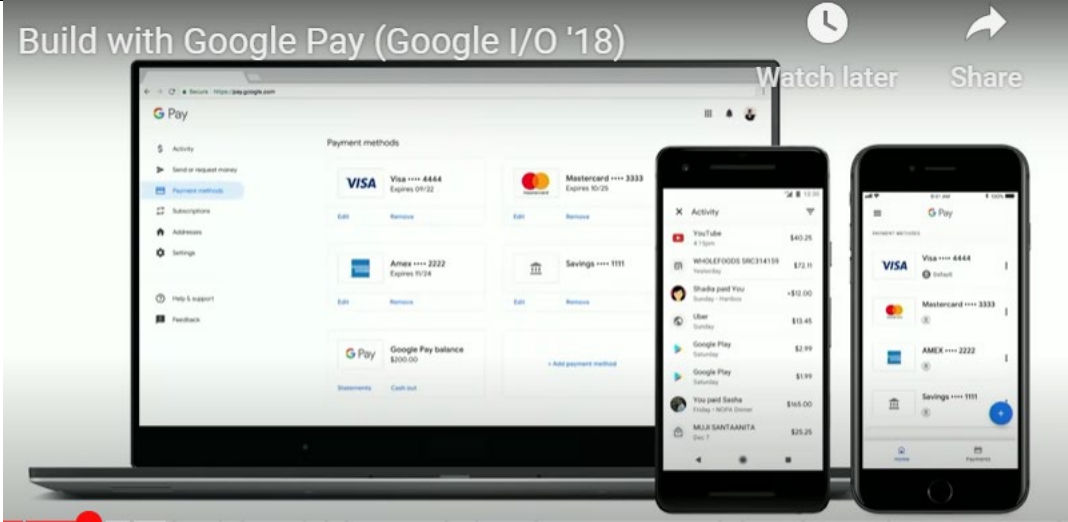
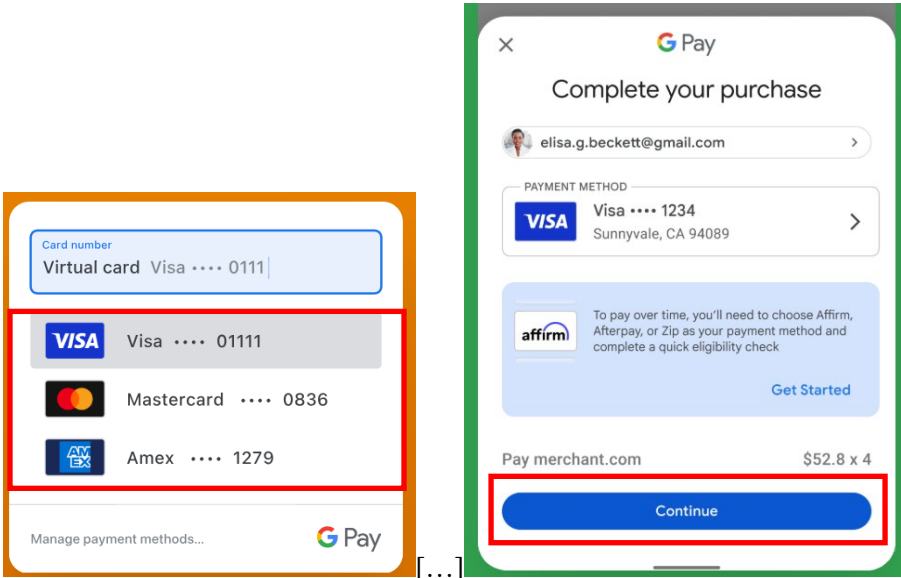
Claim No.	Accused Products
	<div><div>Pixel 9 Pro Fold (2024)</div><div><div>Pixel 9 Pro Fold</div><div><div>Memory & storage</div><div><div>Memory</div><ul style="list-style-type: none">• 16 GB RAM<div>Storage</div><ul style="list-style-type: none">• [US]: 256 GB / 512 GB⁸</div><div>SIMs</div><ul style="list-style-type: none">• Dual SIM (Single Nano SIM and eSIM)²³</div><div>[...]</div></div><div>See, e.g., <i>Pixel phone hardware tech specs</i>, Pixel Phone Help, https://support.google.com/pixelphone/answer/7158570.</div><div><h3>Host-based card emulation</h3><p>When an NFC card is emulated using host-based card emulation, the data is routed directly to the host CPU instead of being routed to a secure element. Figure 2 illustrates how host-based card emulation works:</p><p>The diagram shows an Android device with a Host CPU and an NFC Controller. An NFC Reader is connected to the NFC Controller via a wireless signal. A red arrow indicates data flow from the NFC Reader to the Host CPU, bypassing the NFC Controller. The Host CPU is highlighted with a red box.</p><p>Figure 2. NFC card emulation without a secure element.</p><p>See, e.g., <i>Host-based card emulation overview</i>, https://developer.android.com/develop/connectivity/nfc/hce.</p></div></div>

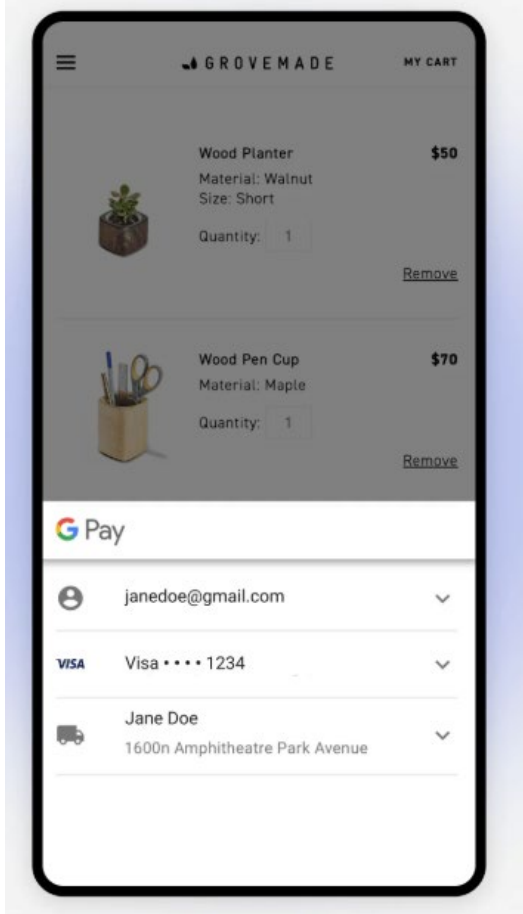
Claim No.	Accused Products
	<ul style="list-style-type: none"> Google Pay on Fitbit is the extension of Google Pay wallet to Secure Element technology, under Google Pay Wallet ID and a different Token Requestor ID (TRID) for Google Pay SE versus Google Pay HCE. <p>See, e.g., <i>Fitbit Pay FAQ</i>, https://developers.google.com/pay/issuers/support/fitbit-faq.</p>  <p>See, e.g., <i>Google Pixel Watch Technical & Device Specifications</i>, Google Pixel Watch Help, https://support.google.com/googlepixelwatch/answer/12651869.</p> <ul style="list-style-type: none"> MediaTek MT3333 GPS SoC Kingston EMMC04G-M627 4GB flash memory Fitbit FBT18SW ARM application processor USI chip (most likely WiFi module) Cirrus Logic CS47L35 Smart Codec with Low Power Audio DSP Cirrus Logic CS40L25B boosted haptic driver NXP SN100T Secure Element <p>See, e.g., <i>Fitbit Sense Teardown</i>, https://www.ifixit.com/Teardown/Fitbit+Sense+Teardown/137130 (Last visited December 8, 2024).</p>
25[a] accept a priming action of the electronic device by an identified valid device user, identified from the device inputs;	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, accepts a priming action of the electronic device (e.g., double pressing the digital crown, opening the Google pay app, unlocking the device, clicking the “G pay” button) by an identified valid device user, identified from the device inputs (e.g., input on the touchscreen of the smartwatch or smartphone).</p> <p>See <i>supra</i> limitation 1[a].</p>

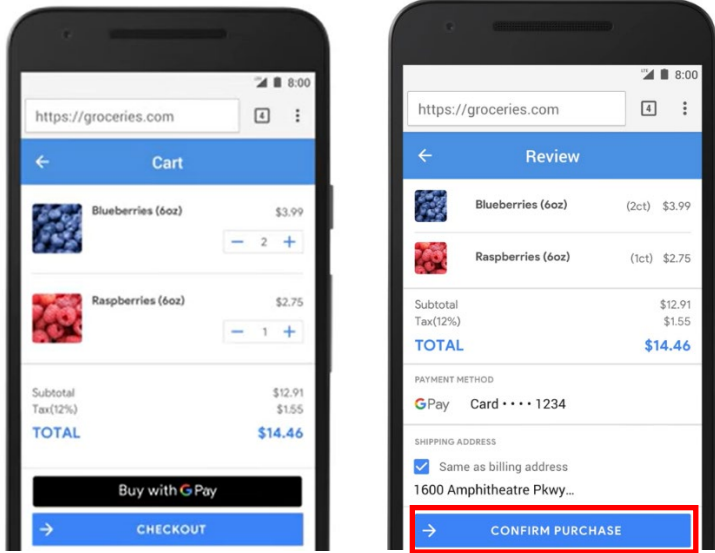
Claim No.	Accused Products
	<div><div>Build with Google Pay (Google I/O '18)</div><div><div><div>Watch later</div><div>Share</div></div><div><div><div><div>Activity</div><div>Send or request money</div><div>Payment methods</div><div>Subscriptions</div><div>Addresses</div><div>Settings</div><div>Help & support</div><div>Feedback</div></div><div><div><div>VISA</div><div>Visa **** 4444</div><div>Expires 01/22</div><div>Edit</div><div>Remove</div></div><div><div>Mastercard</div><div>Mastercard **** 3333</div><div>Expires 02/25</div><div>Edit</div><div>Remove</div></div><div><div>Amex</div><div>Amex **** 2222</div><div>Expires 01/24</div><div>Edit</div><div>Remove</div></div><div><div>Savings</div><div>Savings **** 1111</div><div>Edit</div><div>Remove</div></div><div><div>Google Pay balance</div><div>\$200.00</div><div>Statements</div><div>Cash out</div></div><div><div>+ Add payment method</div></div></div></div></div><div><div><div>Activity</div><div>YouTube</div><div>\$40.25</div><div>4 11pm</div><div>WHOLEFOODS</div><div>\$72.11</div><div>Yesterday</div><div>Shirley paid You</div><div>+\$12.00</div><div>Sunday - Monday</div><div>User</div><div>\$13.45</div><div>Sunday</div><div>Google Play</div><div>\$2.99</div><div>Saturday</div><div>Google Play</div><div>\$1.99</div><div>Saturday</div><div>You paid Shirley</div><div>-\$165.00</div><div>Friday - Monday (Order)</div><div>MILL SANTANITA</div><div>\$25.25</div><div>Dec 7</div></div><div><div><div>Payment methods</div><div>VISA</div><div>Visa **** 4444</div><div>Default</div><div>Mastercard</div><div>Mastercard **** 3333</div><div>AMEX</div><div>AMEX **** 2222</div><div>Savings</div><div>Savings **** 1111</div><div>+ Add payment method</div></div></div></div></div><div>See, e.g., <i>Building with Google Pay</i>, https://android-developers.googleblog.com/2018/05/building-with-google-pay.html.</div></div>

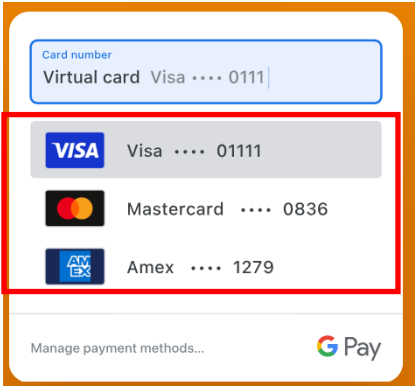
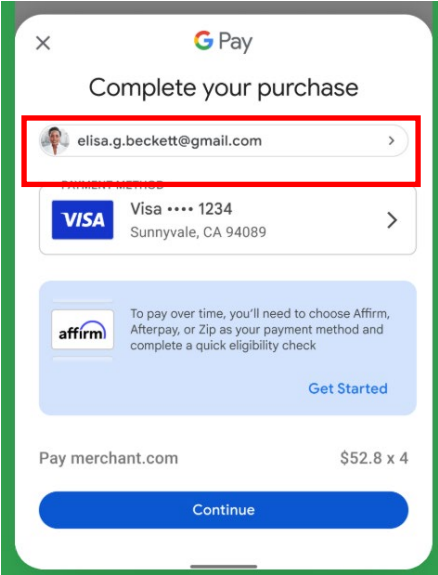
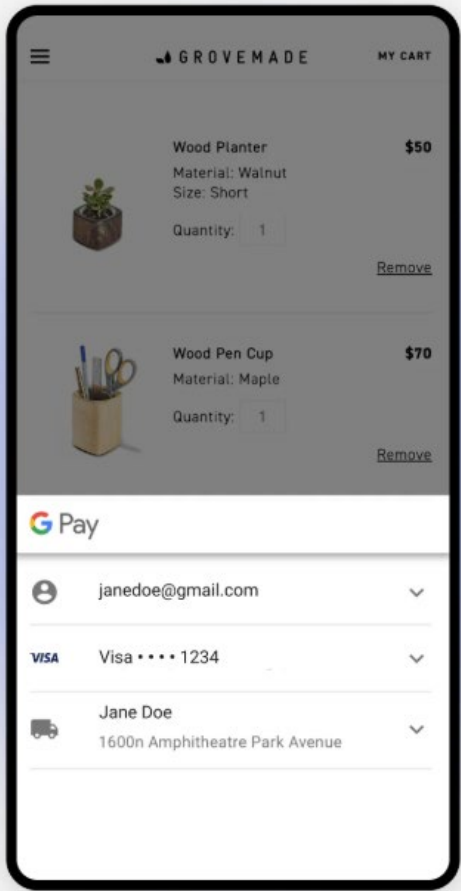
Claim No.	Accused Products
	<div></div> <p>[...]</p> <p>See, e.g., <i>Seamless online checkout</i>, Google, https://pay.google.com/about/pay-online/; Accept Google Pay in your online store, across browsers, and on Android devices, https://www.shopify.com/google-pay.</p>

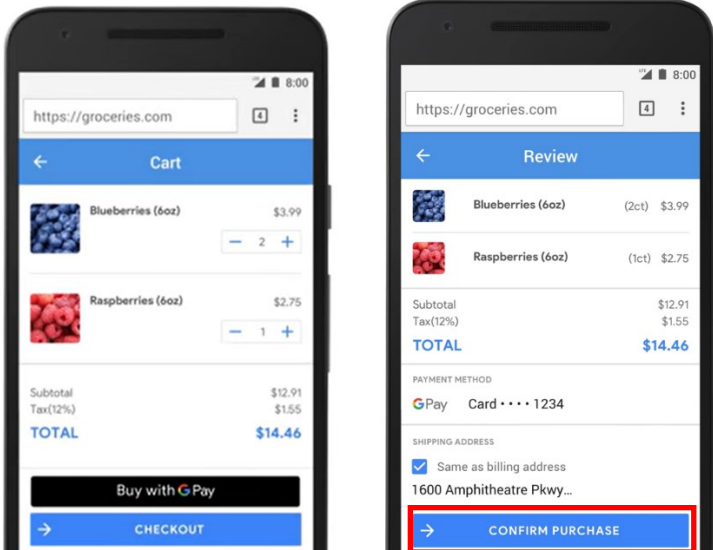
Claim No.	Accused Products
	<p>Just look for Google Pay at checkout in your favorite apps and sites. Finally, confirm your purchase.</p>  <p><i>See, e.g., How do you pay online with Google Pay?, Google Help, https://www.youtube.com/watch?v=yl5SGXiPnDY.</i></p>
25[b] enable the electronic device for imminent performance of a payment operation responsive to the priming action of said valid user;	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, is enabled for the imminent performance of a payment operation (e.g., displaying one or more payment options) responsive to the priming action of said valid user.</p> <p><i>See, e.g., 19[a], 19[b], 19[c].</i></p>

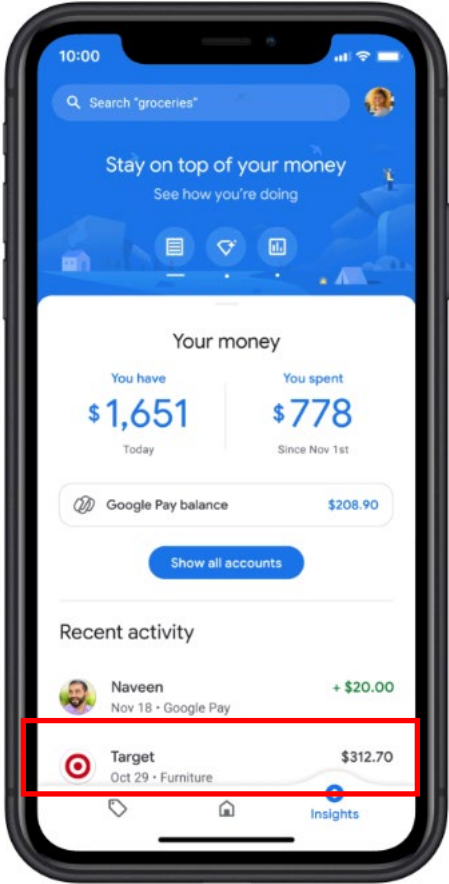
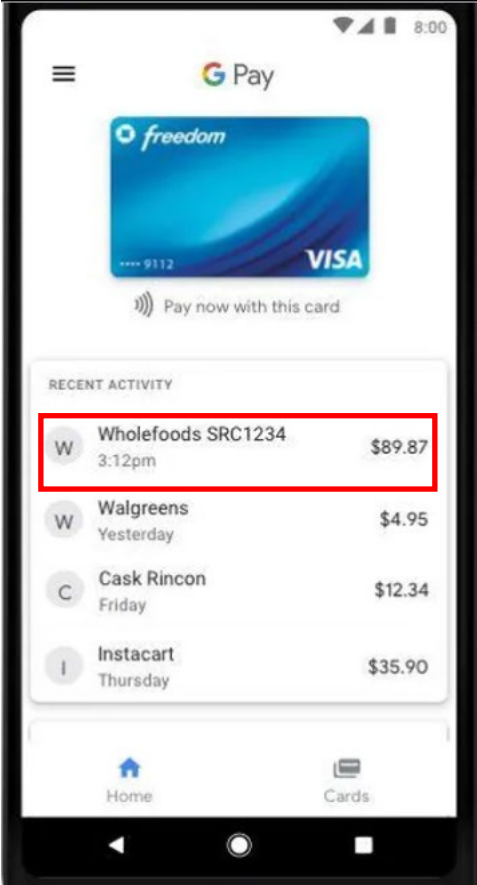
Claim No.	Accused Products
	<div></div> <p>See, e.g., <i>Building with Google Pay</i>, https://android-developers.googleblog.com/2018/05/building-with-google-pay.html.</p> <div></div> <p>See, e.g., <i>Seamless online checkout</i>, Google, https://pay.google.com/about/pay-online/.</p>

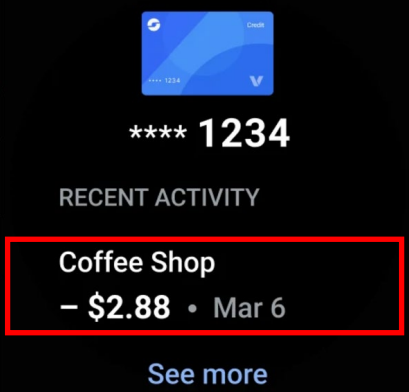
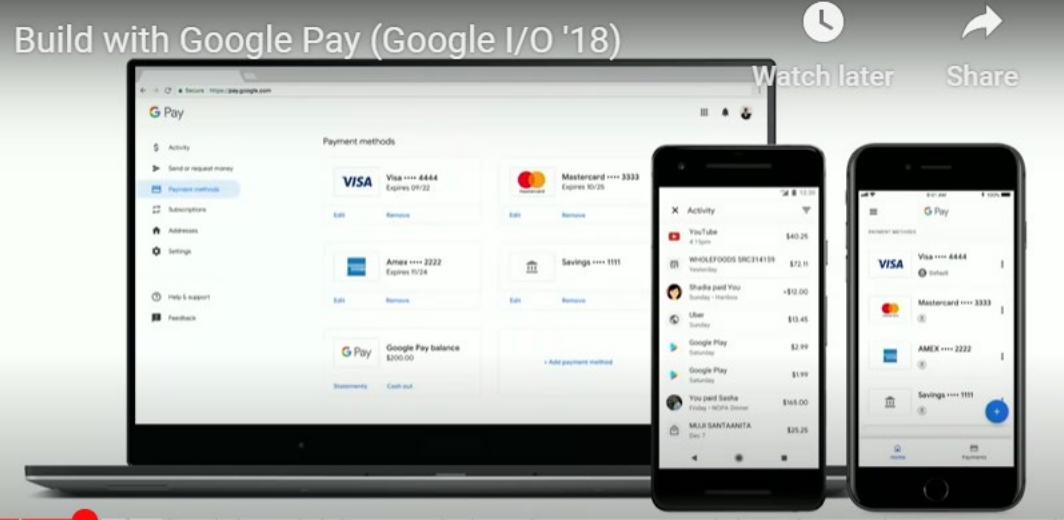
Claim No.	Accused Products
	<div></div> <p>See, e.g., Accept Google Pay in your online store, across browsers, and on Android devices, https://www.shopify.com/google-pay.</p>

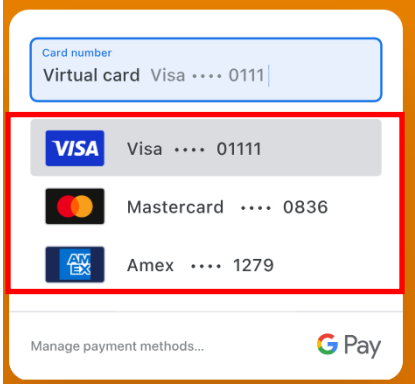
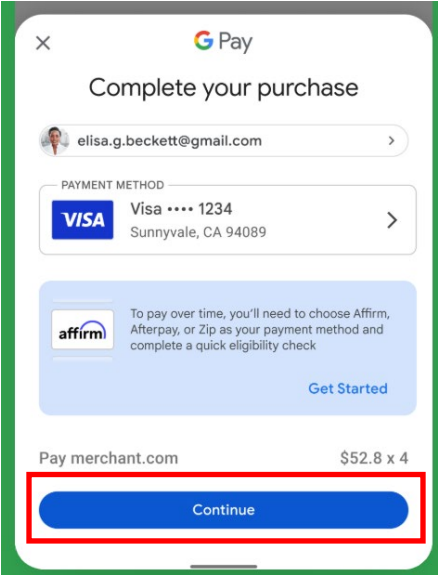
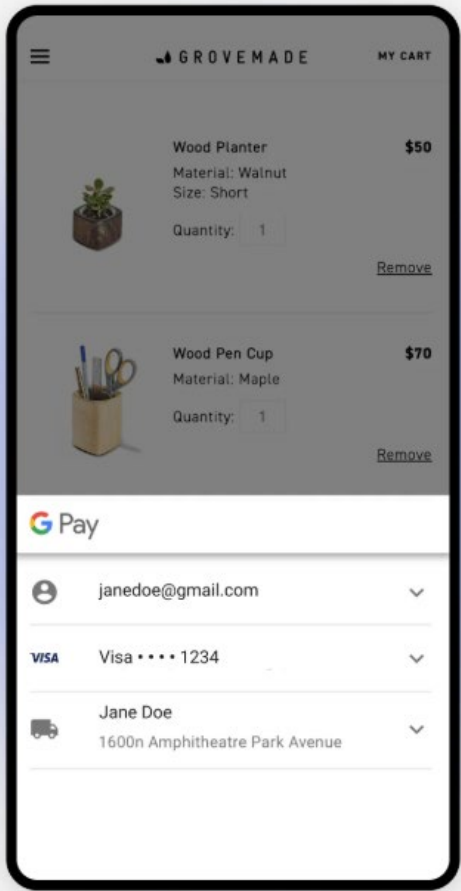
Claim No.	Accused Products
	<p data-bbox="457 240 789 337">Just look for Google Pay at checkout in your favorite apps and sites.</p> <p data-bbox="821 272 1188 305">Finally, confirm your purchase.</p>  <p data-bbox="432 935 1829 967"><i>See, e.g., How do you pay online with Google Pay?, Google Help, https://www.youtube.com/watch?v=yl5SGXiPnDY.</i></p>
25[c] display a summary of online purchase information including the merchant information and the purchase amount; and,	<p data-bbox="432 971 1997 1068">A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, displays a summary of online purchase information including the merchant information (e.g., Whole Foods, Coffee Shop, etc.) and the purchase amount (e.g., dollar amount).</p> <p data-bbox="432 1105 768 1138"><i>See supra</i> limitation 19[pre].</p>

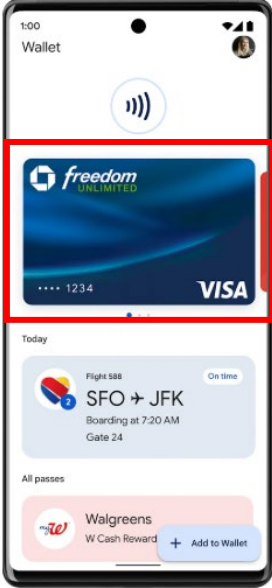
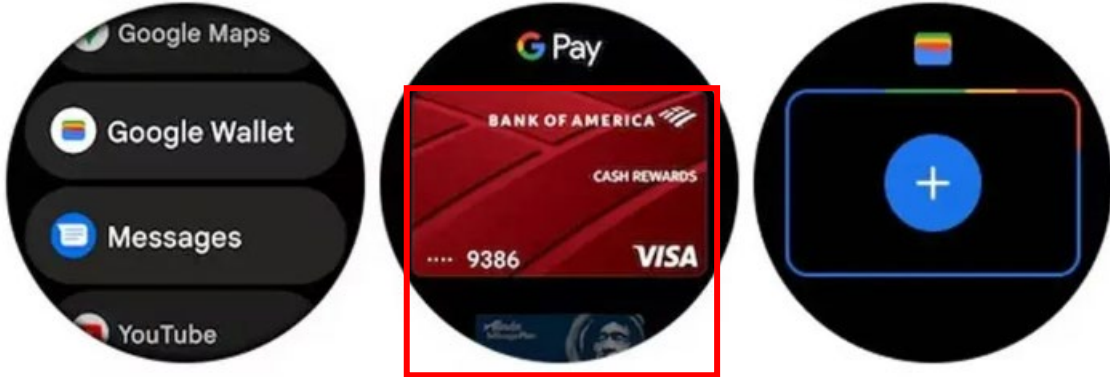
Claim No.	Accused Products
	<div></div> <p>[...] [.]</p> <p>See, e.g., <i>Seamless online checkout</i>, Google, https://pay.google.com/about/pay-online/; Accept Google Pay in your online store, across browsers, and on Android devices, https://www.shopify.com/google-pay.</p>

Claim No.	Accused Products
	<div>Just look for Google Pay at checkout in your favorite apps and sites.</div> <div>Finally, confirm your purchase.</div> <div></div> <div>See, e.g., How do you pay online with Google Pay?, Google Help, https://www.youtube.com/watch?v=y15SGXiPnDY.</div>

Claim No.	Accused Products
	<div></div> <p>See, e.g., <i>Google Pay reimaged: pay, save, manage expenses and more</i>, Google Pay, https://blog.google/products/google-pay/reimagined-pay-save-manage-expenses-and-more/; 6 things you should know about the new Google Pay app, CNET, https://www.cnet.com/tech/services-and-software/things-you-should-know-about-the-new-google-pay-app/.</p>

Claim No.	Accused Products
	 <p>See, e.g., Google Play, Google Wallet, https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfcrel&hl=en_US.</p>
<p>25[d] display at least one selectable issuer payment account methods on a display; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, displays at least one selectable issuer payment account methods (e.g., payment cards) on a display.</p> <p>See <i>supra</i> limitation 19[c].</p>  <p>See, e.g., Building with Google Pay, https://android-developers.googleblog.com/2018/05/building-with-google-pay.html.</p>

Claim No.	Accused Products
	<div></div> <p>See, e.g., <i>Seamless online checkout</i>, Google, https://pay.google.com/about/pay-online/; Accept Google Pay in your online store, across browsers, and on Android devices, https://www.shopify.com/google-pay.</p>

Claim No.	Accused Products
	 <p>See, e.g., Molly McHugh-Johnson, <i>Ask a Techspert: How do digital wallets work?</i>, Google – The Keyword (May 11, 2022), https://blog.google/products/android/ask-a-techspert-google-wallet/.</p>  <p>See, e.g., Vinay Patel, <i>The 6 Best Google Pixel Watch features that make you say wow</i> (October 28, 2022), https://www.gizchina.com/2022/10/28/the-6-best-google-pixel-watch-features-that-make-you-say-wow/.</p>

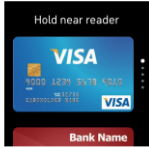
Claim No.	Accused Products
25[e] receive a payment selection and approval authorization from said valid device user via a human input sensing at the device; and	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, receives a payment selection and approval authorization from said valid device user via a human input sensing at the device (e.g., selecting a payment option using a mouse click, or tap). <i>See supra</i> limitation 19[d].
25[f] responsive to receiving a valid user transaction payment approval, generate a device-specific limited-use payment information for use in place of at least a portion of said selected issuer payment account information on the device,	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, responsive to receiving a valid user transaction payment approval, generates a device-specific limited-use payment information (e.g., DPAN) for use in place of at least a portion of said selected issuer payment account information (e.g., PAN) on the device. <i>See supra</i> limitation 19[e].
25[g] form a complete combined device payment information from a dynamically generated portion and a statically generated portions stored in a memory of the device,	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, forms a complete combined device payment information from a dynamically generated portion (e.g., dynamic cryptogram) and a statically generated portions (e.g., DPAN) stored in a memory (e.g., secure element, HCE, memory in a SIM/eSIM, or combination of the same) of the device. <i>See supra</i> limitation 19[f].
25[h] wherein the communication interface is operable to transmit said complete device payment information from said electronic device to the recipient of the online purchase transaction; and	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein the communication interface (e.g., Wifi) is operable to transmit said complete device payment information from said electronic device to the recipient of the online purchase transaction (e.g., an online merchant). <i>See supra</i> limitation 19[i].
25[i] wherein further the processor is operable to	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein further the processor is operable to receive an approval and a denial confirmation from an online payment facility

Claim No.	Accused Products
<p>receive an approval and a denial confirmation from an online payment facility of the complete device payment information, and cause the display to visually convey a status of the online purchase transaction.</p>	<p>(e.g., payment processor, token service provider) of the complete device payment information, and cause the display to visually convey a status of the online purchase transaction.</p> <p><i>See supra</i> limitation 1[j].</p>
<p>26[a] The non-transitory, computer-readable medium of claim 25, wherein the executable instructions further cause the one or more processors to: receive the priming action of a user via the device human input sensors;</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein the executable instructions further cause the one or more processors to: receive the priming action of a user via the device human input sensors (e.g., touch sensors on smartphone, smartwatch, tablet, trackpad, etc.).</p> <p><i>See supra</i> limitations 19[a], 19[b], 19[c].</p>
<p>26[b] identify an authorized valid device user through a human to device inputs, selected from at least one security challenge, of a set of human to device input challenges comprising: a correct passcode touch entry sequence, a correct touch gesture, a touch input of a known device user, a biometric recognition of a valid user,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations to identify an authorized valid device user through a human to device inputs, selected from at least one security challenge, of a set of human to device input challenges comprising: a correct passcode touch entry sequence (e.g., a PIN), a correct touch gesture (e.g., a pattern), a touch input of a known device user, a biometric recognition of a valid user (e.g., face unlock), a biometric sensing of a valid user's skin touch (e.g., fingerprint), a touch input sensor recognition of a unique customer identifier (e.g., fingerprint), a security question which a valid user could answer correctly, and receiving a correct user response input, from a security challenge presented on the device display (e.g., on Account recovery page).</p> <p><i>See supra</i> limitation 1[b].</p>

Claim No.	Accused Products
<p>a biometric sensing of a valid user's skin touch, a touch input sensor recognition of a unique customer identifier, a security question which a valid user could answer correctly, and receiving a correct user response input, from a security challenge presented on the device display; and</p>	<div data-bbox="449 240 1339 297" style="border: 2px solid red; padding: 5px;"> <h2>Sign in to websites with PIN or fingerprint</h2> </div> <p>For quicker access to supported websites and apps in Chrome, you can sign in with your Chromebook PIN or fingerprint.</p> <p>You can sign in with a PIN or fingerprint if:</p> <ul style="list-style-type: none"> • The website supports WebAuthn, a secure web authentication protocol. The website prompts you to turn on WebAuthn for future sign-ins while you use your Chromebook. • You already set up your Chromebook for PIN or fingerprint unlock. <p>Because the credentials are device-specific, you must agree to use WebAuthn on each new device.</p> <p>See, e.g., <i>Chromebook Help</i>, https://support.google.com/chromebook/answer/10364515?hl=en.</p> <hr/> <h3>Tips to complete account recovery steps</h3> <p>If you can't sign in, to try to get back into your Google Account, follow these steps:</p> <ol style="list-style-type: none"> 1. Go to the Account recovery page . 2. As you complete the steps, use as many of the tips below as you can. <p>Tip: You may not find all the questions described here.</p> <p>If you already tried to recover your account and got a “Google couldn't verify this account belongs to you” message, you can try again.</p> <p>Answer as many questions as possible</p> <p>Try not to skip questions. If you're unsure of an answer, take your best guess rather than moving on to another question. Wrong guesses won't kick you out of the process.</p> <p>See, e.g., <i>Google Account Help</i>, https://support.google.com/accounts/answer/7299973.</p>

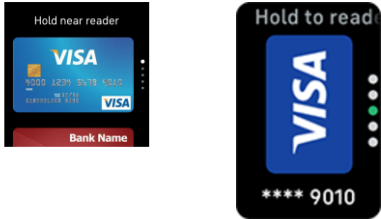
Claim No.	Accused Products
	<p>Verify it’s you to make a purchase</p> <p>To make payments with Google Wallet, you must have a screen lock set up on your device and verify it’s you for your security.</p> <p>You can verify it’s you in Google Wallet with several methods:</p> <ul style="list-style-type: none"> • PIN • Pattern • Password • Class 3 biometric unlock <p>Tip: Google Wallet doesn’t work with Class 1 or Class 2 biometric unlocks or screen locks like Smart Unlock or Knock to Unlock.</p> <p>See, e.g., <i>Verify it’s you to make a purchase</i>, Google Wallet Help, https://support.google.com/wallet/answer/12059519; <i>Set up screen lock for tap to pay transactions</i>, Google Wallet Help Center (captured Dec. 15, 2023), https://web.archive.org/web/20231215153739/https://support.google.com/wallet/answer/12059519#zippy=%2Cpayment-limits-on-a-locked-device (noting for the United States that “Unlock is required for all transactions except for transit”); <i>Set screen lock on your Pixel phone</i>, Pixel Phone Help, https://support.google.com/pixelphone/answer/2819522.</p> <p>7.3.10. Biometric Sensors</p> <p>Biometric sensors can be classified as Class 3 (formerly Strong), Class 2 (formerly Weak), or Class 1 (formerly Convenience) based on their spoof and imposter acceptance rates, and on the security of the biometric pipeline. This classification determines the capabilities the biometric sensor has to interface with the platform and with third-party applications. Sensors need to meet additional requirements as detailed below if they wish to be classified as either Class 1, Class 2 or Class 3.</p> <p>Both Class 2 and Class 3 biometrics get additional capabilities as detailed below.</p> <p>See, e.g., Android 15 Compatibility Definition, https://source.android.com/docs/compatibility/15/android-15-cdd.</p>

Claim No.	Accused Products
	<p>BIOMETRIC_STRONG Added in API level 30</p> <div> <pre>public static final int BIOMETRIC_STRONG</pre> </div> <p>Any biometric (e.g. fingerprint, iris, or face) on the device that meets or exceeds the requirements for Class 3 (formerly Strong), as defined by the Android CDD.</p> <p>This corresponds to <code>KeyProperties.AUTH_BIOMETRIC_STRONG</code> during key generation.</p> <p>See, e.g., BiometricManager.Authenticators, Android Developers, https://developer.android.com/reference/android/hardware/biometrics/BiometricManager.Authenticators#BIOMETRIC_STRONG.</p> <h3>How to use Google Wallet on Pixel Watch</h3> <p>With Screen Lock and Google Wallet set up on Pixel Watch, now it's just a matter of putting the tap-to-pay functionality to use.</p> <ol style="list-style-type: none"> 1. Double-press the crown. 2. Your default card will appear on the screen. 3. If you want to pay with a different card, swipe until you find the card you want to use. 4. Hold your Pixel Watch near the payment terminal. 5. Once the payment has been completed successfully, you will hear a chime and a checkmark appears on your watch. <p>See, e.g., <i>How to use Google Wallet on the Pixel Watch</i>, AndroidCentral (Oct. 19, 2022), https://www.androidcentral.com/wearables/how-to-use-google-wallet-pixel-watch.</p>

Claim No.	Accused Products
	<p>1. If prompted enter your 4-digit device PIN code. your default card appears on the screen.</p> <div style="display: flex; justify-content: space-around; align-items: center;">   </div> <p>2. To pay with your default card, hold your wrist near the payment terminal. To pay with a different card:</p> <p><i>See, e.g., What should I know about using my Fitbit device to make contactless payments?</i> Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</p>
<p>26[c] responsive to receiving an incorrect user response input, offer a reduced number of additional challenge attempts before failing the user authorization at the device, and denying the payment authorization.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, responsive to receiving an incorrect user response input, offers a reduced number of additional challenge attempts (e.g., requiring a PIN, pattern, or password) before failing the user authorization at the device (e.g., fingerprint isn’t recognized), and denying the payment authorization.</p> <p>Authorize payments or unlock apps</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>If a message asks you to scan your fingerprint, follow its instructions. Your fingerprint information isn't shared with the app.</p> </div> <p style="text-align: right;">[...]</p>

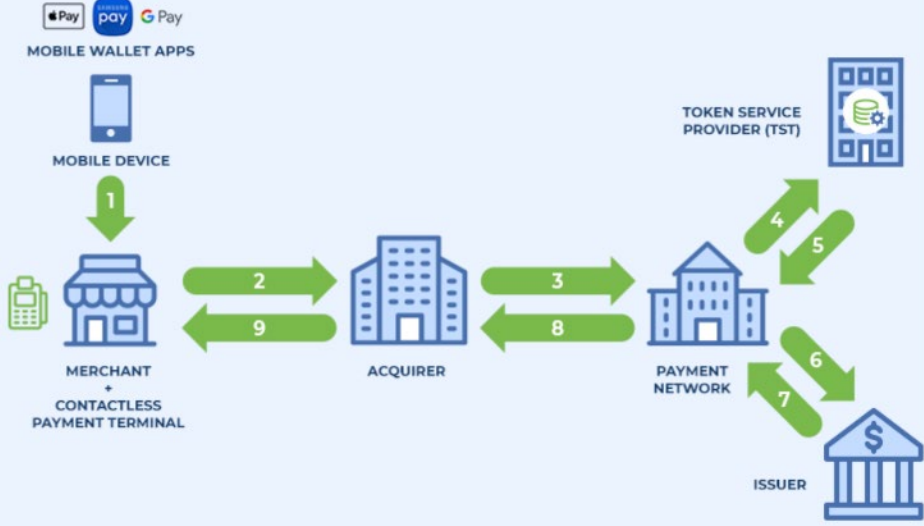
Claim No.	Accused Products
	<p>About fingerprint security</p> <p>We strongly recommend locking your screen to help protect your phone. Your fingerprint sensor gives you a convenient unlocking option.</p> <p>But there are a few things to keep in mind:</p> <ul style="list-style-type: none">• A fingerprint can be less secure than a strong PIN, pattern, or password.• A copy of your fingerprint could be used to unlock your phone. You leave fingerprints on many things you touch, including your phone.• You'll be asked to add a backup PIN, pattern, or password. Remember your backup, because you'll need to use it sometimes, like after restarting your phone, or if your fingerprint isn't recognized. <p>See, e.g., How to unlock your Pixel phone with your fingerprint, https://support.google.com/pixelphone/answer/6285273.</p> <p>Verify it's you to make a purchase</p> <p>To make payments with Google Wallet, you must have a screen lock set up on your device and verify it's you for your security.</p> <p>You can verify it's you in Google Wallet with several methods:</p> <ul style="list-style-type: none">• PIN• Pattern• Password• Class 3 biometric unlock <p>Tip: Google Wallet doesn't work with Class 1 or Class 2 biometric unlocks or screen locks like Smart Unlock or Knock to Unlock.</p> <p>See, e.g., <i>Verify it's you to make a purchase</i>, Google Wallet Help, https://support.google.com/wallet/answer/12059519; <i>Set up screen lock for tap to pay transactions</i>, Google Wallet Help Center (captured Dec. 15, 2023), https://web.archive.org/web/20231215153739/https://support.google.com/wallet/answer/12059519#zippy=%2Cpayment-limits-on-a-locked-device (noting for the United States that “Unlock is required for all transactions except for transit”); <i>Set screen lock on your Pixel phone</i>, Pixel Phone Help, https://support.google.com/pixelphone/answer/2819522.</p>

Claim No.	Accused Products
	<p>7.3.10. Biometric Sensors</p> <p>Biometric sensors can be classified as Class 3 (formerly Strong), Class 2 (formerly Weak), or Class 1 (formerly Convenience) based on their spoof and imposter acceptance rates, and on the security of the biometric pipeline. This classification determines the capabilities the biometric sensor has to interface with the platform and with third-party applications. Sensors need to meet additional requirements as detailed below if they wish to be classified as either Class 1, Class 2 or Class 3. Both Class 2 and Class 3 biometrics get additional capabilities as detailed below.</p> <p>See, e.g., Android 15 Compatibility Definition, https://source.android.com/docs/compatibility/15/android-15-cdd.</p> <p>BIOMETRIC_STRONG Added in API level 30</p> <div> <pre>public static final int BIOMETRIC_STRONG</pre> </div> <p>Any biometric (e.g. fingerprint, iris, or face) on the device that meets or exceeds the requirements for Class 3 (formerly Strong), as defined by the Android CDD.</p> <p>This corresponds to <code>KeyProperties.AUTH_BIOMETRIC_STRONG</code> during key generation.</p> <p>See, e.g., BiometricManager.Authenticators, Android Developers, https://developer.android.com/reference/android/hardware/biometrics/BiometricManager.Authenticators#BIOMETRIC_STRONG.</p>

Claim No.	Accused Products
	<p>How to use Google Wallet on Pixel Watch</p> <p>With Screen Lock and Google Wallet set up on Pixel Watch, now it's just a matter of putting the tap-to-pay functionality to use.</p> <ol style="list-style-type: none"> 1. Double-press the crown. 2. Your default card will appear on the screen. 3. If you want to pay with a different card, swipe until you find the card you want to use. 4. Hold your Pixel Watch near the payment terminal. 5. Once the payment has been completed successfully, you will hear a chime and a checkmark appears on your watch. <p><i>See, e.g., How to use Google Wallet on the Pixel Watch, AndroidCentral (Oct. 19, 2022), https://www.androidcentral.com/wearables/how-to-use-google-wallet-pixel-watch.</i></p> <ol style="list-style-type: none"> 1. If prompted enter your 4-digit device PIN code. Your default card appears on the screen. <div data-bbox="478 841 856 1058">  </div> <ol style="list-style-type: none"> 2. To pay with your default card, hold your wrist near the payment terminal. To pay with a different card: <p><i>See, e.g., What should I know about using my Fitbit device to make contactless payments? Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</i></p>
<p>27[a] The non-transitory, computer-readable medium of claim 25, wherein the one or more processors include a cryptographic processor, and</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein the one or more processors include a cryptographic processor (e.g., processor, coprocessor, secure element, or any combination of the same).</p> <p><i>See supra</i> limitation 1[e], claim 9.</p>

Claim No.	Accused Products
27[b] wherein the executable instructions further cause the one or more processors to: cryptographically compute a dynamically generated one-time-use cryptogram number,	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, cryptographically computes a dynamically generated one-time-use cryptogram number (e.g., dynamic cryptogram). <i>See supra</i> claims 9, 18.
27[c] and combine said dynamically generated portion with a static device-specific account number known to a payment processing authority and limited in use to the device use in place of an issuer payment method; and,	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, combines said dynamically generated portion (e.g., dynamic cryptogram) with a static device-specific account number (e.g., DPAN) known to a payment processing authority and limited in use to the device use in place of an issuer payment method. <i>See supra</i> limitations 1[h], 9[f], 25[g].
27[d] wherein further said cryptogram number is created by said device processor cryptographic combination of device transaction sequence counter count, a payment account information, a user information, and information stored in the device and specific to the device and which is not communicated in the transaction; and,	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein further said cryptogram number is created by said device processor cryptographic combination of device transaction sequence counter count (e.g., transaction-unique value), a payment account information (e.g., DPAN), a user information, and, upon information and belief, information stored in the device and specific to the device and which is not communicated in the transaction (e.g., IMEI no., MAC ID, SSID, BSSID). <i>See supra</i> limitation 20[a].
27[e] wherein said transaction sequence counter, said information	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein said transaction sequence counter (e.g., transaction-unique value), said information and said secrets (e.g., secret keys) are known to both said device, and to said payment processing authority (e.g., TSP).

Claim No.	Accused Products
and said secrets are known to both said device, and to said payment processing authority; and,	<i>See supra</i> limitation 20[a].
27[f] wherein further said static device-specific device account number is known to a payment issuer, and has a device-specific expiration date of limited duration of validity; and,	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein further said static device-specific device account number (e.g., DPAN) is known to a payment issuer (e.g., issuing Bank), and has a device-specific expiration date of limited duration of validity (e.g., token expiration date).</p> <div style="border: 2px solid red; padding: 10px; margin: 10px 0;"> <p>5. If everything is correct, the TSP registers the PAN and links it to a new token in a secure database (<i>Token Vault</i>). Along with the TR identifier, the token expiration date, and a number of additional security features called <i>Token Domain</i>, including restrictions on the use of the new token on certain channels, use by a particular merchant, limitation on the number of permitted uses, and verification of the cryptogram.</p> </div> <p>6. The TSP notifies the application of the newly generated token.</p> <p>7. The application stores the generated token (<i>Device Account Number</i> (DAN) for Apple Pay or Digitized PAN (DPAN) for Samsung Pay) in a secure location (Secure Element (SE) or Host Card Emulation (HCE)).</p> <p>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:</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p style="text-align: right;">[. . .]</p> <p>2. The merchant sends the token and dynamic cryptogram data to the acquirer.</p>

Claim No.	Accused Products
	 <p><i>See, e.g., Mobile payments with digital wallets and tokenization: How Google Pay, Apple Pay and Samsung Pay protect your card details</i>, Advantio (Feb. 22, 2021), available at https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details.</p>
27[g] wherein the generating said complete combined device payment information comprises a device combining said static device-specific device account number, said device account expiration date, said user information, said payment account information, and said dynamically generated cryptogram,	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein the generating said complete combined device payment information comprises a device combining said static device-specific device account number (e.g., DPAN), said device account expiration date, said user information, said payment account information, and said dynamically generated cryptogram (e.g., dynamic cryptogram).</p> <p><i>See supra</i> limitation 1[h].</p>
27[h] and transmitting said complete device	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations transmits said complete device payment information when said issuer payment account method is selected.</p>

Claim No.	Accused Products
payment information when said issuer payment account method is selected.	<i>See supra</i> limitation 1[i].
28[a] The non-transitory, computer-readable medium of claim 25, wherein the executable instructions further causes the one or more processors to perform: a combining of a static device-specific payment account information, a device generated information, and other user and account information stored on the device which is uniquely identifying the specific user, specific selected account, and the specific device; and,	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, combines a static device-specific payment account information (e.g., DPAN), a device generated information (e.g., dynamic cryptogram), and other user and account information stored on the device which is uniquely identifying the specific user, specific selected account, and the specific device. <i>See supra</i> limitation 1[i].
28[b] a generating of a limited-use payment information by the one or more device processors cryptographically generating at least one one-time limited-use cryptogram numbers; and,	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, generates limited-use payment information by the one or more device processors cryptographically generating at least one one-time limited-use cryptogram numbers (e.g., dynamic cryptogram). <i>See supra</i> limitation 1[f].
28[c] wherein the one or more device processors are further operable to combine said limited-use	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein the one or more device processors are further operable to combine said limited-use static device account information (e.g., DPAN) and said one-time use cryptogram number(s) (e.g., dynamic cryptogram) to produce the complete combined device payment information.

Claim No.	Accused Products
static device account information and said one-time use cryptogram number(s) to produce the complete combined device payment information; and,	<i>See supra</i> limitation 1[i].
28[d] wherein the one or more device processors are further operable to transmit said complete payment information in place of said user-selected payment account information in a device payment transaction; and,	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein the one or more device processors are further operable to transmit said complete payment information (e.g., DPAN and dynamic cryptogram) in place of said user-selected payment account information in a device payment transaction. <i>See supra</i> limitation 1[j].
28[e] wherein the one or more device processors are further operable to display at least a portion of said user-specific selected account information associated with said complete device payment information used during said transaction, via a user interface disposed of the device.	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein the one or more device processors are further operable to display at least a portion of said user-specific selected account information associated with said complete device payment information (e.g., last 4 digits) used during said transaction, via a user interface (e.g., touchscreen display) disposed of the device. <i>See supra</i> limitations 19[c], 25[d].
29[a] The non-transitory, computer-readable medium of claim 25, wherein the executable instructions further cause the one or more	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations including dynamically generating a one-time limited-use cryptogram number (e.g., dynamic cryptogram), via a known cryptographic combination of at least one information unique to the electronic device, and also known to at least one of a payment processing authority and a payment issuer authority (e.g., transaction count), and selected from a set of information known and stored at both said payment authorities, and on said device, including: a transaction sequence counter (e.g., transaction-unique value), a device account number (e.g., DPAN), a device account expiration date (e.g., expiration date associated with DPAN), a device secret,

Claim No.	Accused Products
processors to dynamically generate a one-time limited-use cryptogram number, via a known cryptographic combination of at least one information unique to the electronic device, and also known to at least one of a payment processing authority and a payment issuer authority, and selected from a set of information known and stored at both said payment authorities, and on said device, including: a transaction sequence counter, a device account number, a device account expiration date, a device secret, a payment processing authority secret, a user information, a payment account information, a payment issuer information, a payment amount, transactional information; and,	a payment processing authority secret (e.g., limited-use keys), a user information, a payment account information, a payment issuer information, a payment amount, transactional information. <i>See supra</i> limitations 27[c]–[d].
29[b] wherein said one or more processors uses said one-time limited-use cryptogram number	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein said one or more processors uses said one-time limited-use cryptogram number (e.g., dynamic cryptogram) in place of at least a portion of an issuer's static payment information (e.g., CVV), in a payment transaction using said payment account.

Claim No.	Accused Products
in place of at least a portion of an issuer's static payment information, in a payment transaction using said payment account; and,	<i>See supra</i> limitation 1[g].
29[c] wherein said payment authorities are operable to recognize from the transactional payment information, the correct set of user, device and account specific information to be cryptographically combined into an authority computed cryptogram, for comparing with device transmitted limited-use payment information; and,	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein said payment authorities (e.g., payment network, TSP) are operable to recognize from the transactional payment information, the correct set of user, device and account specific information to be cryptographically combined into an authority computed cryptogram, for comparing with device transmitted limited-use payment information (e.g., dynamic cryptogram).</p> <p><i>See supra</i> limitation 5[c].</p>
29[d] wherein said payment processing authorities are operable to deny as invalid a transaction including a cryptogram not matching an authority computed cryptogram; and,	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein said payment processing authorities are operable to deny as invalid a transaction including a cryptogram (e.g., dynamic cryptogram) not matching an authority computed cryptogram.</p> <p><i>See supra</i> limitation 23[c].</p>
29[e] wherein said payment authorities are operable to approve as valid a transaction including a cryptogram matching the payment	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein said payment authorities are operable to approve as valid a transaction including a cryptogram matching the payment processing authority computed cryptogram.</p> <p><i>See supra</i> limitation 25[i].</p>

Claim No.	Accused Products
processing authority computed cryptogram; and,	
29[f] wherein said device is operable to receive an approval and a denial status of said transaction, from said payment authorities, and visually convey said transaction status in the user-interface on the display disposed of the device.	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein said device is operable to receive an approval and a denial status of said transaction, from said payment authorities, and visually convey said transaction status in the user-interface on the display disposed of the device.</p> <p><i>See supra</i> limitation 25[i].</p>
30[a] The electronic device of claim 25, further comprising a processor and a non-transitory, computer-readable medium storing computer executable instructions that when executed by the one or more processors, cause the one or more device processors to dynamically generate a one-time limited-use cryptogram number by a cryptographic combination, of at least one information known to: the device, the payment issuer authority, and a payment processing authority, and unique to the electronic	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, comprises a processor (e.g., processor) and a non-transitory, computer-readable medium (e.g., a memory, flash, memory of secure element or combination of the same) storing computer executable instructions that when executed by the one or more processors, cause the one or more device processors to dynamically generate a one-time limited-use cryptogram number (e.g., a dynamic cryptogram) by a cryptographic combination, of at least one information known to: the device, the payment issuer authority, and a payment processing authority, and unique to the electronic device, and selected from a set of information including: a transaction sequence counter (e.g., transaction-unique value); a user payment account number; a device payment account number (e.g., DPAN); a device secret; device keys (e.g., limited-use keys); a payment issuer original account information; a payment issuer device account information; a payment processing authority secret; a transaction information; and a user private information.</p> <p><i>See supra</i> limitation 20[a].</p>

Claim No.	Accused Products
device, and selected from a set of information including: a transaction sequence counter; a user payment account number; a device payment account number; a device secret; device keys; a payment issuer original account information; a payment issuer device account information; a payment processing authority secret; a transaction information; and a user private information; and,	
30[b] wherein said cryptogram is operable to be used in place of at least a portion of an issuer's static payment information, in a payment transaction for said selected payment account; and,	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein said cryptogram (e.g., dynamic cryptogram) is operable to be used in place of at least a portion of an issuer's static payment information (e.g., CVV), in a payment transaction for said selected payment account. <i>See supra</i> limitation 1[g].
30[c] wherein said payment processing authority is operable to deny as invalid, a transaction including a cryptogram not matching a payment processing authority computed cryptogram; and,	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein said payment processing authority is operable to deny as invalid, a transaction including a cryptogram (e.g., dynamic cryptogram) not matching a payment processing authority computed cryptogram. <i>See supra</i> limitation 23[c].

Claim No.	Accused Products
30[d] wherein said payment processing authority is operable to approve as valid, a transaction including a cryptogram matching the payment processing authority computed cryptogram; and,	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein said payment processing authority is operable to approve as valid, a transaction including a cryptogram (e.g., dynamic cryptogram) matching the payment processing authority computed cryptogram.</p> <p><i>See supra</i> limitation 25[i].</p>
30[e] wherein said user device is operable to receive an approval and a denial status of said transaction information validation, and visually convey said transaction status in the user-interface on the display disposed of the device; and,	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein said user device is operable to receive an approval and a denial status of said transaction information validation, and visually convey said transaction status in the user-interface on the display disposed of the device.</p> <p><i>See supra</i> limitation 25[i].</p>
30[f] wherein said user device is operable to emulate the behavior of an issuer account payment transaction, when said complete device payment information is used in electronic payment facilities.	<p>A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone, laptop, tablet, or smartwatch, performs operations wherein said user device is operable to emulate the behavior of an issuer account payment transaction (e.g., a credit card transaction), when said complete device payment information (e.g., as identified above) is used in electronic payment facilities.</p> <p><i>See supra</i> limitations 1[g], 19[e], 25[f].</p>

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 ’538 Patent and all processes employed by Defendant that practice the methods claimed by the ’538 Patent, consisting of at least products that support Google Pay (alone or with Google Wallet), including the following smartphones, smartwatches, tablets, and Chromebooks⁶, and other smartphones, Chromebooks, and tablets that run on an Android operating system, and other smartwatches that run on Wear OS.

I. Accused Smartphones

The accused smartphones include all variations (e.g., all colors and all storage capacities) of Google Pixel models with Android operating system⁷, and all variations (e.g., all colors and all storage capacities) of other smartphones that run on an Android operating system.

Product	Model Nos.	Product	Model Nos.
Pixel 9 Pro Fold	GGH2X, GC15S	Pixel 5a (5G)	G1F8F, G4S1M
Pixel 9 Pro XL	GGX8B, GZC4K, GQ57S	Pixel 5	GD1YQ, GTT9Q
Pixel 9 Pro	GR83Y, GEC77, GWVK6	Pixel 4a (5G)	GD1YQ, G025I
Pixel 9	G2YBB, GUR25, G1B60	Pixel 4a	G025J
Pixel 8a	GKV4X, G6GPR, G8HHN, G576D	Pixel 4 XL	G020J, GA01181, GA01182, GA01180
Pixel 8 Pro	GKWS6, G9BQD, GA04851-US, GZPFO, GPJ41	Pixel 4	G020M, G020I, GA01188, GA01187, GA01189, GA01191, GA01189
Pixel 8	GKWS6, G9BQD, GA04851-US, GZPFO, GPJ41	Pixel 3a XL	G020C, G020G, G020F
Pixel Fold	G9FPL	Pixel 3a	G020A, G020E, G020B
Pixel 7a	GWKK3, GHL1X, G0DZQ, G82U8	Pixel 3 XL	G013C
Pixel 7 Pro	GVU6C, GQML3, GO3Z5	Pixel 3	G013A
Pixel 7	GVU6C, GQML3, GO3Z5	Pixel 2 XL*	G011C
Pixel 6a	GX7AS, GB62Z, G1AZG, GB17L	Pixel 2*	G011A
Pixel 6 Pro	GLUOG, G8VOU, GF5KQ	Pixel XL*	G-2PW2100, G-2PW2200
Pixel 6	GB7N6, G9S9B16, G9S9B, GR1YH	Pixel*	G-2PW4100, G-2PW4200
Samsung Galaxy A01*	SM-A015A (AT&T), SM-A015T1 (T-Mobile), SM-A015V (Verizon)	BlackBerry DTEK50*	STH100-1
Samsung Galaxy* A02s	SM-A025U, SM-A025A (AT&T), SM-A025T (T-Mobile)	BlackBerry DTEK60*	BBA100-1
Samsung Galaxy A10e*	SM-A102U, SM-A102U1	BlackBerry Evolve X*	BBE100-1

⁶ See, e.g., *Supported devices*, Google Pay (Jul. 19, 2024), <https://developers.google.com/pay/issuers/overview/supported-devices>.

⁷ See, e.g., *Pixel phone hardware tech specs*, Pixel Phone Help, <https://support.google.com/pixelphone/answer/7158570> (last visited Nov. 5, 2024).

Product	Model Nos.	Product	Model Nos.
Samsung Galaxy A11*	SM-A115U, SM-A115A (AT&T), SM-A115T (T-Mobile)	BlackBerry KEY2*	BBF100-1
Samsung Galaxy A12*	SM-A125U, SM-A125U1	BlackBerry KEY2 LE*	BBE100-5
Samsung Galaxy A13*	SM-A135U, SM-A135U1	BlackBerry KEYone*	BBB100-1
Samsung Galaxy A13 5G*	SM-A136U, SM-A136U1	BlackBerry Motion*	BBD100-1
Samsung Galaxy A14 5G*	SM-A146U, SM-A146U1	BlackBerry Priv*	STV100-1
Samsung Galaxy A15 5G*	SM-A156U	Blackview BV9900 Pro*	BV9900Pro
Samsung Galaxy A16*	SM-A165F, SM-A165F/DS, SM-A165M, SM-A165M/DS	Blackview BV9900E*	BV9900E
Samsung Galaxy A16 5G*	SM-A166B, SM-A166B/DS, SM-A166P, SM-A166P/DS, SM-A166E, SM-A166E/DS	Blackview BV4900*	BV4900
Samsung Galaxy A20*	SM-A205U, SM-A205U1	Blackview Wave 8*	Blackview Wave 8
Samsung Galaxy A21*	SM-A215U, SM-A215U1	BLU Advance 4.0*	A010U
Samsung Galaxy A32 5G*	SM-A326U, SM-A326U1	BLU Advance 4.0 L*	A010L
Samsung Galaxy A32 LTE*	SM-A325U, SM-A325U1	BLU Bold N1*	N0010UU
Samsung Galaxy A42*	SM-A426U, SM-A426U1	BLU C5L*	C090U
Samsung Galaxy A50*	SM-A505U, SM-A505U1	BLU C6L*	C130L
Samsung Galaxy A51*	SM-A515U, SM-A515U1	BLU Dash* 5.0+	D410a
Samsung Galaxy A51 5G*	SM-A516U, SM-A516U1	BLU Dash L*	D050U
Samsung Galaxy A52*	SM-A525U, SM-A525U1	BLU Energy X Plus*	E030U
Samsung Galaxy A52 5G*	SM-A526U, SM-A526U1	BLU G80*	G0310WW
Samsung Galaxy A53 5G*	SM-A536U, SM-A536U1	BLU G9*	G0090UU
Samsung Galaxy A54 5G*	SM-A546U, SM-A546U1	BLU G9 Pro*	G0230WW
Samsung Galaxy A55 5G*	SM-A556V, SM-A556B, SM-A556B/DS, SM-A556E, SM-A556E/DS, SM-A5560	BLU G90*	G0370WW
Samsung Galaxy A6*	SM-A600A (AT&T), SM-A600T (T-Mobile)	BLU G90 Pro*	G0370WW
Samsung Galaxy A6+*	SM-A605G (Unlocked)	BLU G91s*	G0410WW

Product	Model Nos.	Product	Model Nos.
Samsung Galaxy A70*	SM-A705MN (Unlocked)	BLU Grand M3*	G0200UU
Samsung Galaxy A71*	SM-A715U, SM-A715U1	BLU Life Max*	L0110UU
Samsung Galaxy A71 5G*	SM-A716U, SM-A716U1	BLU Life One X2*	L0090UU
Samsung Galaxy A71 5G UW*	SM-A716V (Verizon)	BLU Life One X3*	L0150UU
Samsung Galaxy A8 (2018)*	SM-A530F (Unlocked)	BLU Life Play 2*	L190L
Samsung Galaxy A8 Star*	SM-G885F (Unlocked)	BLU Life X8*	L280L
Samsung Galaxy A8+ (2018)*	SM-A730F (Unlocked)	BLU Pure XL*	P0010UU
Samsung Galaxy A9 (2018)*	SM-A920F (Unlocked)	BLU R1 HD*	R0010UU
Samsung Galaxy A90 5G*	SM-A908U (Unlocked)	BLU R2 Plus*	R0170WW
Samsung Galaxy Alpha*	SM-G850A (AT&T), SM-G850T (T-Mobile)	BLU Star 4.5*	S410a
Samsung Galaxy Amp 2*	SM-J120AZ (Cricket Wireless)	BLU Studio 5.5 K*	D670a
Samsung Galaxy Amp Prime*	SM-J320AZ (Cricket Wireless)	BLU Studio 5.5C*	D690a
Samsung Galaxy Amp Prime 2*	SM-J327AZ (Cricket Wireless)	BLU Studio 6.0 HD*	D650a
Samsung Galaxy Amp Prime 3*	SM-J337AZ (Cricket Wireless)	BLU Studio 7.0*	D700a
Samsung Galaxy Avant*	SM-G386T (T-Mobile)	BLU Studio 7.0 II*	D750a
Samsung Galaxy Core Prime*	SM-G360T (T-Mobile), SM-G360V (Verizon)	BLU Studio 7.0 LTE*	S0010UU
Samsung Galaxy Express 3*	SM-J120A (AT&T)	BLU Studio C*	D830U
Samsung Galaxy Express Prime*	SM-J320A (AT&T)	BLU Studio C 5+5*	D890U
Samsung Galaxy Express Prime 2*	SM-J327A (AT&T)	BLU Studio C 5+5 LTE*	D890L
Samsung Galaxy Fold*	SM-F900U, SM-F900U1	BLU Studio C HD*	S090Q
Galaxy Z Flip*	SM-F700	BLU Studio C Super Camera*	S0950UU
Galaxy Z Flip 5G*	SM-F707	BLU Studio Energy*	D810L
Galaxy Z Flip 3*	SM-F711	BLU Studio G*	D790U
Galaxy Z Flip 4*	SM-F721	BLU g64*	G1010WW
Galaxy Z Flip 5*	SM-F731	BLU f5 5g*	F0090UU
Galaxy Z Flip 6*	SM-F741	BLU k10*	K1010WW

Product	Model Nos.	Product	Model Nos.
Samsung Galaxy Z Fold*	SM-F900	BLU g44*	G1010WW
Galaxy Z Fold 2*	SM-F916	Acer Liquid M220*	Acer Liquid M220
Galaxy Z Fold 3*	SM-F926	Alcatel 1*	5033D, 5033X, 5033Y
Galaxy Z Fold 4*	SM-F936	Alcatel 1x Evolve*	5059, 5059D, 5059I, 5059A, 5059Y, 5059X, 5059J, 5059T, 5059Z
Galaxy Z Fold 5*	SM-F946	Alcatel 7*	6062W
Galaxy Z Fold 6*	SM-F956	Alcatel A30*	A30
Samsung Galaxy Grand Prime*	SM-G530T (T-Mobile), SM-G530P (Sprint)	Alcatel A30 Fierce*	5049Z
Samsung Galaxy J1* (2016)	SM-J120A (AT&T)	Alcatel Apprise*	Alcatel Apprise
Samsung Galaxy J2 Core*	SM-J260A (AT&T)	Alcatel Avalon V*	Alcatel Avalon V
Samsung Galaxy J3 (2016)*	SM-J320A (AT&T), SM-J320P (Sprint), SM-J320V (Verizon)	Alcatel Dawn*	Alcatel Dawn
Samsung Galaxy J3 (2017)*	SM-J327A (AT&T), SM-J327P (Sprint), SM-J327V (Verizon)	Alcatel Fierce 4*	5056N, 5056W
Samsung Galaxy J3 (2018)*	SM-J337A (AT&T), SM-J337P (Sprint), SM-J337V (Verizon)	Alcatel Idol 4*	STH-100-2
Samsung Galaxy J3 Emerge*	SM-J327P (Sprint)	Alcatel Idol 4s*	6070K, 6070Y, 6070O
Samsung Galaxy J3 Prime*	SM-J327T (T-Mobile)	Alcatel Idol 5S*	6060X
Samsung Galaxy J3 V*	SM-J337V (Verizon)	Alcatel Insight*	Alcatel Insight
Samsung Galaxy J5*	SM-J500M (Unlocked)	Alcatel Lume*	Alcatel Lume
Samsung Galaxy J5 (2016)*	SM-J510FN (Unlocked)	Alcatel OneTouch Conquest*	OT-7046T
Samsung Galaxy J5* (2017)	SM-J530GM (Unlocked)	Alcatel OneTouch Elevate*	5017B
Samsung Galaxy J6*	SM-J600G (Unlocked)	Alcatel OneTouch Fierce XL*	5054N
Samsung Galaxy J7*	SM-J700T (T-Mobile), SM-J700P (Sprint)	Alcatel OneTouch Flash*	6042D
Samsung Galaxy J7 (2016)*	SM-J710F (Unlocked)	Alcatel OneTouch Flash Plus*	7054D
Samsung Galaxy J7 (2017)*	SM-J727A (AT&T), SM-J727P (Sprint), SM-J727V (Verizon)	Alcatel OneTouch IDOL 3 (4.7")*	6039Y

Product	Model Nos.	Product	Model Nos.
Samsung Galaxy J7 (2017) AT&T*	SM-J727A (AT&T)	Alcatel OneTouch Idol X*	6040D, 6040E, 6040A
Samsung Galaxy J7 (2018)*	SM-J737A (AT&T), SM-J737P (Sprint), SM-J737V (Verizon)	Alcatel OneTouch PIXI 3 (4.5)*	4027X
Samsung Galaxy J7 Perx*	SM-J727P (Sprint)	Alcatel OneTouch PIXI 3 (4)*	4013X
Samsung Galaxy J7 Pop*	SM-J727A (AT&T)	Alcatel OneTouch PIXI 3 (7")*	9002X
Samsung Galaxy J7 Prime*	SM-G610M (Unlocked)	Alcatel OneTouch Pop 2 (4)*	4045X
Samsung Galaxy J7 Refine*	SM-J737P (Sprint)	Alcatel OneTouch POP 2 (5)*	7043E
Samsung Galaxy J7 Star*	SM-J737T (T-Mobile)	Alcatel OneTouch POP 2 (5) Premium*	7044A
Samsung Galaxy J7 V*	SM-J737V (Verizon)	Alcatel ONYX*	Alcatel ONYX
Samsung Galaxy Luna*	SM-S120VL (TracFone)	Alcatel Pixi 4 (6)*	8050D, 9001X, 5098O, 5098S
Samsung Galaxy Mega 2*	SM-G750A (AT&T)	Alcatel Pixi 4 Plus Power*	5023F, 5023E
Samsung Galaxy Mega 6.3*	SGH-I527 (AT&T)	Alcatel POP 4s*	5095K, 5095I
Samsung Galaxy Note 20*	SM-N981U, SM-N981U1	Alcatel POP 7 LTE*	9015W
Samsung Galaxy Note 20 Ultra*	SM-N986U, SM-N986U1	Alcatel SHINE LITE*	5080U, 5080X
Samsung Galaxy Note Fan Edition*	SM-N935F (Unlocked)	Alcatel Streak*	4060O
Samsung Galaxy Mega 2*	SM-G7508Q	Alcatel Tru*	5056N
Samsung Galaxy Mega 6.3*	GT-I9200	Alcatel U5*	4047D, 5044Y, 5044D, 4047X, 5044A, 5044T, 5044O, 4047F, 4047A, 5044I, 5044G
Samsung Galaxy Note 20*	SM-N980F/DS	Alcatel Verso*	Alcatel Verso
Samsung Galaxy Note 20 Ultra*	SM-N985F/DS	Amazon Fire*	SD4930UR
Samsung Galaxy Note Fan Edition*	SM-N935F/DS	ARCHOS 50 Graphite*	AC50G

Product	Model Nos.	Product	Model Nos.
Samsung Galaxy Note10*	SM-N970F/DS	ARCHOS 50 Helium Plus*	AC50HP
Samsung Galaxy Note*	GT-N7000	ARCHOS 55 Graphite*	AC55G
Samsung Galaxy Note 2*	SGH-I317,SCH-I605,SPH-L900	ARCHOS 55 Helium Plus*	AC55HP
Samsung Galaxy Note10+*	SM-N975F/DS	ARCHOS Diamond Omega*	ACDMO
Samsung Galaxy Note10+ 5G*	SM-N976B/DS	Asus ROG Phone*	ZS600KL
Samsung Galaxy Note3*	SM-N9005	Asus ROG Phone 3*	ZS661KS
Samsung Galaxy Note4*	SM-N910F	Asus ROG Phone 3 Strix Edition*	ZS661KS
Samsung Galaxy Note5*	SM-N920F	Asus ROG Phone 5*	ZS673KS
Samsung Galaxy Note8*	SM-N950F	Asus ROG Phone 5 Ultimate*	ZS673KS
Samsung Galaxy Note9*	SM-N960F	Asus ROG Phone 5s*	ZS676KS
Samsung Galaxy Note7*	SM-N930F	Asus ROG Phone 6*	AI2201
Samsung Galaxy Note 2*	GT-N7100	Asus ROG Phone 6 Pro*	AI2201
Samsung Galaxy On7 Prime*	SM-G611F	Asus ROG Phone 6D*	AI2203
Samsung Galaxy On8*	SM-A800F	Asus ROG Phone 6D Ultimate*	AI2203
Samsung Galaxy Pocket 2*	GT-S5310	Asus ROG Phone 7*	AI2205
Samsung GALAXY S II Plus*	GT-I9105	Asus ROG Phone 7 Ultimate*	AI2205
Samsung Galaxy S III mini Value Edition*	GT-I8200N	Asus ROG Phone 8*	AI2401
Samsung Galaxy S10*	SM-G973F	Asus ROG Phone 8 Pro*	AI2401
Samsung Galaxy S10 5G*	SM-G977B	Asus ROG Phone 9*	AI2501
Samsung Galaxy S10 Lite*	SM-G770F	Asus ROG Phone 9 Pro*	AI2501
Samsung Galaxy S10+*	SM-G975F	Asus ROG Phone II*	ZS660KL

Product	Model Nos.	Product	Model Nos.
Samsung Galaxy S10e*	SM-G970F	Asus Zenfone 10*	AI2302
Samsung Galaxy S20*	SM-G980F	Asus Zenfone 11 Ultra*	AI2401_H
Samsung Galaxy S20 FE*	SM-G780F	Asus ZenFone 2 (ZE500CL)*	ZE500CL
Samsung Galaxy S20 Ultra 5G*	SM-G988B	Asus ZenFone 2 Laser*	ZE500KL, ZE550KL, ZE600KL, ZE601KL
Samsung Galaxy S20+*	SM-G985F	Asus ZenFone 2 Laser (US)*	ZE551KL
Samsung Galaxy S21*	SM-G991B	Asus ZenFone 2 Laser 5.5-inch*	ZE550KL
Samsung Galaxy S21 FE*	SM-G990B	Asus Zenfone 2 Laser 6-inch*	ZE601KL
Samsung Galaxy S21 Ultra*	SM-G998B	Asus ZenFone 2E*	Z00D
Samsung Galaxy S21+*	SM-G996B	Asus ZenFone 3*	ZE520KL, ZE552KL
Samsung Galaxy S22*	SM-S901B	Asus ZenFone 3 Deluxe*	ZS570KL, ZS550KL
Samsung Galaxy S22 Ultra*	SM-S908B	Asus ZenFone 3 Deluxe (ZS550KL)*	ZS550KL
Samsung Galaxy S22+*	SM-S906B	Asus ZenFone 3 Ultra*	ZU680KL
Samsung Galaxy S23*	SM-S911B	Asus ZenFone 3 Zoom*	ZE553KL
Samsung Galaxy S23 FE*	SM-S711B	Asus Zenfone 3s Max*	ZC521TL
Samsung Galaxy S23 Ultra*	SM-S918B	Asus ZenFone 4*	ZE554KL
Samsung Galaxy S23+*	SM-S916B	Asus ZenFone 4 Max*	ZC520KL, ZC554KL
Samsung Galaxy S24*	SM-S921B	Asus ZenFone 4 Pro*	ZS551KL

Product	Model Nos.	Product	Model Nos.
Samsung Galaxy S24 FE*	SM-S721B	Asus ZenFone 4 Selfie*	ZD553KL
Samsung Galaxy S24 Ultra*	SM-S928B	Asus ZenFone 4 Selfie Pro*	ZD552KL
Samsung Galaxy S24+*	SM-S926B	Asus ZenFone 5*	ZE620KL
Samsung Galaxy S3*	SGH-I747,SCH-I535,SPH-L710,T999	Asus ZenFone 5Q*	ZC600KL
Samsung Galaxy S4*	SGH-I337 , SCH-I545	Asus ZenFone 5z*	ZS620KL
Samsung Galaxy S4 Active*	GT-I9295	Asus ZenFone 6 (2019)*	ZS630KL
Samsung Galaxy S5*	SM-G900F	Asus ZenFone 7*	ZS670KS
Samsung Galaxy S5 Active*	SM-G870F	BLU Studio Mini LTE*	X100Q
Samsung Galaxy S5 Neo*	SM-G903F	BLU Studio X8 HD 2019*	S532L, S532V, S532U
Samsung Galaxy S6*	SM-G920F	BLU Studio XL*	S790Q
Samsung Galaxy S6 Active*	SM-G890A	BLU Studio XL 2*	S0270UU
Samsung Galaxy S6 edge*	SM-G925F	BLU Vivo 8*	V0150UU
Samsung Galaxy S6 edge+*	SM-G928F	BLU Vivo 8L*	V0170UU
Samsung Galaxy S7*	SM-G930F	BLU Vivo Air*	V050Q
Samsung Galaxy S7 Active*	SM-G891A	BLU Vivo Air LTE*	V0510UU
Samsung Galaxy S7 edge*	SM-G935F	BLU VIVO GO*	V0400WW
Samsung Galaxy S8*	SM-G950F	BLU Vivo Selfie*	V0200EE
Samsung Galaxy S8 Active*	SM-G892A	BLU Vivo X*	V0230UU
Samsung Galaxy S8+*	SM-G955F	BLU VIVO XI*	V0310WW
Samsung Galaxy S9*	SM-G960F	BLU VIVO XI+*	V0320WW
Samsung Galaxy S9+*	SM-G965F	BLU VIVO XL4*	V0330WW
Sonim XP8*	XP8800	CAT S31*	S31
Sony Xperia 1*	J8110	CAT S32*	s32
Sony Xperia 1 II*	XQ-AT51	CAT S40*	S40

Product	Model Nos.	Product	Model Nos.
Sony Xperia 1 III*	XQ-BC62	CAT S41*	S41
Sony Xperia 1 IV*	XQ-CT54	CAT S42*	S42
Sony Xperia 10*	I3113	CAT S48c*	S48c
Sony Xperia 10 II*	XQ-AU51	CAT S50*	S50
Sony Xperia 10 III*	XQ-BT52	CAT S60*	S60
Sony Xperia 10 IV*	XQ-CC54	CAT S61*	S61
Sony Xperia 10 Plus*	I4213	CAT S62 Pro*	S62 Pro
Sony Xperia 5*	J8210	Coolpad Catalyst*	3622A
Sony Xperia 5 II*	XQ-AS52	Coolpad Illumina*	3310A
Sony Xperia 5 III*	XQ-BQ72	Coolpad Legacy*	3705A
Sony Xperia 5 IV*	XQ-CQ62	Coolpad Legacy Brisa*	3706A
Sony Xperia PRO*	XQ-AQ52	Coolpad Legacy S*	3503A
Sony Xperia PRO-I*	XQ-BE62	Coolpad Rogue*	3320A
Sony Xperia X*	F5121	Emporia SMART*	V100
Sony Xperia X Compact*	F5321	Essential Phone*	PH-1
Sony Xperia X Performance*	F8131	HMD Fusion*	TA-1640, TA-1643, TA-1648, or TA-1658
Sony Xperia XA*	F3113	HMD Skyline 5G*	TA-1600
Sony Xperia XA Ultra*	F3213	HMD Vibe*	TA-1590
Sony Xperia XA1*	G3123	HMD XR21 5G*	HMD XR21 5G
Sony Xperia XA1 Plus*	G3423	HTC 10*	HTC 2PS6200
Sony Xperia XA1 Ultra*	G3223	HTC Bolt*	HTC_2PYB2
Sony Xperia XA2*	H3123	HTC Desire 10 Lifestyle*	HTC_D10u
Sony Xperia XA2 Ultra*	H3223	HTC Desire 10 Pro*	HTC_D10i
Sony Xperia XZ*	F8331	HTC Desire 12*	2Q5V100
Sony Xperia XZ Premium*	G8142	HTC Desire 12+*	HTC Desire 12+
Sony Xperia XZ1*	G8342	HTC Desire 22 Pro*	HTC_2QAF100
Sony Xperia XZ1 Compact*	G8441	HTC Desire 510*	HTC_0PCV1

Product	Model Nos.	Product	Model Nos.
Sony Xperia XZ2*	H8266	HTC Desire 516*	HTC_0PCV220
Sony Xperia XZ2 Compact*	H8324	HTC Desire 520*	HTC_0PM11
Sony Xperia XZ2 Premium*	H8166	HTC Desire 526*	HTC_0PM92
Sony Xperia XZ3*	H8416	HTC Desire 530*	HTC_2PST1
Sony Xperia ZL*	C650x	HTC Desire 555*	HTC_2PST5
Sony Xperia Z*	C6606	HTC Desire 626*	HTC_0PM9120
Sony Xperia Z1 Compact*	D5503	HTC Desire 626s*	HTC_0PM9120
Sony Xperia Z2*	D6503	HTC Desire 628*	HTC_2PRG100
Sony Xperia Z3+*	E6553	HTC Desire 630*	HTC_2PST2
Sony Xperia T2 Ultra*	D5303, D5316	HTC Desire 650*	HTC_2PST3
Sony Xperia M2*	D2303, D2305, D2306	HTC Desire 728*	HTC_D728w
T-Mobile REVVL*	T-Mobile REVVL 5049W	HTC Desire 825*	HTC_2PAG100
T-Mobile REVVL 2*	T-Mobile REVVL 2 5052W	HTC Desire 826*	HTC_D826w
T-Mobile REVVL 2 Plus*	T-Mobile REVVL 2 Plus 5060W	HTC One (M7)*	HTC6500,HTC6500LVW,HTC6500L K
T-Mobile REVVL 4*	T-Mobile REVVL 4 5062W	HTC One (M8)*	HTC_0P6B100
T-Mobile REVVL 4+*	T-Mobile REVVL 4+ 5062Z	HTC One A9*	HTC_2PQ9100
T-Mobile REVVL 5G*	T-Mobile REVVL 5G T790W	HTC One E9+*	HTC_A55
T-Mobile REVVL Plus*	T-Mobile REVVL Plus 5049Z	HTC One M9*	HTC_0PJA10
T-Mobile REVVL V+ 5G*	T-Mobile REVVL V+ 5G 5061W	HTC One M9+*	HTC_0PKVZ3
T-Mobile Revvlry*	T-Mobile Revvlry XT1952-T	HTC One ME*	HTC_M9ew
T-Mobile Revvlry+*	T-Mobile Revvlry+ XT1965-T	HTC One Mini 2*	HTC_0P8B2
TCL 10 5G UW*	T790S	HTC One S9*	HTC_2PQ9100
TCL 10 Pro*	T799B	HTC One X10*	HTC_2PS6200
TCL 10L*	T770B	HTC One X9*	HTC_2PS5200
TCL 20 5G*	T781	HTC U Play*	HTC_2PZM100

Product	Model Nos.	Product	Model Nos.
TCL 20 Pro 5G*	T810S	HTC U Ultra*	HTC_2PZF100
TCL 20 SE*	T671H	HTC U11*	HTC_2PZC100
TCL 20S*	T774B	HTC U11 EYEs*	HTC_2Q4R100
TCL 30 V 5G*	T781S	HTC U11 Life*	HTC_2Q33100
TCL 30 XE 5G*	T767W	HTC U11+*	HTC_2Q4D100
TCL 30XL*	T671G	HTC U12+*	HTC_2Q55100
TCL SIGNA*	5004S	HTC U23 Pro*	HTC_2QBA100
Verizon Ellipsis 7*	QMV7A	HTC Wildfire X*	HTC_2Q5G100
Vertu Aster*	RM-980V	Huawei Mate 10 Pro*	HUAWEI_BLA-L29
Vertu Signature Touch*	RM-980	Huawei Mate SE*	HUAWEI_BND-L34
Vertu Signature Touch for Bentley*	RM-980B	Huawei P10*	HUAWEI_VTR-L29
Verykool Jet SL5009*	SL5009	Huawei P20 Lite*	HUAWEI_ANE-LX1
Verykool Spark II s5015*	s5015	Huawei Mate 9*	HUAWEI_MHA-L29
Verykool Maverick LTE SL5550*	SL5550	Huawei SnapTo*	HUAWEI_G620-A2
Verykool Luna s4510*	s4510	Huawei Union*	HUAWEI_Y538
Yezz Andy 4.5E LTE*	4.5E	Huawei Y3*	HUAWEI_Y360-U61
Yezz Andy 4.5EL LTE*	AM45EL133, AM4EL137	Huawei Y6*	HUAWEI_SCL-L01
Yezz Andy 4E*	Yezz Andy 4E	Huawei Y9*	HUAWEI_FLAX-LX1
Yezz Andy 4E LTE*	Yezz Andy 4E LTE	ICEMOBILE Gravity 4.0*	ICEMOBILE Gravity 4.0
Yezz Andy 4E2I*	Yezz Andy 4E2I	ICEMOBILE Prime 5.0*	ICEMOBILE Prime 5.0
Yezz Andy 4EI*	Yezz Andy 4EI	ICEMOBILE Prime 5.0 Plus*	ICEMOBILE Prime 5.0 Plus
Yezz Andy 5.5EI*	Yezz Andy 5.5EI	ICEMOBILE Prime 5.5*	ICEMOBILE Prime 5.5
Yezz Andy 5.5T LTE VR*	Yezz Andy 5.5T LTE VR	Kyocera DuraForce Pro*	KYOCERA_E6820
Yezz Andy 5EI*	Yezz Andy 5EI	Kyocera DuraForce Pro 2*	KYOCERA_E6910

Product	Model Nos.	Product	Model Nos.
Yezz Andy 5EL LTE*	Yezz Andy 5EL LTE	Kyocera DuraForce Ultra*	KYOCERA_E7110
Yezz Andy 5M LTE*	AM5ML133	Kyocera DuraForce XD*	KYOCERA_E6790
Yezz Andy 6EL LTE*	Yezz Andy 6EL LTE	Kyocera Hydro AIR*	KYOCERA_C6745
Yezz Andy C5ML*	Yezz Andy C5ML	Kyocera Hydro Reach*	KYOCERA_C6743
Yezz Andy C5QL*	Yezz Andy C5QL	Kyocera Hydro View*	KYOCERA_C6742
Yezz Andy C5VP*	Yezz Andy C5VP	Kyocera Hydro Wave*	KYOCERA_C6740
Zen Mobile 105 Max*	Zen Mobile 105 Max	Lenovo Phab 2 Pro*	LENOVO_PB2-690Y
Zen Mobile 303 Elite 2*	Zen Mobile 303 Elite 2	LG V10*	H960A
Zen Mobile Admire* Curve*	Zen Mobile Admire Curve	LG V20*	H918
Zen Mobile Admire Fab*	Zen Mobile Admire Fab	LG V30*	H930
Zen Mobile Admire Fab Q*	Zen Mobile Admire Fab Q	LG V35 ThinQ*	V350AWM
Zen Mobile Cinemax 2*	Zen Mobile Cinemax 2	LG V40 ThinQ*	LM-V405UA,LM-V405EBW
Zen Mobile Ultrafone 303 Elite*	Zen Mobile Ultrafone 303 Elite	LG V50 ThinQ*	LM-V450PM
Zen Mobile Ultrafone 303 Quad*	Zen Mobile Ultrafone 303 Quad	LG V60 ThinQ*	LM-V600TM,LM-V600AM
Zen Mobile Ultrafone 402 Sport*	Zen Mobile Ultrafone 402 Sport	LG Arena 2*	LM-X320
Zen Mobile Ultrafone 506*	Zen Mobile Ultrafone 506	LG Aristo*	MS210
Zen Mobile Ultrafone Megashot 1*	Zen Mobile Ultrafone Megashot 1	LG Aristo 2*	LM-X210MA
Zen Mobile WOW*	Zen Mobile WOW	LG Aristo 4+*	LM-X320MA
ZTE Avid Plus*	Z828	LG Aristo 5*	LM-K300MM
ZTE Avid Trio*	ZTE Avid Trio	LG Escape 2*	H443
ZTE Axon*	ZTE Axon	LG Escape Plus*	LM-X320
ZTE Axon 10 Pro*	A10P3251, A10P3351	LG Fortune*	M153
ZTE Axon 30 Ultra*	A2022P, A2022PG	LG Fortune 3*	LM-K300AM
ZTE Axon 40 Pro*	A2023G, A2023	LG G Pro 2*	D838

Product	Model Nos.	Product	Model Nos.
ZTE Axon 40 Ultra*	ZTE Axon 40 Ultra	LG G Stylo*	H631, LS770
ZTE Axon 7*	ZTE Axon 7	LG G Vista 2*	H740
ZTE Axon 7 Mini*	B2017G	LG G flex*	D959 ,D950 , LS995
ZTE Axon M*	Z999	LG G2*	D800, LS980,VS980
ZTE Axon Pro*	ZTE Axon Pro	LG G3*	D850, D851, D855
ZTE Blade 10*	ZTE Blade 10	LG G4*	H810, H811, H815
ZTE Blade 11 Prime*	ZTE Blade 11 Prime	LG G5*	H820, H830, H850
ZTE Blade Max 2s*	ZTE Blade Max 2s	LG G6*	H870, H871, H872
ZTE Blade Max 3*	ZTE Blade Max 3	LG G6+*	H870DS
ZTE Blade Max View*	Z610DL	LG G8 ThinQ*	LM-G820
ZTE Blade Spark*	ZTE Blade Spark	LG G8X ThinQ*	LM-G850
ZTE Blade Vantage*	ZTE Blade Vantage	LG Harmony*	M257
ZTE Blade Vantage 2*	ZTE Blade Vantage 2	LG Harmony 2*	LM-X410CS
ZTE Blade X*	ZTE Blade X	LG Harmony 3*	LM-X420CS
ZTE Blade X Max*	ZTE Blade X Max	LG Harmony 4*	LM-K400AM
ZTE Blade Z Max*	Z610DL	LG K10*	K420N, K430DS
ZTE Fanfare*	ZTE Fanfare	LG K20 V*	VS501
ZTE Fanfare 2*	ZTE Fanfare 2	LG K3*	K100
ZTE Grand X 3*	Z959	LG K30*	LM-X410MK
ZTE Grand X 4*	ZTE Grand X 4	LG K30 2019*	LM-X320QMG
ZTE Grand X Max 2*	Z988	LG K31*	LM-K300QM
ZTE Maven*	ZTE Maven	LG K40*	LM-X420
ZTE Maven 2*	Z831	LG K51*	LM-K500UM
ZTE Maven 3*	ZTE Maven 3	LG K92*	LM-K920AM
ZTE Max XL*	N9560, Z983	LG K8*	K350N
ZTE Max+*	ZTE Max+	LG K8 2017*	X240
ZTE Obsidian*	Z820	LG K8V*	VS500
ZTE Optik 2*	ZTE Optik 2	LG K8x*	LM-X120EMW
ZTE Overture 2*	ZTE Overture 2	LG L70*	D320
ZTE Prestige*	ZTE Prestige	LG L90*	D405
ZTE Prestige 2*	ZTE Prestige 2	LG Lancet for Android*	VW820
ZTE Sonata 2*	ZTE Sonata 2	LG Optimus L9 II*	D605

Product	Model Nos.	Product	Model Nos.
ZTE Sonata 3*	ZTE Sonata 3	LG Optimus Zone 3*	VS425PP
ZTE Tempo*	ZTE Tempo	LG Phoenix 2*	K371
ZTE Tempo Go*	N9137GO	LG Phoenix 3*	M150
ZTE Tempo X*	ZTE Tempo X	LG Phoenix 5*	LM-K300AM
ZTE Warp 7*	N9519	LG Phoenix Plus*	LM-X410AS
ZTE Warp Elite*	ZTE Warp Elite	LG Prime 2*	LM-X320AA
ZTE ZMAX 2*	Z958	LG Q Stylus*	Q710MS
ZTE Zmax Pro*	Z981	LG Risio 4*	LM-K300CM
REDMAGIC 10 Pro*	NX789J	LG Spree*	K120
REDMAGIC 9S Pro*	NX769J	LG Stylo 2*	LS775
NUU B30 Pro*	NUU B30 Pro	Motorola Defy (2021)*	XT2083-8
NUU N10*	NUU N10	Motorola DROID MAXX*	XT1080
NUU A25*	NUU A25	Motorola DROID MAXX 2*	XT1565
NUU A15*	NUU A15	Motorola DROID Turbo 2*	XT1585
NUU A23 Plus*	NUU A23 Plus	Motorola DROID Ultra*	XT1080
NUU B20 5G*	NUU B20 5G	Motorola Edge*	XT2063-2
NUU B10*	NUU B10	Motorola Edge (2021)*	XT2141-1
ulefone Armor X31 Pro*	ulefone Armor X31 Pro	Motorola Edge (2022)*	XT2205-3
ulefone Armor Mini 20*	ulefone Armor Mini 20	Motorola Edge (2023)*	XT2301-4
ulefone Armor 27T*	ulefone Armor 27T	Motorola Edge 20*	XT2143-1
ulefone Armor 27*	ulefone Armor 27	Motorola Edge 20 Lite*	XT2139-1
Ulefone Armor 27T Pro*	Ulefone Armor 27T Pro	Motorola Edge 20 Pro*	XT2153-1

Product	Model Nos.	Product	Model Nos.
Ulefone Armor 25T Pro*	Ulefone Armor 25T Pro	Motorola Edge 30*	XT2203-1
Ulefone Armor 26 Ultra Walkie-Talkie*	Ulefone Armor 26 Ultra Walkie-Talkie	Motorola Edge 30 Fusion*	XT2243-1
Ulefone Armor X13*	Ulefone Armor X13	Motorola Edge 30 Neo*	XT2245-1
Ulefone Armor X12 Pro*	Ulefone Armor X12 Pro	Motorola Edge 30 Ultra*	XT2241-1
Ulefone Armor X12*	Ulefone Armor X12	Motorola Edge 40*	XT2303-1
Ulefone Armor 24*	Ulefone Armor 24	Motorola Edge 40 Neo*	XT2307-1
Ulefone Armor 21*	Ulefone Armor 21	Motorola Edge 40 Pro*	XT2301-4
Ulefone Armor 22*	Ulefone Armor 22	Motorola Edge 50*	XT2401-1
Ulefone Armor 20WT*	Ulefone Armor 20WT	Motorola Edge 50 Fusion*	XT2403-1
Ulefone Armor 17 Pro*	Ulefone Armor 17 Pro	Motorola Edge 50 Neo*	XT2405-1
Ulefone Armor 15*	Ulefone Armor 15	Motorola Edge 50 Pro*	XT2407-1
Ulefone Armor 12S*	Ulefone Armor 12S	Motorola Edge 50 Ultra*	XT2409-1
Ulefone Armor 11T 5G*	Ulefone Armor 11T 5G	Motorola Edge+*	XT2061-1
Ulefone Armor 11 5G*	Ulefone Armor 11 5G	Motorola Edge+ (2022)*	XT2201-1
Ulefone Armor 10*	Ulefone Armor 10	Motorola Edge+ (2023)*	XT2301-4
Ulefone Armor 9*	Ulefone Armor 9	Motorola Moto C*	XT1750
Ulefone Note 21*	Ulefone Note 21	Motorola Moto C Plus*	XT1723
Ulefone Note 20 Pro*	Ulefone Note 20 Pro	Motorola Moto E*	XT1021
Ulefone Note 19*	Ulefone Note 19	Motorola Moto E (2020)*	XT2052-1

Product	Model Nos.	Product	Model Nos.
Ulefone Note 18 Ultra*	Ulefone Note 18 Ultra	Motorola Moto E20*	XT2155-1
Ulefone Note 18 Pro	Ulefone Note 18 Pro	Motorola Moto E3*	XT1700
Ulefone Power Armor 18T Ultra Version*	Ulefone Power Armor 18T Ultra Version	Motorola Moto E4*	XT1766
Ulefone Power Armor 18 Ultra Version*	Ulefone Power Armor 18 Ultra Version	Motorola Moto E4 Plus*	XT1770
Ulefone Power Armor 16S*	Ulefone Power Armor 16S	Motorola Moto E40*	XT2159-3
Ulefone Power Armor 19T*	Ulefone Power Armor 19T	Motorola Moto E5*	XT1944-4
Ulefone Power Armor 19*	Ulefone Power Armor 19	Motorola Moto E5 Play*	XT1921-1
Ulefone Power Armor 18T*	Ulefone Power Armor 18T	Motorola Moto E6*	XT2005-3
Ulefone Power Armor 18*	Ulefone Power Armor 18	Motorola Moto E6 Play*	XT2029-1
Ulefone Power Armor 16 Pro*	Ulefone Power Armor 16 Pro	Motorola Moto E6 Plus*	XT2025-1
Ulefone Power Armor 14 Pro*	Ulefone Power Armor 14 Pro	Motorola Moto E6s*	XT2025-2
Ulefone Power Armor 13*	Ulefone Power Armor 13	Motorola Moto E7 Plus*	XT2081-2
UMIDIGI A15*	UMIDIGI A15	Motorola Moto G (2013)*	XT1031
UMIDIGI A15C*	UMIDIGI A15C	Motorola Moto G (2014)*	XT1063,XT1064
UMIDIGI A15T*	UMIDIGI A15T	Motorola Moto G (2015)*	XT1540
UMIDIGI A13 Pro*	UMIDIGI A13 Pro	Motorola Moto G 5G*	XT2113-3
UMIDIGI A13S*	UMIDIGI A13S	Motorola Moto G 5G (2022)*	XT2213-3
UMIDIGI G9 5G*	UMIDIGI G9 5G	Motorola Moto G 5G (2023)*	XT2313-3
UMIDIGI G9T*	UMIDIGI G9T	Motorola Moto G Play 5G (2024)*	XT2413-3

Product	Model Nos.	Product	Model Nos.
UMIDIGI G9A*	UMIDIGI G9A	Motorola Razr 2022*	XT2251-1
UMIDIGI G6 5G*	UMIDIGI G6 5G	Motorola Razr 5G*	XT2071-4
UMIDIGI G5 Mecha*	UMIDIGI G5 Mecha	Motorola Razr 2024*	PB250016us
UMIDIGI BISON GT2 5G*	UMIDIGI BISON GT2 5G	Motorola Razr +*	Xt2451-2
UMIDIGI BISON GT2 PRO 5G*	UMIDIGI BISON GT2 PRO 5G	Nokia 1*	TA-1047
UMIDIGI BISON 2*	UMIDIGI BISON 2	Nokia 1 Plus*	TA-1130
UMIDIGI BISON 2 PRO*	UMIDIGI BISON 2 PRO	Nokia 1.3*	TA-1205
UMIDIGI BISON X20*	UMIDIGI BISON X20	Nokia 1.4*	TA-1322
UMIDIGI Power 5*	UMIDIGI Power 5	Nokia 2*	TA-1029
Nokia T10*	TA-1447	Nokia 2 V*	TA-1136
Nokia X*	RM-980	Nokia 2 V Tella*	TA-1273
Nokia X+*	RM-1053	Nokia 2.1*	TA-1080
Nokia X10*	TA-1332	Nokia 2.2*	TA-1183
Nokia X100*	TA-1395	Nokia 2.3*	TA-1206
Nokia X20*	TA-1341	Nokia 2.4*	TA-1270
Nokia X30*	TA-1450	Nokia 3*	TA-1032
Nokia XR20*	TA-1362	Nokia 3 V*	TA-1153
Nothing Phone (1)*	A063	Nokia 3.1*	TA-1063
Nothing Phone (2)*	A065	Nokia 3.1 A*	TA-1140
Nubia Red Magic 3/3S*	NX629J	Nokia 3.1 C*	TA-1141
Nubia Red Magic 5G/5S*	NX659J	Nokia 3.1 Plus*	TA-1118
Nubia Red Magic 7*	NX679J	Nokia 3.2*	TA-1159
Nubia Red Magic 7 Pro*	NX709J	Nokia 3.4*	TA-1285
Nubia Red Magic Mars*	NX619J	Nokia 4.2*	TA-1133
OnePlus 10 Pro*	NE2215	Nokia 5*	TA-1053
OnePlus 10T*	CPH2417	Nokia 5.1*	TA-1075
OnePlus 11*	CPH2451	Nokia 5.1 Plus*	TA-1105
OnePlus 12*	CPH2583	Nokia 5.3*	TA-1234
OnePlus 12R*	CPH2585	Nokia 5.4*	TA-1333
OnePlus 2*	A2005	Nokia 6*	TA-1021
OnePlus 3*	A3000	Nokia 6 (2018)*	TA-1054

Product	Model Nos.	Product	Model Nos.
OnePlus 3T*	A3000	Nokia 6.1 Plus*	TA-1103
OnePlus 5*	A5000	Nokia 6.2*	TA-1198
OnePlus 5T*	A5010	Nokia 7 plus*	TA-1046
OnePlus 6*	A6003	Nokia 7.1*	TA-1100
OnePlus 6T*	A6013	Nokia 7.2*	TA-1196
OnePlus 7 Pro*	GM1917	Nokia 8*	TA-1004
OnePlus 7T Pro 5G McLaren*	HD1925	Nokia 8 Sirocco*	TA-1005
OnePlus 8*	IN2015	Nokia 8 V 5G UW*	TA-1243
OnePlus 8 Pro*	IN2025	Nokia 8.1*	TA-1121
OnePlus 8 UW*	IN2019	Nokia 8.3 5G*	TA-1243
OnePlus 8T*	KB2007	Nokia 9 PureView*	TA-1082
OnePlus 9*	LE2115	Nokia C1 Plus*	TA-1312
OnePlus 9 Pro*	LE2125	Nokia C10*	TA-1342
OnePlus Nord N10*	BE2025	Nokia C110*	N156DL
OnePlus Nord N100*	BE2013	Nokia C2 Tava*	TA-1214
OnePlus Nord N20 5G*	GN2200	Nokia C30*	TA-1357
OnePlus Nord N200 5G*	DE2117, DE2118	Nokia C300*	N152DL
OnePlus Nord N30*	CPH2513	Nokia C5 Endi*	TA-1222
OnePlus Nord N300 5G*	CPH2389	Nokia G10*	TA-1338
OnePlus Open*	CPH2579	Nokia G11 Plus*	TA-1424
Orbic Myra 5G*	R678L5	Nokia G20*	TA-1346
Palm Phone*	PVG100	Nokia G21*	TA-1404
Razer Phone*	RZ35-0215	Nokia G310*	TA-1571
Razer Phone 2*	RZ35-0259	Nokia G400*	TA-1448
RED Hydrogen One*	H1A1000	Nokia G50*	TA-1361
LG Optimus F6*	D500 (T-Mobile)	LG Tribute Empire*	LG Tribute Empire
LG Optimus F7*	D710 (Sprint)	LG Tribute HD*	LG Tribute HD
LG Optimus L4 II*	L4 II (Unlocked USA)	LG Tribute Monarch*	LG Tribute Monarch
LG Optimus L5 II*	L5 II (Unlocked USA)	LG Tribute Royal*	LG Tribute Royal

Product	Model Nos.	Product	Model Nos.
LG Optimus Zone*	VS410PP (Verizon Prepaid)	Asus ZenFone 7 Pro*	ASUS_I002D
LG Q6*	LG Q6	Asus ZenFone 8*	ZS50D
LG Q60*	LM-Q620 (Unlocked)	Asus ZenFone 8 Flip*	ZS672KS
LG Q7*	LG Q7	Asus Zenfone 9*	ZS670KS
LG Q7+*	LG Q7+	Blackview BV5100*	Blackview BV5100
LG Q70*	LM-Q730 (Unlocked)	Blackview BV5200*	Blackview BV5200
LG Q8*	V34 (AT&T)	Blackview BV5300 Pro*	Blackview BV5300 Pro
LG Stylo 2 Plus*	K550 (T-Mobile)	Huawei Mate 20*	HMA-L29
LG Stylo 2 V*	VS880 (Verizon)	Huawei Mate 20 Pro*	LYA-L29
LG Stylo 3*	K550 (T-Mobile)	Huawei P30 Pro*	ELE-L29
LG Stylo 3 Plus*	LG Stylo 3 Plus	Huawei P9 Plus*	VIE-L09
LG Stylo 4*	LM-Q710 (T-Mobile)	LG G7 ThinQ*	LG-G710
LG Stylo 5*	LM-Q710 (T-Mobile)	LG Velvet*	LM-G900
LG Stylo 5+*	LM-Q710 (T-Mobile)	LG Wing*	LM-F100N
LG Stylo 6*	LM-Q730 (T-Mobile)	Motorola Moto G5 Plus*	XT1687
LG Stylus 2*	K520 (T-Mobile)	Motorola Moto G6 Play*	XT1922-4
LG Stylus 2 Plus*	K535 (T-Mobile)	Motorola Moto Z Droid Edition*	XT1650-03
LG Tribute 2*	LS665 (Boost Mobile)	Motorola Moto Z Force Droid Edition*	XT1650-05
LG Tribute 5*	LG Tribute 5	Motorola Moto Z Play*	XT1635-03
LG Tribute Dynasty*	LG Tribute Dynasty		

*Accused to the extent that Google has induced or contributed to third parties’ use of such devices to practice the accused methods.

II. Accused Smartwatches and Trackers

The accused smartwatches include all variations (e.g., all sizes, all colors, and connectivities) of Google Pixel Watch and Fitbit-branded smartwatches and trackers, and all variations (e.g., all sizes, all colors, and connectivities) of other smartwatches and trackers with Wear OS 2.0 or later.⁸

Product	Model No.	Product	Model No.
Google Pixel Watch 3	GA05758-US, GA05786-US	Fitbit Versa 3*	FB511GLNV
Google Pixel Watch 2	G4TSL, GC3G8, GD2WG	Fitbit Versa 2*	FB507RGRW
Google Pixel Watch	GQF4C, GBZ4S, GWT9R	Fitbit Versa Special Edition (containing NFC chip)*	FB505BKGY
Fitbit Ace LTE	Ace LTE	Fitbit Charge 6	GA05185, GA05195
Fitbit Sense 2	FB521BKGB	Fitbit Charge 5*	FB421BKBK
Fitbit Sense*	FB512GLWT	Fitbit Charge 4*	FB417BKBK
Fitbit Versa 4	FB523BKBK	Fitbit Charge 3 Special Edition (containing NFC chip)*	FB409GMBK
Samsung Galaxy Watch 4*	SM-R860NZDAXAA	Samsung Galaxy Watch 4 Classic*	SM-R890NZKCXAA
Samsung Galaxy Watch 5*	SM-R910NZAAXAA, SM-R915UZAAXAA	Samsung Galaxy Watch 5 Pro*	Galaxy Watch 5 Pro
Samsung Galaxy Watch 6*	SM-R940NZKAXAA, SM-R930NZKAXAA	Samsung Galaxy Watch 6 Classic*	SM-R960NZKAXAA
Samsung Galaxy Watch 7*	SM-L310F, SM-L315F, SM-L300NZEAXAA, SM-L310NZSAXAA	Samsung Galaxy Watch Ultra*	L705U, SM-L705FDAAMXO
Samsung Galaxy Watch FE*	SM-R861NZKAXAA, SM-R861NIDAXAA	Mobvoi TicWatch Atlas*	TicWatch Atlas
OnePlus Watch 2R*	OnePlus Watch 2R	Mobvoi TicWatch Pro 5 Enduro*	TicWatch Pro 5 Enduro, WH12088
Citizen CZ Smart PQ2*	JX2005-55E	Mobvoi TicWatch Pro 5*	TicWatch Pro 5
OnePlus Watch 2*	OnePlus Watch 2	Oppo Watch X*	OWWE231
Xiaomi Watch 2*	M2320W1	Xiaomi Watch 2 Pro*	M2233W1
TAG Heuer Connected Calibre*	SBR8010.BT6255	Diesel Griffed*	DZT2040V
Montblanc Summit 3*	Montblanc Summit 3	Fossil Q Explorist HR*	FTW4018
Fossil Q Venture HR*	FTW6015	Fossil Q Sport*	FTW4063V
Fossil Q The Carlyle HR*	FTW4026	Fossil Q Julianna HR*	FTW6036
Fossil Garrett HR*	FTW4041	Fossil HR*	FTW7056
Huawei Watch 2*	VID-B19	Huawei Watch 2 Classic*	Huawei Watch 2 Classic
Kate Spade Scallop Smartwatch 2*	KST2009	LG Watch Urbane*	MD05196020

⁸ See, e.g., *Tap to pay with your smartwatch*, Wear OS by Google Help, <https://support.google.com/wearos/answer/12059876>; *Tap to pay with your Fitbit device*, Google Wallet Help, <https://support.google.com/wallet/answer/12967766> (last visited Nov. 5, 2024).

Product	Model No.	Product	Model No.
LG Watch Sport*	W280A	Louis Vuitton Tambour Horizon*	Louis Vuitton Tambour Horizon
Michael Kors Runway*	MK9073	Misfit Vapor 2*	Misfit Vapor 2
Misfit Vapor X*	Misfit Vapor X	Mobvoi TicWatch Pro*	TicWatch Pro
Mobvoi TicWatch Pro 4G*	WF11018	Mobvoi TicWatch Pro 2020*	TicWatch Pro 2020
Mobvoi TicWatch C2*	TicWatch C2 20mm, TicWatch C2 18mm	Mobvoi TicWatch Pro 3*	Pro 3 Ultra GPS
Mobvoi TicWatch E3*	TicWatch E3	Motorola 360*	M360FS19-RG
Oppo Watch LTE*	Oppo Watch LTE	Oppo Watch Wi-fi*	Oppo Watch Wi-fi
Oppo Watch 2*	Oppo Watch 2	Oppo Watch 3*	Oppo Watch 3
Oppo Watch 3 Pro*	Oppo Watch 3 Pro	Skagen Falster 2*	Skagen Falster 2
Skager Falster 3*	Skager Falster 3	Skagen Flaster 6*	Skagen Flaster 6
Sony Smartwatch 3*	Sony Smartwatch 3	Suunto 7*	SS050568000
TAG Heuer Connected E4*	SBR8A10.BA0616	Xiaomi Mi Watch*	XMWT06
Michael Kors Access Gen 6 Bradshaw*	Michael Kors Access Gen 6 Bradshaw	Fossil Men’s Gen 6*	FTW4061V

*Accused to the extent that Google has induced or contributed to third parties’ use of such devices to practice the accused methods.

III. Accused Tablets

The accused tablets include all variations (e.g., all sizes, all colors, all storage capacities, and connectivities) of the Google Pixel Tablet, and all variations (e.g., all sizes, all colors, all storage capacities, and connectivities) of other tablets that run on an Android operating system.⁹

Product	Model No.	Product	Model No.
Pixel Tablet	G-2PW4100 / G-2PW4200	Google Nexus 7*	ASUS-1A005A
Samsung Galaxy Tab Active 5*	SM-X306B / SM-X300	Google Nexus 10*	P8110
Samsung Galaxy Tab Active 4 Pro*	SM-T630N / SM-T636	Google Nexus 7 (2013)*	ME571KL
Samsung Galaxy Tab Active 3*	SM-T210 / T211 / T217A	Google Nexus 9 (2014)*	0P82100-16-BLK
Samsung Galaxy Tab Active Pro*	SM-T545	Google Nexus 10 (2013)*	GT-P8110
Samsung Galaxy Tab Active 2*	SM-T395	Lenovo Tab P12*	TB370FU
Samsung Galaxy Tab Active*	SM-T360	Lenovo Tab M9*	ZAC30056US
Samsung Galaxy Tab S9 FE*	SM-X510 / SM-X516	Lenovo Tab K11 LTE*	ZADK00
Samsung Galaxy Tab S6*	SM-T860 / SM-T865	Lenovo Tab M10 Plus*	TB-X606 / TB-X606F/ TB-X606X / TB-X606V
Samsung Galaxy Tab S5E*	SM-T720 / SM-T725	Lenovo Tab M8 Gen 4*	ZABW0030JP / ZABX0031JP

⁹ See, e.g., *Google Pixel Tablet technical specifications*, Google Pixel Tablet Help, <https://support.google.com/googlepixelttablet/answer/13555146?hl=en>.

Product	Model No.	Product	Model No.
Samsung Galaxy Tab S4*	SM-T830 / SM-T835	Lenovo Yoga Smart Tab*	YT-X705F / YT-X705L / YT-X705X
Samsung Galaxy Tab A*	SM-P205	Lenovo Tab M7*	TB-7305X / TB-7305I / TB-7305F
Samsung Galaxy Tab S3*	SM-T820 / SM-T825	Lenovo Tab V7*	PB-6505M / PB-6505MC
Samsung Galaxy Note*	SGH-I717	Huawei MediaPad M6 8.4*	VRD-AL09
Lenovo Yoga Tab 11*	ZA8W0084US	Huawei MediaPad M5 Lite 8.0*	JDN2-AL00
Lenovo Tab Plus*	TB351FU	Huawei MediaPad M5 8.0*	SHT-AL09
Lenovo Tab M11*	TB330FU / TB330XU	Huawei MediaPad M5 10*	CMR-AL09
Alcatel 3T 10*	8088X / 8088Q	Huawei MediaPad T3 10*	AGS2-L09
Huawei MediaPad M6 10.8*	SCM-AL09 / SCM-W09	LG G Pad 5	LM-T600L / T600L
Huawei Honor Tab 5*	JDN2-W09HN	Acer Enduro*	ET110-31W-C2KN
Hyundai Hytab Plus 8*	HT8WB3RBK01	Hyundai Hytab Plus 10*	HT10WB1MSG
ZTE Grand X View*	ZTE Grand X View	Alcatel Joy Tab*	9029Z

*Accused to the extent that Google has induced or contributed to third parties’ use of such devices to practice the accused methods.

IV. Accused Chromebooks

The accused Chromebooks include all variations (e.g., all sizes, all colors, all storage capacities, and connectivities) of the Google Chromebook with touchscreen capability.

Product	Model No.	Product	Model No.
Acer Chromebook Plus 514	NX.KV0AA.002, NX.KQ2AA.001	Acer Chromebook Spin 312	NX.J0PAA.001
Acer Chromebook Spin 514	NX.KB2AA.001	Asus ExpertBook	CX5403
Asus Chromebook Plus	CX3402	Asus Chromebook Flip	CM1402F
Asus Chromebook Flip	CX1400	HP Chromebook	X360
HP Chromebook	5A959UA#ABA	HP Elite	5Z8L4AV_MB
HP Elite Dragonfly	A4EC9UT#ABA, A4ED0UT#ABA, A4ED1UT#ABA, A4ED2UT#ABA	Lenovo Chromebook Duet Gen 9	83HH0002US, 83HH0000US, 83HH0001US
Lenovo 3i Chromebook	82N40045US, 82N4004EUS, 83BN001AUS	Lenovo ThinkPad C14	21CAS19500
Lenovo Chromebook Duet 3	82T6003HUS, 82T6000EUS, 82QS001HUS	Lenovo IdeaPad	83EK0000UX, 83BN001AUS, 82XJ0000US
Samsung Galaxy Chromebook	XE550XGAA, XE550XGA-KC1US	Dell Chromebook	3310
Dell Chromebook 2-in-1	3310 2-in-1	Dell Chromebook 2-in-1	3120 2-in-1