

Exhibit D to CardWare’s Preliminary Infringement Contentions
Infringement of U.S. Patent No. 11,620,634

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

Google infringed and continues to infringe U.S. Patent No. 11,620,634 (the “’634 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 payment transaction, covered by one or more claims of the ’634 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 ’634 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.

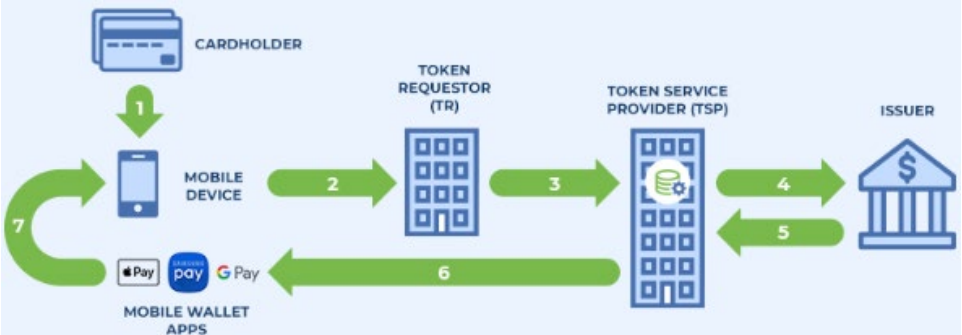
I. Claim 1 and Dependent Claims 2–13, 15–28

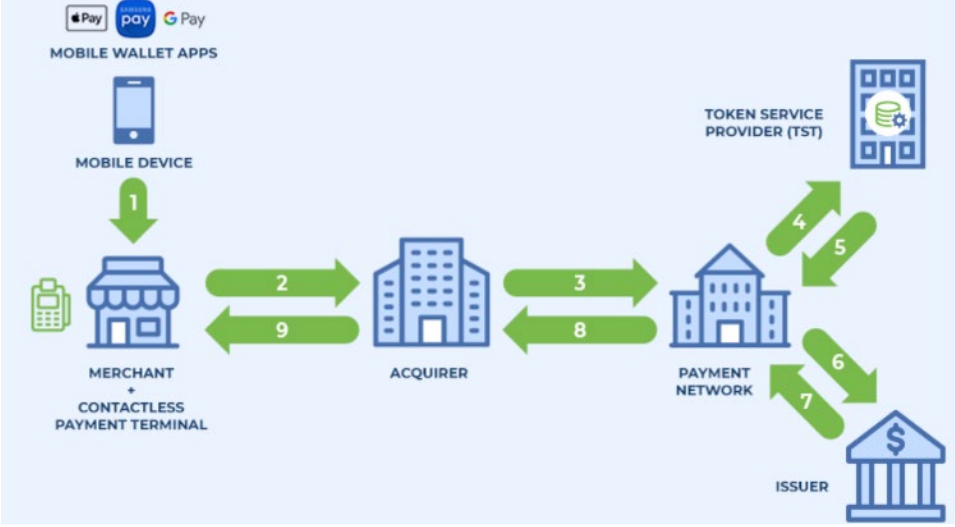
Claim No.	Accused Products
<p>1[pre]: A method of generating and using limited-use payment information for performing a payment transaction, the method comprising:</p>	<p>To the extent the preamble is limiting, a Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone or smartwatch, practices a method of generating and using limited-use payment information (e.g., a payment cryptogram /transaction cryptogram/ application cryptogram/ token cryptogram/ dynamic cryptogram (hereinafter “dynamic cryptogram”), or any combination including the same) for performing a payment transaction.</p> <div data-bbox="443 396 795 1024">  </div> <div data-bbox="800 618 1220 1024">  </div> <div data-bbox="1224 626 1421 667"> <h3>Takeaways</h3> </div> <div data-bbox="1251 704 1713 1019"> <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 free ¹ 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 data-bbox="447 1032 924 1081"> <h3>Get help paying the tab</h3> </div> <div data-bbox="1377 1057 1440 1089"> <p>[. . .]</p> </div> <div data-bbox="447 1089 1356 1166" style="border: 2px solid red; padding: 5px;"> <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> </div> <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>Google Pay – Pay In Store</i>, Google, https://pay.google.com/about/pay-in-store/ (“Your phone is now your wallet—just unlock, tap, and look for the check mark.”); <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>

Claim No.	Accused Products
	<div data-bbox="445 196 919 792">  </div> <p data-bbox="926 630 1871 792">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> <p data-bbox="445 797 1997 927">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-govogle-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> <p data-bbox="445 967 1438 1019">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="445 1049 913 1073">Highlights of Google Pay’s security features include:</p> <ul data-bbox="478 1101 1491 1287" 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="445 1292 1896 1390">See, e.g., <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 – 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>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)

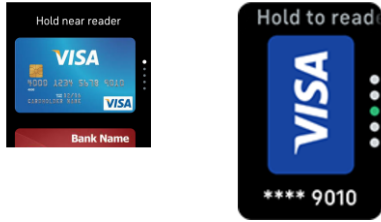
Claim No.	Accused Products
	<p>^a ID&V methods includes text or email or call. OTP is an example. ^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.</p> <p>Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet</p> <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</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>

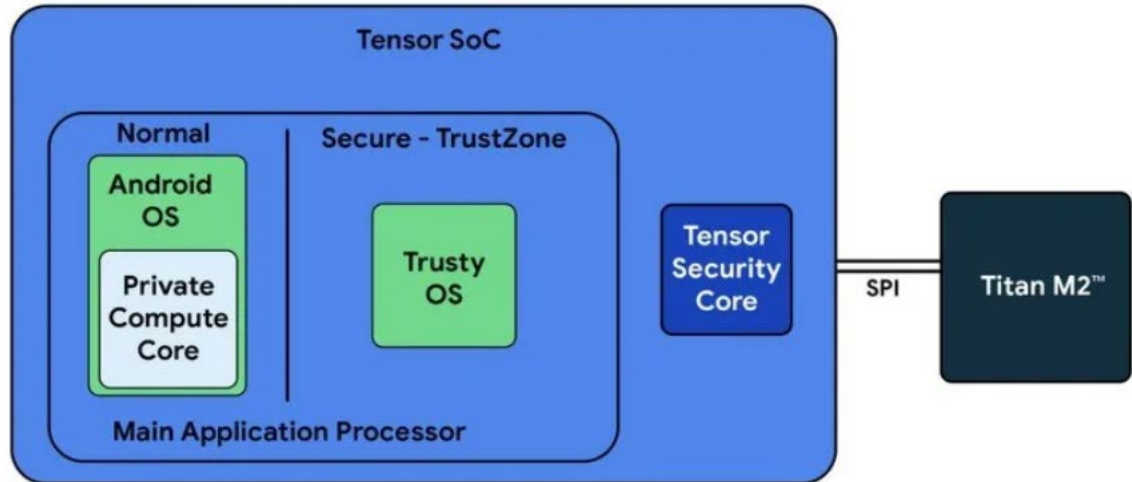
Claim No.	Accused Products
	<p>In general terms, the process for registering a card in a mobile wallet is as follows: [. . .]</p> <ol style="list-style-type: none"> If everything is correct, the TSP registers the PAN and links it to a new token in a secure database (<i>Token Vault</i>). Along with the 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. The TSP notifies the application of the newly generated token. 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"> 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. [. . .]

Claim No.	Accused Products
	 <p><i>See, e.g., Mobile payments with digital wallets and tokenization: How Apple Pay, Google 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-apple-pay-google-pay-samsung-pay-protect-your-card-details (captured May 9, 2024).</p> <p>In addition, Google has induced and/or contributed to third parties’ manufacture, use, sale, offer for sale, and importation of devices that 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 for Developers, Google Wallet API tutorial for Google Developers Google I/O 2022</i>, YouTube (May 11, 2022), https://www.youtube.com/watch?v=2gTCghy-dU4 at 1:25 (Last visited December 4, 2024).</p> <p>In yet another example, the new Motorola Razr Plus 2024, which runs on Android 14, comes with Google Wallet pre-installed on the device. <i>See, e.g., WorldofTech, Motorola RAZR Plus: How to Setup (step by step)</i>, YouTube (September 22, 2023), https://www.youtube.com/watch?v=hR2Zy0V8Oqw at 3:44 (last visited December 4, 2024).</p>

Claim No.	Accused Products
<p>1[a]: receiving an input at an electronic device, wherein the input comprises a priming operation, 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 wherein the input comprises a priming operation (<i>e.g.</i>, double pressing the digital crown, entering a PIN, pattern, using fingerprint, face unlock, etc.).</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> <div data-bbox="443 516 837 690" style="border: 2px solid red; padding: 5px;"> <ul style="list-style-type: none"> • PIN • Pattern • Password • Class 3 biometric unlock </div> <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> <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><i>See, e.g., Android 15 Compatibility Definition</i>, https://source.android.com/docs/compatibility/15/android-15-cdd.</p>

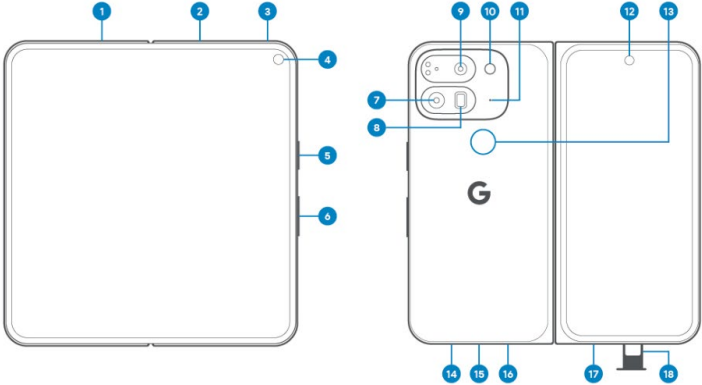
Claim No.	Accused Products
	<p>BIOMETRIC_STRONG Added in API level 30</p> <div> <pre>public static final int BIOMETRIC_STRONG</pre> </div> <p>Any biometric (e.g. fingerprint, iris, or face) on the device that meets or exceeds the requirements for Class 3 (formerly Strong), as defined by the Android CDD.</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>  <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? Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</i></p>				
1[b]: wherein the electronic device comprises:	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, is an electronic device.</p> <p><i>See supra</i> limitation 1[pre].</p>				
1[c]: a processor;	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (e.g., system processor, or system coprocessor, or processor of secure element, or processor of SIM/eSIM, or any combination of the same).</p> <div data-bbox="438 946 1549 1219"> <p>Pixel 9 Pro Fold</p> <p>Pixel 9 Pro Fold (2024)</p> <table border="1"> <tr> <td>Processor</td> <td> <ul style="list-style-type: none"> Google Tensor G4 Titan M2™ security coprocessor </td> </tr> <tr> <td>SIMs</td> <td> <ul style="list-style-type: none"> Dual SIM (Single Nano SIM and eSIM)²³ </td> </tr> </table> </div> <p><i>See, e.g., Pixel phone hardware tech specs, Pixel Phone Help, https://support.google.com/pixelphone/answer/7158570.</i></p>	Processor	<ul style="list-style-type: none"> Google Tensor G4 Titan M2™ security coprocessor 	SIMs	<ul style="list-style-type: none"> Dual SIM (Single Nano SIM and eSIM)²³
Processor	<ul style="list-style-type: none"> Google Tensor G4 Titan M2™ security coprocessor 				
SIMs	<ul style="list-style-type: none"> Dual SIM (Single Nano SIM and eSIM)²³ 				

Claim No.	Accused Products		
	<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> <div></div> <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> <div><p>Google Pixel Watch 3 Specifications</p><table><tr><th>Chip</th><td><ul style="list-style-type: none">Qualcomm Snapdragon W5 Gen 1Cortex M33 co-processor</td></tr></table><p>See, e.g., <i>Google Pixel Watch Technical & Device Specifications</i>, Google Pixel Watch Help, https://support.google.com/googlepixelwatch/answer/12651869.</p><p>The Fitbit Sense 2 FB521 smartwatch and activity tracker is based on the Ambiq Micro programmable Apollo4 Plus SoC controller. The controller has a built-in one-core 96 -192 MHz ARM Cortex-M4 processor. The IC package measures 5 x 5 mm and has 146 connections.</p><p>See, e.g., <i>Deep Dive Teardown of the Fitbit Sense 2 FB521 Smartwatch</i>, https://www.techinsights.com/products/ddt-2210-813.</p></div>	Chip	<ul style="list-style-type: none">Qualcomm Snapdragon W5 Gen 1Cortex M33 co-processor
Chip	<ul style="list-style-type: none">Qualcomm Snapdragon W5 Gen 1Cortex M33 co-processor		

Claim No.	Accused Products																						
1[d]: a touch-screen display coupled to the processor; and	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a touch-screen display coupled to the processor.</p> <div> <div>Outer display touch panel</div> <div> <table> <tr> <th>Symptom</th><th>Potential root cause</th></tr> <tr> <td></td><td>Connectivity problem</td></tr> <tr> <td>T044: Multi-touch poor response</td><td></td></tr> <tr> <td>T045: Multi-touch no response</td><td></td></tr> <tr> <td>T046: Multi-touch erratic response</td><td></td></tr> <tr> <td></td><td>Touch screen Fingerprint sensor</td></tr> </table> </div> </div> <div> <div>Inner display touch panel</div> <div> <table> <tr> <th>Symptom</th><th>Potential root cause</th></tr> <tr> <td></td><td>Connectivity problem</td></tr> <tr> <td>T177: Inner display multi-touch poor response</td><td>Touch screen Fingerprint sensor</td></tr> <tr> <td>T178: Inner display multi-touch no response</td><td></td></tr> <tr> <td>T179: Inner display multi-touch erratic response</td><td>Module problem</td></tr> </table> </div> </div> <p>See, e.g., <i>Service repair manuals for Pixel devices</i>, Pixel 9 Pro Fold Repair Manual, https://storage.googleapis.com/support-kms-prod/cotCXgR6PJJ7HUt3HCJGSXMmIvCcOAnMRQ8x.</p> <div> <div>Pixel 9 Pro Fold</div> <div> <div>Pixel 9 Pro Fold (2024)</div> <div> <div>Display</div> <div> <div>External cover</div> <ul style="list-style-type: none"> • [US, SG]: 6.3-inch (160 mm) Actua display¹ • [ROW]: 160 mm Actua display¹ • 20:9 aspect ratio • 1080 x 2424 OLED at 422 PPI </div> <div>Internal folding</div> <ul style="list-style-type: none"> • [US]: 8-inch (204 mm) Super Actua Flex display¹ (LTPO) • [ROW]: 204 mm Super Actua Flex display¹ (LTPO) • 2076 x 2152 OLED at 373 PPI </div> </div> </div> <p>See, e.g., <i>Pixel phone hardware tech specs</i>, Pixel Phone Help, https://support.google.com/pixelphone/answer/7158570.</p> <div>Google Pixel Watch 3 Specifications</div>	Symptom	Potential root cause		Connectivity problem	T044: Multi-touch poor response		T045: Multi-touch no response		T046: Multi-touch erratic response			Touch screen Fingerprint sensor	Symptom	Potential root cause		Connectivity problem	T177: Inner display multi-touch poor response	Touch screen Fingerprint sensor	T178: Inner display multi-touch no response		T179: Inner display multi-touch erratic response	Module problem
Symptom	Potential root cause																						
	Connectivity problem																						
T044: Multi-touch poor response																							
T045: Multi-touch no response																							
T046: Multi-touch erratic response																							
	Touch screen Fingerprint sensor																						
Symptom	Potential root cause																						
	Connectivity problem																						
T177: Inner display multi-touch poor response	Touch screen Fingerprint sensor																						
T178: Inner display multi-touch no response																							
T179: Inner display multi-touch erratic response	Module problem																						

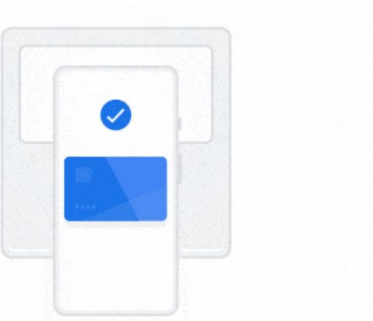
Claim No.	Accused Products
	<div data-bbox="447 191 1539 456"> <div data-bbox="447 191 758 456">Display</div> <div data-bbox="758 191 1539 456"> <ul style="list-style-type: none"> • Actua display • Custom 3D Corning® Gorilla® Glass 5 • 320 ppi AMOLED LTPO display with DCI-P3 color • Up to 2000 nits (peak brightness) • 1 nit minimum brightness • Responsive Display (1–60 Hz)⁶ • Always-on display </div> </div> <p data-bbox="447 456 2001 529">See, e.g., <i>Google Pixel Watch Technical & Device Specifications</i>, Google Pixel Watch Help, https://support.google.com/googlepixelwatch/answer/12651869.</p> <p data-bbox="447 565 2001 695">The Fitbit Sense 2 is a smartwatch compatible with iOS and Android and includes real-time heart rate monitor, steps, sleep and calories. It has a touchscreen display with 336 x 336 screen resolution. Has always-on display capability, on-screen battery indicator and a magnetic charging connector.</p> <p data-bbox="447 695 2001 768">See, e.g., <i>Consumer Reports, Smartwatches</i>, https://www.consumerreports.org/electronics-computers/smartwatch/fitbit-sense-2/m408200/ (Last visited December 3, 2024).</p>
<p data-bbox="96 797 436 935">1[e]: a near field communications (NFC) interface coupled to the processor;</p>	<p data-bbox="436 797 2001 870">A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a near field communications (NFC) interface (e.g., an NFC chip) coupled to the processor.</p> <p data-bbox="436 870 2001 935">Set up tap to pay</p> <ol data-bbox="436 935 2001 1073" style="list-style-type: none"> 1. Open the Google Wallet app 🇵🇸. 2. At the top right, tap your Profile picture or Account 👤 > Payment setup. 3. To make contactless payments, make sure to meet these requirements: <div data-bbox="447 1073 1066 1169"> <ul style="list-style-type: none"> • Turn NFC on your phone. • Set Google Pay as your default payment app. </div>

Claim No.	Accused Products
	<div>Pay in a store</div> <div> <div>Step 1: Wake up & unlock your phone</div> <div> <div>Important:</div> <div>For users with a Pixel 7 or Pixel 7 Pro, Face Unlock is currently not supported for tap to pay transactions. Consider adding an instruction to open the Wallet app first before the payment.</div> </div> <div> <div>Tips:</div> <div> <div>You don't need to open the Google Wallet app.</div> <div>For users with a Pixel 7 or Pixel 7 Pro, Face Unlock is currently not supported for tap to pay transactions.</div> <div>To use tap to pay on Pixel Fold or another foldable device, fold your device.</div> </div> </div> <div> <div>Step 2: Hold the back of your phone to the payment reader</div> <div> <div>Important:</div> <div>You need to verify the transaction with one of the supported Android screen lock methods.</div> </div> <div> <div>Step 3: If the payment is successful, a blue check mark will appear on the screen.</div> <div>See, e.g., Tap to pay with your phone, Google Wallet Help, https://support.google.com/wallet/answer/12060043 (last visited Jan. 7, 2025).</div> </div> <div> <div>Pixel 9 Pro Fold</div> <div> <div>To learn about the features of your Pixel 9 Pro Fold phone, refer to the diagram below:</div> <div> <div>  <div> <div>1. Top speaker</div> <div>2. mmWave antenna cover</div> <div>3. Top microphone</div> <div>4. Inner front-facing camera</div> <div>5. Power button/fingerprint sensor</div> <div>6. Volume up/down button</div> <div>7. Rear-facing camera: Ultrawide lens</div> <div>8. Rear-facing camera: 5x Telephoto lens</div> <div>9. Rear-facing camera: Wide lens</div> <div>10. LED flash</div> <div>11. Rear-facing microphone</div> <div>12. Outer front-facing camera</div> <div>13. NFC</div> </div> </div> </div> </div> <div>See, e.g., Pixel phone hardware diagram, Pixel Phone Help, https://support.google.com/pixelphone/answer/7157629.</div> </div></div></div>

Claim No.	Accused Products										
	<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> <p>Google Pixel Watch 3 Specifications ⬆ [...]</p> <table border="1"> <thead> <tr> <th>Connectivity</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>• 4G LTE and UMTS³</td> </tr> <tr> <td></td> <td>• Bluetooth® 5.3</td> </tr> <tr> <td></td> <td>• Wifi 802.11a/b/g/n/ac/ax 2.4Ghz, 5Ghz</td> </tr> <tr> <td></td> <td>• NFC</td> </tr> </tbody> </table> <p>See, e.g., <i>Google Pixel Watch Technical & Device Specifications</i>, Google Pixel Watch Help, https://support.google.com/googlepixelwatch/answer/12651869.</p> <p>The Versa 4 and Sense 2 also feature a Near Field Communication (NFC) radio for mobile payments via <u>Google Pay</u> (which recently replaced Fitbit Pay on these devices) as well as a built-in microphone and 75dB speaker for voice features like Amazon Alexa and on-wrist Bluetooth calls.</p> <p>See, e.g., Angela Moscaritolo, <i>Fitbit Versa 4 Review</i>, PC Magazine (Aug. 24, 2023), https://www.pcmag.com/reviews/fitbit-versa-4; <i>Fitbit Versa 4 Smartwatch – Tech Specs</i>, Google Store, https://store.google.com/product/fitbit_versa_4_specs?hl=en-US (last visited Nov. 6, 2024).</p>	Connectivity			• 4G LTE and UMTS ³		• Bluetooth® 5.3		• Wifi 802.11a/b/g/n/ac/ax 2.4Ghz, 5Ghz		• NFC
Connectivity											
	• 4G LTE and UMTS ³										
	• Bluetooth® 5.3										
	• Wifi 802.11a/b/g/n/ac/ax 2.4Ghz, 5Ghz										
	• NFC										

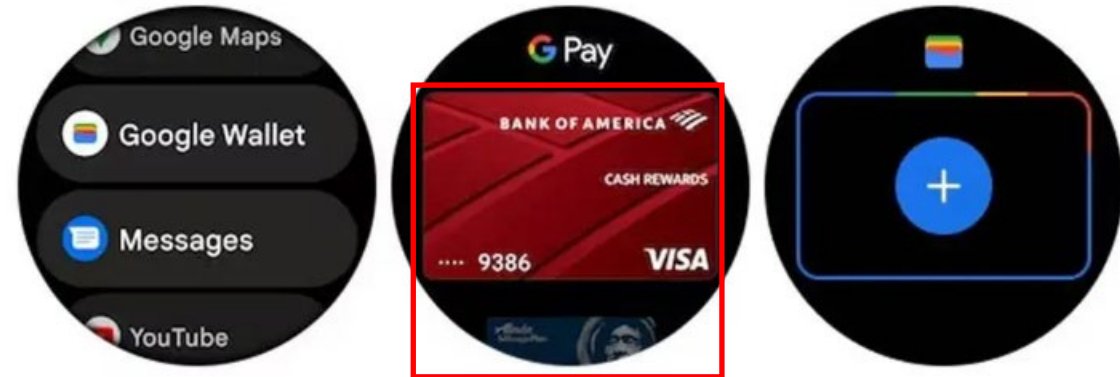
Claim No.	Accused Products
1[f]: responsive to said priming operation, readying said device to perform a payment transaction by an identified user;	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, responsive to said priming operation, readies to perform a payment transaction by an identified user (<i>e.g.</i>, user authenticates with double pressing the digital crown, entering a PIN, a pattern, using fingerprint, or face unlock).</p> <h3>Pay in a store</h3> <div>Step 1: Wake up & unlock your phone</div> <p>Important: For users with a Pixel 7 or Pixel 7 Pro, Face Unlock is currently not supported for tap to pay transactions. Consider adding an instruction to open the Wallet app first before the payment.</p> <p>Tips:</p> <ul style="list-style-type: none">• You don't need to open the Google Wallet app.• For users with a Pixel 7 or Pixel 7 Pro, Face Unlock is currently not supported for tap to pay transactions.• To use tap to pay on Pixel Fold or another foldable device, fold your device. <p><i>See, e.g., Tap to pay with your phone, Google Wallet Help, https://support.google.com/wallet/answer/12060043?hl=en.</i></p> <h3>Unlock your Android device to verify it's you</h3> <p>To help protect your account, we may ask you to verify it's you. You can easily verify it's you through simple ways that unlock your Android device.</p> <h3>Screen lock options</h3> <p>If you've set up a screen lock on your Android device, you can use it to verify it's you. Screen lock options include:</p> <div><ul style="list-style-type: none">• Pattern: Draw a simple pattern with your finger.• Pin: Enter 4 or more numbers.• Password: Enter a combination of 4 or more letters, numbers, or characters.• Fingerprint: Touch your finger to a sensor.</div> <p><i>See, e.g., Google Account Help, https://support.google.com/accounts/answer/9395014?hl=en.</i></p>

Claim No.	Accused Products
	<p>Google Pixel Watch - Unlock the Device</p> <p>1. From the watch screen, press the Crown button to open the apps screen.</p>  <p>2. Swipe up on the Home Screen.</p> <p>3. Do one of the following:</p> <ul style="list-style-type: none"> Enter the 4-digit PIN. Draw the unlock pattern. <p>See, e.g., Google Pixel Watch - Unlock the Device, https://www.verizon.com/support/knowledge-base-303380/ (Last visited December 4, 2024).</p> <p>Why should I use the device lock on my Fitbit device? ^</p> <p>To help keep your Fitbit device secure, turn on the device lock in the Fitbit app. You'll be prompted to enter a personal 4-digit PIN code to unlock your device. If you set up Google Wallet, the device lock is turned on automatically and you're prompted to set a code.</p> <p>See, e.g., How do I use the device lock on my Fitbit device? https://support.google.com/fitbit/answer/14236813 (Last visited December 4, 2024).</p>
I[g]: receiving a payment request for the payment transaction at said electronic device;	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch receives a payment request (e.g., from a user selecting a payment method or from the merchant payment terminal) for the payment transaction.

Claim No.	Accused Products
	<div data-bbox="445 191 1402 828">  </div> <div data-bbox="1411 506 1885 828"> <p>TAP TO PAY IN STORES</p> <h2>Pay with a tap at stores worldwide</h2> <p>Hold your Android device near the card reader and wait for the checkmark. Pay with your default card or select another. Google Pay will handle the rest.</p> </div> <p>See, e.g., <i>Google Pay – Pay In Store</i>, Google, https://pay.google.com/about/pay-in-store/.</p> <p>You can pay with Google Wallet wherever you find the contactless or Google Pay symbols on the payment terminal screen or cash register.</p> <div data-bbox="865 977 1234 1295">  </div> <ol style="list-style-type: none"> 1. Turn on your screen, then unlock your phone. You don’t need to open the Google Wallet app. 2. Hold the back of your phone to the payment reader. 3. If prompted for a PIN or signature, follow the on-screen instructions. <p>When you’re done paying, a blue check mark appears on the screen.</p>

Claim No.	Accused Products
	<p>See, e.g., <i>Set up tap to pay on your phone – 5. Pay in store</i>, Google Wallet Help, https://support.google.com/wallet/answer/14188457 (last visited Jan. 15, 2025).</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>

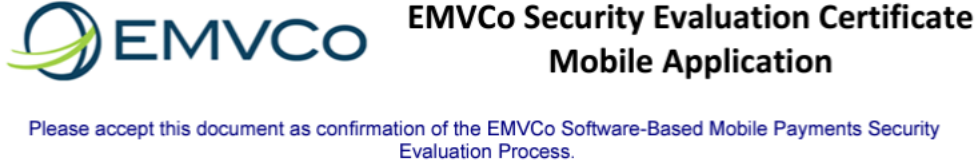
Claim No.	Accused Products
	<p>Make a payment in a store</p> <p>Important: For QUICPay and iD, you don't need to open the Google Wallet app to pay. Just hold your watch to the reader.</p> <ol style="list-style-type: none">1. Open the Google Wallet app 🇬🇧.2. Hold your watch over the contactless payment 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><i>See, e.g., Tap to pay with your smartwatch, Wear OS by Google Help, https://support.google.com/wallet/answer/12059876 (last visited Jan. 15, 2025).</i></p> <p>Pay with a different card</p> <p>You can tap and pay with other cards that aren't your default card.</p> <ol style="list-style-type: none">1. Open the Google Wallet app 🇬🇧.2. At the top, on your card, swipe from the right edge of the screen to left until you find the card that you want to use.3. Hold the back of your phone against the payment terminal.4. If prompted, choose “Credit,” no matter your type of card. <p><i>See, e.g., Change your default payment method in the Google Wallet app, Google Wallet Help, https://support.google.com/wallet/answer/12059255 (last visited Jan. 15, 2025).</i></p>

Claim No.	Accused Products
1[h]: displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account;	<p data-bbox="443 196 2003 326">A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, displays, on the touch-screen display, information reflecting the payment request (<i>e.g.</i>, NFC tap transaction screen with, <i>e.g.</i>, direction to “Hold to reader”), and an image representing a selected issued payment account (<i>e.g.</i>, a view of the default card or another user-selected payment method).</p>  <p data-bbox="443 867 1583 932"><i>See, e.g.</i>, Some Google Pixel phones can’t make contactless payments after March patch (Mar. 7, 2022), https://9to5google.com/2022/03/14/google-pixel-uncertified-contactless-pay/.</p>  <p data-bbox="443 1398 1688 1463"><i>See, e.g.</i>, 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>

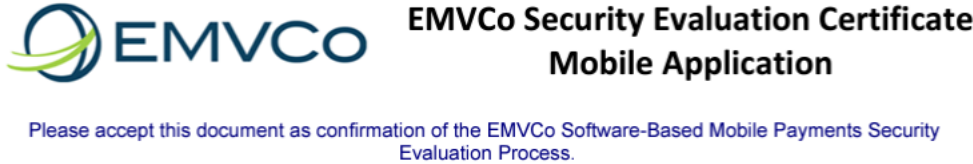
Claim No.	Accused Products
	
1[i]: dynamically generating, by the processor, limited-use payment information;	<p>See, e.g., <i>How to Use Google Wallet on Your Google Pixel Watch</i>, https://www.youtube.com/watch?v=Sa6ULG8MNUA.</p> <p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, dynamically generates by a processor (e.g., as identified above) of the device, limited-use payment information (e.g., as identified above).</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>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> <h2>5.0 Secure Limited-Use Key Storage</h2> <h3>5.1 Context</h3> <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> <h2>3. Tokenization Use Case Scenarios</h2> <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
	<div data-bbox="451 203 1507 365" style="border: 2px solid red; padding: 5px;"> <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.</p> </div> <p>See, e.g., EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).</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. <div data-bbox="451 836 1402 1388"> <p>The diagram illustrates the payment flow for mobile payments with digital wallets and tokenization. It shows the following components and steps:</p> <ul style="list-style-type: none"> MOBILE WALLET APPS (Apple Pay, Samsung Pay, Google Pay) on a MOBILE DEVICE. MERCHANT + CONTACTLESS PAYMENT TERMINAL. ACQUIRER. PAYMENT NETWORK. ISSUER. TOKEN SERVICE PROVIDER (TST). <p>The flow is numbered 1 through 9:</p> <ol style="list-style-type: none"> 1: Mobile Device to Merchant. 2: Merchant to Acquirer. 3: Acquirer to Payment Network. 4: Payment Network to TST. 5: TST to Issuer. 6: Issuer to Payment Network. 7: Payment Network to Acquirer. 8: Acquirer to Merchant. 9: Merchant to Mobile Device. </div> <p>[...]</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>

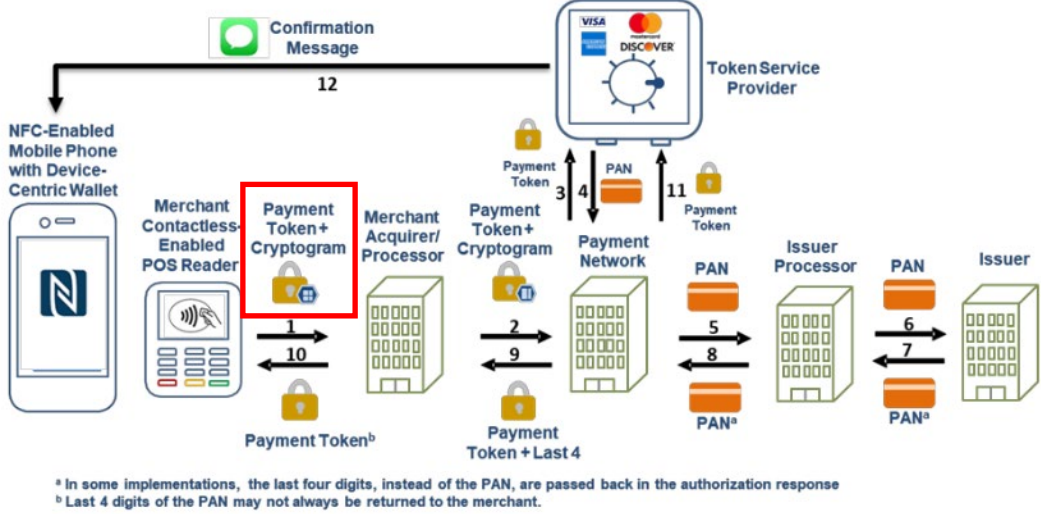
Claim No.	Accused Products
	 <p>Evaluation Certificate Number: SECN0069.03</p> <p>Date SECN Issued: 22 Apr 2021 Next security review due: 22 Apr 2025</p> <p>Company Name: Google, LLC Address: 1600 Amphitheatre Pkwy Mountain View, CA 94043 United States of America</p> <p>Product Name: Google Wallet</p> <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>1[j]: wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device;</p>	<p>A 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., as identified above) dynamically based on a per-transaction sequential parameter originating from the electronic device (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>

Claim No.	Accused Products			
	<div><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><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><h3>5.0 Secure Limited-Use Key Storage</h3><h4>5.1 Context</h4><table><tr><td>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).</td></tr></table><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></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.	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).
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.			
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).				

Claim No.	Accused Products
	<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>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>
1[k]: using said limited-use payment information in connection with the payment transaction in place of issued payment information associated with said selected issued payment account;	<p>An Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, uses said limited-use payment information (e.g., as identified above) in connection with the payment transaction in place of issued payment information (e.g., the primary account number (“PAN”) or associated expiration date or card verification value (“CVV”)) associated with said selected issued payment account (e.g., as identified above).</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>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>

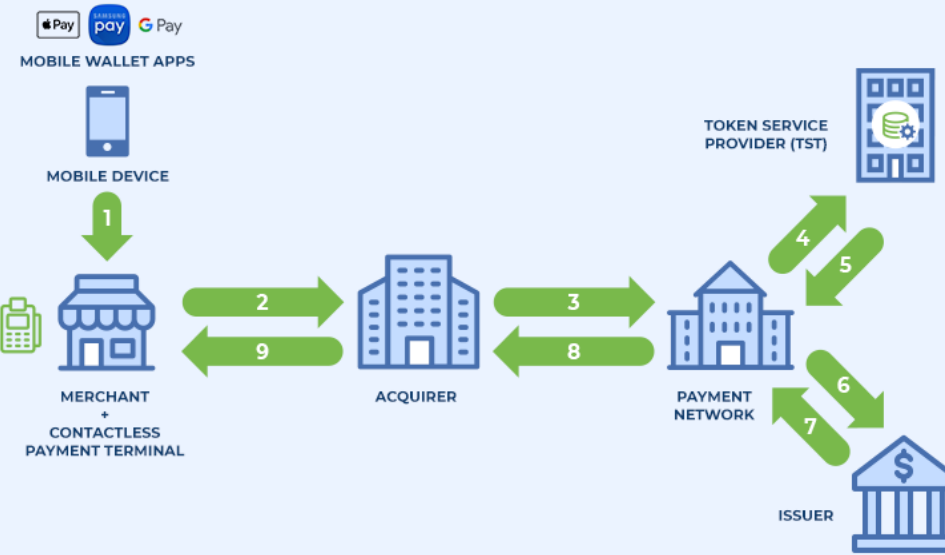
Claim No.	Accused Products
	<p>5.0 Secure Limited-Use Key Storage</p> <p>5.1 Context</p> <p>Conventional provisioning of credit card information to a device (whether tokenized or not) involves storing a Master Key on a trusted piece of hardware like a Secure Element. For the purpose of this document, 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.

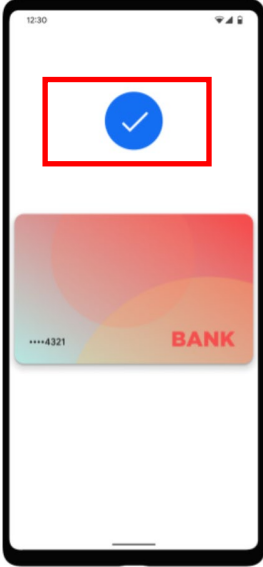
Claim No.	Accused Products
	<div data-bbox="447 191 1402 743"> <p>The diagram illustrates the EMV payment tokenization process. It shows a flow from a Mobile Device (with Mobile Wallet Apps like Apple Pay, Samsung Pay, and Google Pay) to a Merchant + Contactless Payment Terminal (Step 1). The Merchant then communicates with an Acquirer (Step 2). The Acquirer communicates with a Payment Network (Step 3). The Payment Network communicates with an Issuer (Step 4). The Issuer communicates with a Token Service Provider (TST) (Step 5). The TST communicates with the Payment Network (Step 6). The Payment Network communicates with the Acquirer (Step 7). The Acquirer communicates with the Merchant (Step 8). The Merchant communicates with the Mobile Device (Step 9).</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.</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)

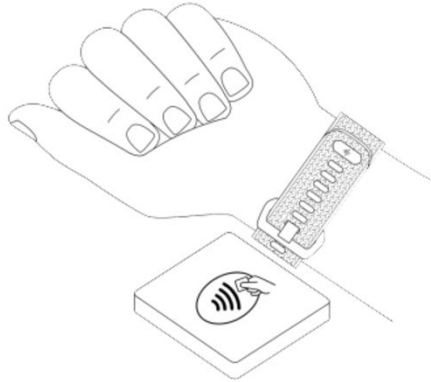
Claim No.	Accused Products
	 <p>Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at 24 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p>
<p>1[1]: transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient;</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, transmits said limited-use payment information (e.g., as identified above) from said electronic device via said NFC interface (e.g., as identified above) for receipt by an NFC recipient (e.g., a contactless reader).</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>

Claim No.	Accused Products
	<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><i>See, e.g., Tap to pay with your smartwatch, Google Wallet Help, https://support.google.com/wallet/answer/12059876.</i></p> <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? Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</i></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><i>See, e.g., Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions, https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf, pp. 14.</i></p>

Claim No.	Accused Products
	<div> <div> <div>5. End-to-End EMV Payment Tokenization Flows</div> <div> <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 EMV payment tokenization transaction. It starts with an 'NFC-Enabled Mobile Phone with Device-Centric Wallet' (labeled with an 'N' logo) interacting with a 'Merchant Contactless-Enabled POS Reader' (highlighted with a red box). The flow proceeds through a 'Merchant Acquirer/Processor' and a 'Payment Network' to a 'Token Service Provider' (VISA and DISCOVER logos) and finally to an 'Issuer'. The process involves the exchange of 'Payment Tokens', 'PANs' (Primary Account Numbers), and 'Cryptograms'. A 'Confirmation Message' is sent from the Token Service Provider back to the mobile phone. The diagram is divided into two main sections: 'Payment Token' and 'PAN'. The 'Payment Token' section shows the flow from the mobile phone to the merchant, then to the payment network, and finally to the token service provider. The 'PAN' section shows the flow from the payment network to the issuer, then back to the payment network, and finally to the token service provider. The diagram includes numbered steps (1-12) and labels for various components like 'Payment Token', 'PAN', 'Cryptogram', and 'Last 4'. A note at the bottom states: 'In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response. Last 4 digits of the PAN may not always be returned to the merchant.'</p> </div> </div> </div>

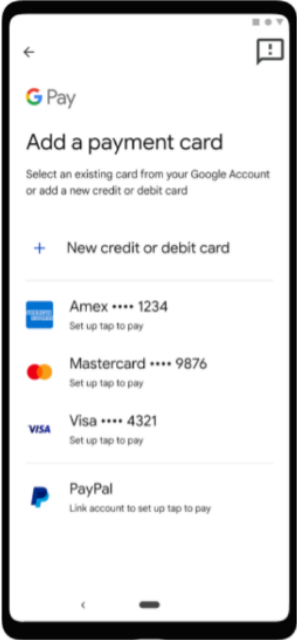
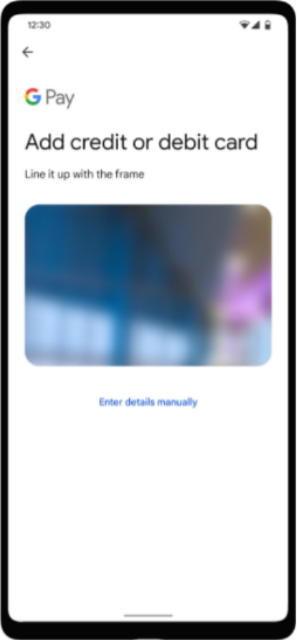
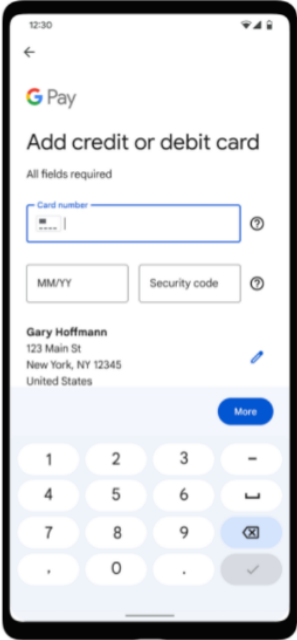
Claim No.	Accused Products
	<div data-bbox="453 201 1392 243" style="border: 2px solid red; padding: 2px;"> <p>2. The merchant sends the token and dynamic cryptogram data to the acquirer.</p> </div>  <p>The diagram illustrates a mobile payment transaction flow involving several entities: MOBILE WALLET APPS (Apple Pay, Android 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, Google 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-google-pay-samsung-pay-protect-your-card-details (captured May 9, 2024).</p>
<p>1[m]: responsive to the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction; and displaying the status of said payment transaction via said touch-screen display.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, responsive to the transmitting the limited-use payment information (e.g., as identified above), receives via the NFC interface information reflecting a status of said payment transaction (e.g., transaction confirmation); and displaying the status of said payment transaction via said touch-screen display (e.g., a blue tick, check mark, or transaction confirmation notification).</p>

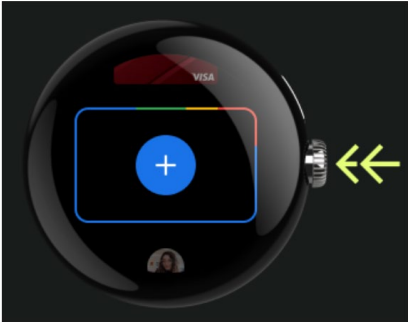
Claim No.	Accused Products
	<div><p>Step 2: Hold the back of your phone to the payment reader</p><p>When you're done paying, a blue tick will appear on the screen.</p><p>NFC Tap (success)</p><p>See, e.g., <i>Google Pay – Device Tokenization – TSP Integration – Google Pay Flows</i>, Google (May 2, 2024), 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>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, wherein the limited-use payment information comprises a cryptogram number.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, generates a limited-use information that includes a cryptogram number (e.g., dynamic cryptogram).</p> <p>See <i>supra</i> limitation 1[pre], 1[i].</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>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>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.		

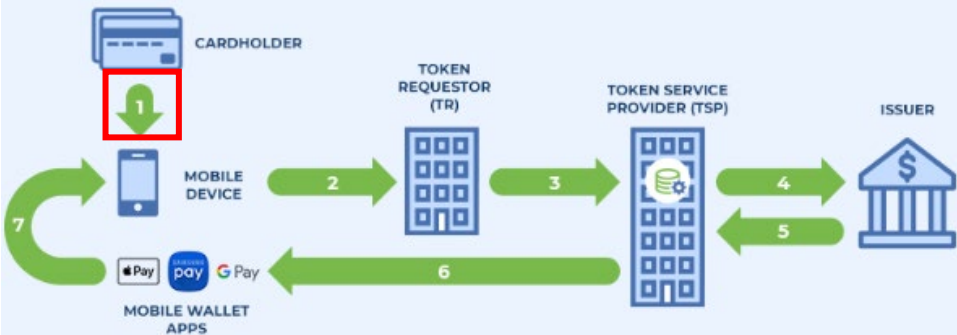
Claim No.	Accused Products
<p>3. The method of claim 2, further comprising: prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and, in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, prior to the priming operation, transmits the issued payment information (<i>e.g.</i>, as discussed above) for receipt by a payment processing authority; and, in response to said transmitting issued payment information, receives a static device account information (<i>e.g.</i>, a device-specific number/ “device token”/ payment token/ dynamic primary account number (“DPAN”) and associated expiration date and limited-use key(s)) that is unique to the electronic device.</p> <p>Add new card</p> <p>With the Google Wallet app </p> <ol style="list-style-type: none"> 1. Open the Google Wallet app . 2. At the bottom, tap Add to Wallet +. 3. Tap Payment card. <ul style="list-style-type: none"> • Any cards you saved to your Google Account are shown. 4. Tap New credit or debit card. <ul style="list-style-type: none"> • To add a card, use your camera or tap Enter details manually. 5. At the bottom, tap Save and continue. <p><i>See, e.g., Add a new debit or credit card, Google Wallet Help, https://support.google.com/wallet/answer/12058983; Make contactless payments with Google Pixel Watch, Google Pixel Watch Help, https://support.google.com/googlepixelwatch/answer/12661007.</i></p>

Claim No.	Accused Products
	<p>Key Google Pay UX flows</p> <p>Cards can be added to Google Pay either through Google Wallet surfaces or an issuer's mobile banking app using the Push Provisioning API. Google Wallet app surfaces let users to enter their card details in multiple ways, including autofilling the details using a card already stored on file, OCR scanning, and manual entry.</p> <div><div><p>Card on File</p></div><div><p>OCR Scanning</p></div><div><p>Manual entry</p></div></div> <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.</p>

Claim No.	Accused Products
	<div><div><div>Add a card to your Google Wallet</div><div></div><div>See, e.g., <i>Make contactless payments with Google Pixel Watch</i>, Google, https://support.google.com/googlepixelwatch/answer/12661007?hl=en.</div></div><div><div>Add a credit or debit card</div><div>If you add a card to your watch, you don't need your phone to pay.</div><div><div>1. On your smartwatch, open the Google Wallet app 🍌.</div><div>2. Tap Get started.</div><div>3. Set up screen lock if you haven't already.</div><div>4. On your phone, follow the instructions to add a Suica, credit, or debit card.</div></div><div><div>Tip:</div><div><div>• This only adds a card to the Google Wallet app on your watch, not your phone.</div></div></div></div></div>

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 User->>Google: User accepts Google Pay ToS Google->>TSP: checkEligibility() Google->>Issuer: checkEligibility() Issuer-->>TSP: Success TSP-->>Google: Success (card metadata, Issuer ToS, card art) Google->>User: Present issuer ToS User->>Google: ToS accpeted Google->>TSP: tokenize(risk signals, provisioning data) Google->>Issuer: tokenize(risk signals, provisioning data) Issuer-->>TSP: idvOutcome(approved, declined,challenge) TSP-->>Google: idvOutcome(approved, declined,challenge) Google->>User: idvOutcome(approved, declined,challenge) 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.</p>

Claim No.	Accused Products
	<p>What device tokens are</p> <p>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>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>See, e.g., Daniel Thomason, <i>How device tokens keep your payment cards safe in Google Wallet</i>, The Keyword (Jun. 27, 2024), https://blog.google/products/google-pay/device-tokens-google-wallet.</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>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>

Claim No.	Accused Products
	<p>In general terms, the process for registering a card in a mobile wallet is as follows:</p> <div data-bbox="447 261 1383 342" style="border: 2px solid red; padding: 5px;"> <p>1. The cardholder uses a device that supports the digital wallet application and registers a card, entering the data into the application.</p> </div> <p>2. The application sends the data to a <i>Token Requestor</i> (TR).</p> <p style="text-align: right;">[. . .]</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>4[a]: The method of claim 3 further comprising: combining said limited-use payment information and said static device account information, to reduce a combined payment information;</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, combines said limited-use payment information (e.g., as described above) and said static device account information (e.g., as described above), to produce a combined payment information.</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>

Claim No.	Accused Products
	<p>See, e.g., <i>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>See, e.g., <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 – Android (Oct. 28, 2024), https://developers.google.com/pay/api/android/guides/resources/payment-data-cryptography.</p> <div style="text-align: center;">  <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> </div> <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>

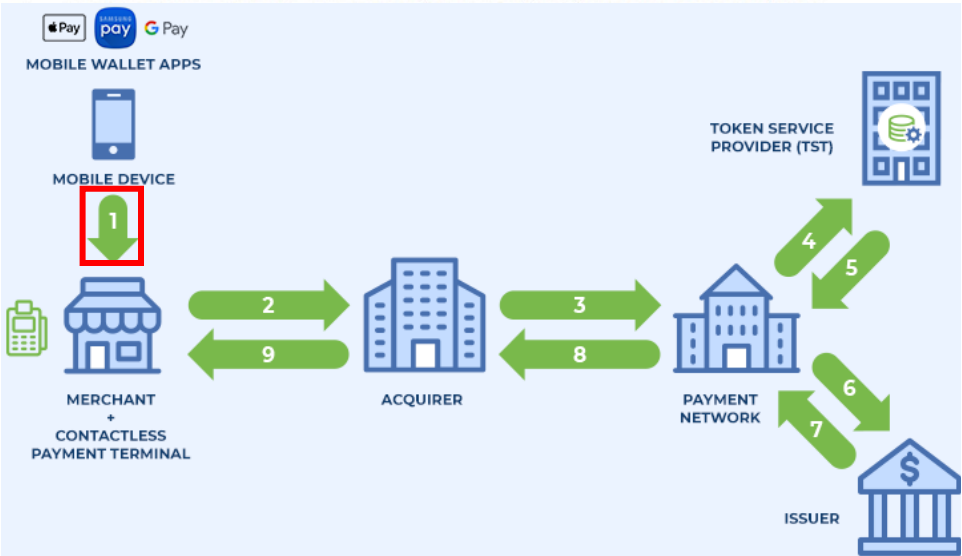
Claim No.	Accused Products
	<p>The original PAN of the card is never stored on the end user's device. Instead, the payment token with which subsequent transactions are made is securely stored. Let's walk through this:</p> <ol style="list-style-type: none"> The cardholder (in this case, the same user 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>  <p>The diagram illustrates the mobile payment process with digital wallets and tokenization. It shows the flow of data between a Mobile Device, Merchant, Acquirer, Payment Network, and Issuer, involving Mobile Wallet Apps, Token Service Provider (TST), and an Issuer.</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>2. The merchant sends the token and dynamic cryptogram data to the acquirer.</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>

Figure 6 illustrates the process of a contactless EMV transaction using an NFC-enabled device-centric digital wallet. The process involves the following steps:

- The NFC-enabled mobile phone sends a **Payment Token + Cryptogram** (1) to the **Merchant Contactless-Enabled POS Reader**.
- The **Merchant Contactless-Enabled POS Reader** sends a **Payment Token + Cryptogram** (2) to the **Payment Network**.
- The **Payment Network** sends a **Payment Token** (3) to the **Token Service Provider**.
- The **Token Service Provider** sends a **PAN** (4) to the **Payment Network**.
- The **Payment Network** sends a **PAN** (5) to the **Issuer Processor**.
- The **Issuer Processor** sends a **PAN** (6) to the **Issuer**.
- The **Issuer** sends a **PAN** (7) back to the **Issuer Processor**.
- The **Issuer Processor** sends a **PAN** (8) back to the **Payment Network**.
- The **Payment Network** sends a **Payment Token + Last 4** (9) back to the **Merchant Contactless-Enabled POS Reader**.
- The **Merchant Contactless-Enabled POS Reader** sends a **Payment Token** (10) back to the **NFC-Enabled Mobile Phone**.
- The **NFC-Enabled Mobile Phone** sends a **Confirmation Message** (12) to the **Token Service Provider**.

^a In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.
^b Last 4 digits of the PAN may not always be returned to the merchant.

Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

Figure 7 illustrates the process of an in-app transaction using a merchant mobile app with tokens provisioned in a device-centric wallet. The process involves the following steps:

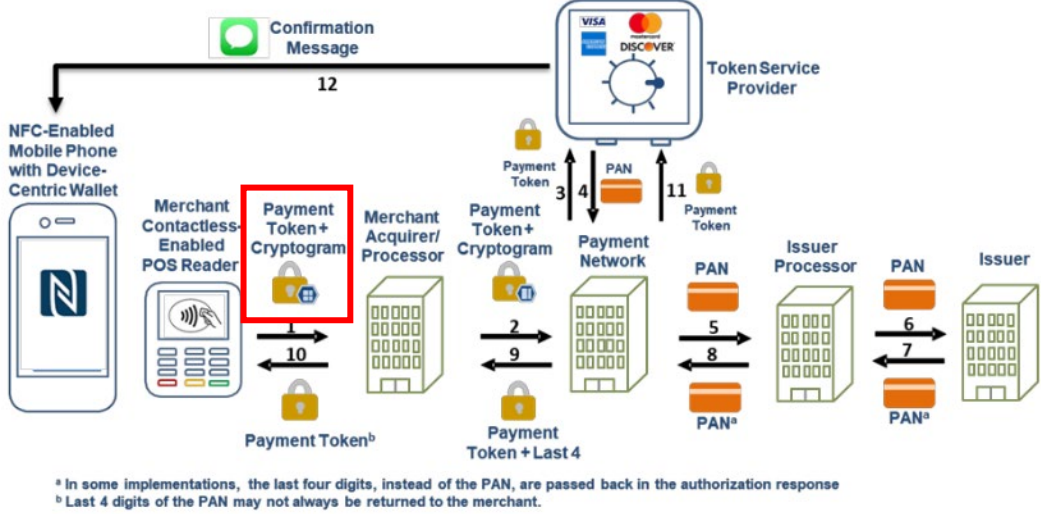
- The **Merchant Mobile App** sends a **Payment Token + Cryptogram** (1) to the **Merchant Acquirer/Processor**.
- The **Merchant Acquirer/Processor** sends a **Payment Token + Cryptogram** (2) to the **Payment Network**.
- The **Payment Network** sends a **Payment Token** (3) to the **Token Service Provider**.
- The **Token Service Provider** sends a **PAN** (4) to the **Payment Network**.
- The **Payment Network** sends a **PAN** (5) to the **Issuer Processor**.
- The **Issuer Processor** sends a **PAN** (6) to the **Issuer**.
- The **Issuer** sends a **PAN** (7) back to the **Issuer Processor**.
- The **Issuer Processor** sends a **PAN** (8) back to the **Payment Network**.
- The **Payment Network** sends a **Payment Token + Last 4** (9) back to the **Merchant Acquirer/Processor**.
- The **Merchant Acquirer/Processor** sends a **Confirmation Message** (10) back to the **Merchant Mobile App**.

^a Other TSP providers are also possible.
^b In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.
^c The payment network to which the transaction is routed may need to be the payment network that provided the token.

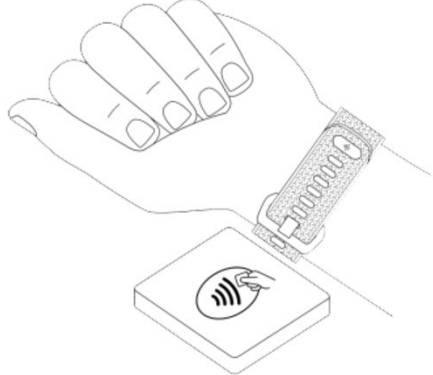
Figure 7. Processing an In-App Transaction Using a Merchant Mobile App with Tokens Provisioned in a Device-Centric Wallet

See, e.g., US Payments Forum, *EMV Payment Tokenization Primer and Lessons Learned* at 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>.

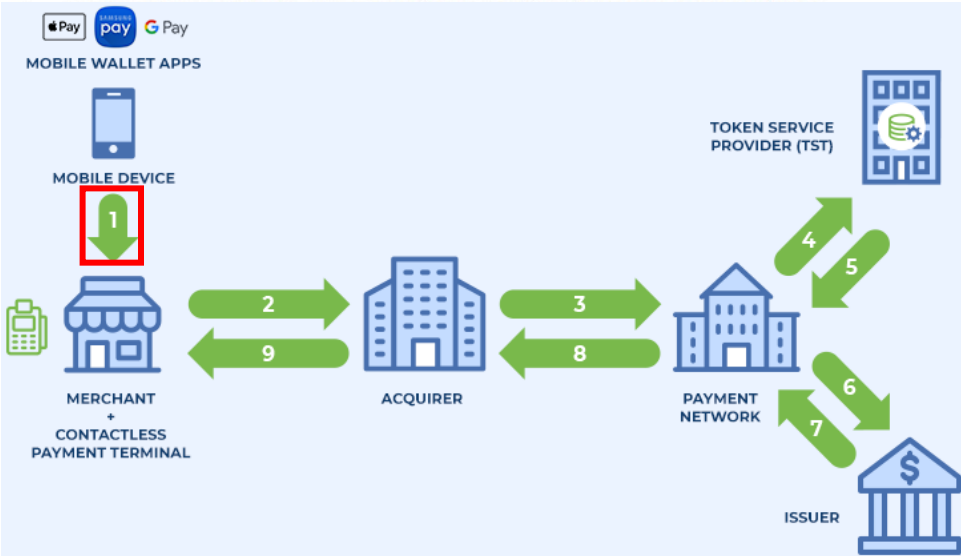
Claim No.	Accused Products
	<p>An HCE transaction takes place as follows:</p> <ol style="list-style-type: none"> 1. To initiate an HCE mobile payment, a customer taps the mobile phone at the POS contactless reader. 2. HCE enables the NFC controller in the mobile phone to route communications from the 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><i>See, e.g., Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions, https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf, pp. 14.</i></p>
<p>4[b]: transmitting said combined payment information, in place of the issued payment account information, via said NFC for receipt by an NFC recipient; and</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, transmits said combined payment information (e.g., a combination including the dynamic cryptogram or dynamic security code, or both, with the DPAN), in place of the issued payment account information (e.g., as identified above), via said NFC for receipt by an NFC recipient (as identified above).</p> <p><i>See supra</i> limitations 1[k], 1[l].</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><i>See, e.g., Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions, https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf, pp. 14.</i></p>

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>
4[c]: receiving, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, receive, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction (e.g., blue tick or transaction confirmation).</p> <p>See <i>supra</i> limitation 1[m].</p>

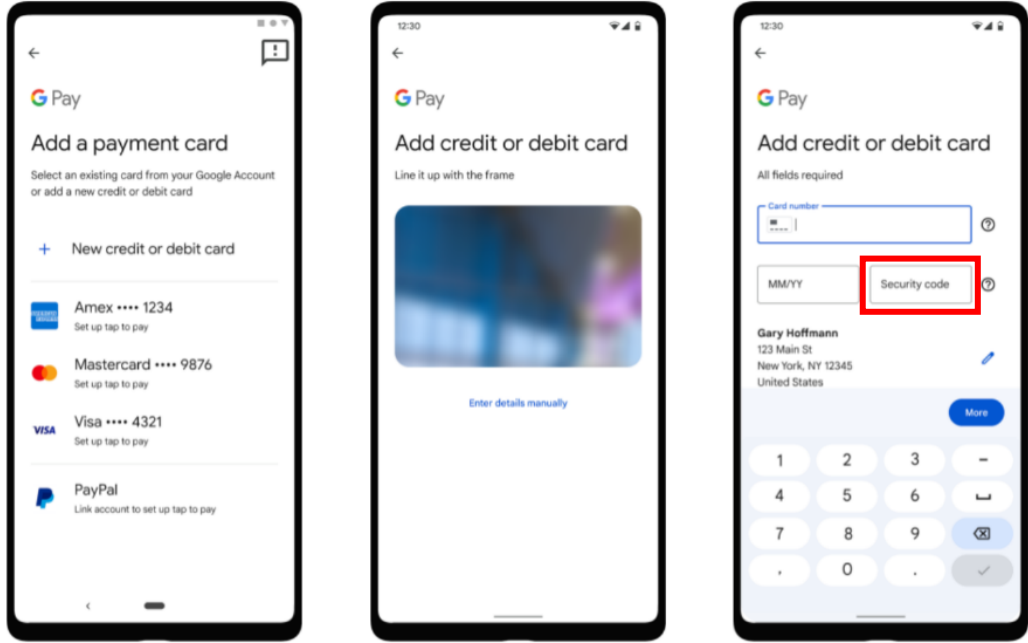
Claim No.	Accused Products
	<div><p>Step 2: Hold the back of your phone to the payment reader</p><p>When you're done paying, a blue tick will appear on the screen.</p><p>NFC Tap (success)</p><p>See, e.g., <i>Google Pay – Device Tokenization – TSP Integration – Google Pay Flows</i>, Google (May 2, 2024), 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>

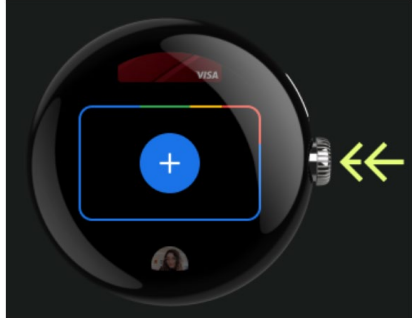
Claim No.	Accused Products
	 <p>When the payment succeeds, your device vibrates and you’ll receive a confirmation on the screen.</p> <p>See, e.g., <i>What should I know about using my Fitbit device to make contactless payments?</i> Google, https://support.google.com/fitbit/answer/14236521 (Last visited December 8, 2024).</p>
<p>5. The method of claim 3, wherein the dynamically generating Lather comprises dynamically generating the limited-use payment information based on payment processing authority secret information.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, dynamically generates the limited-use payment information (e.g., as identified above) further based on payment processing authority secret information (e.g., keys).</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>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)

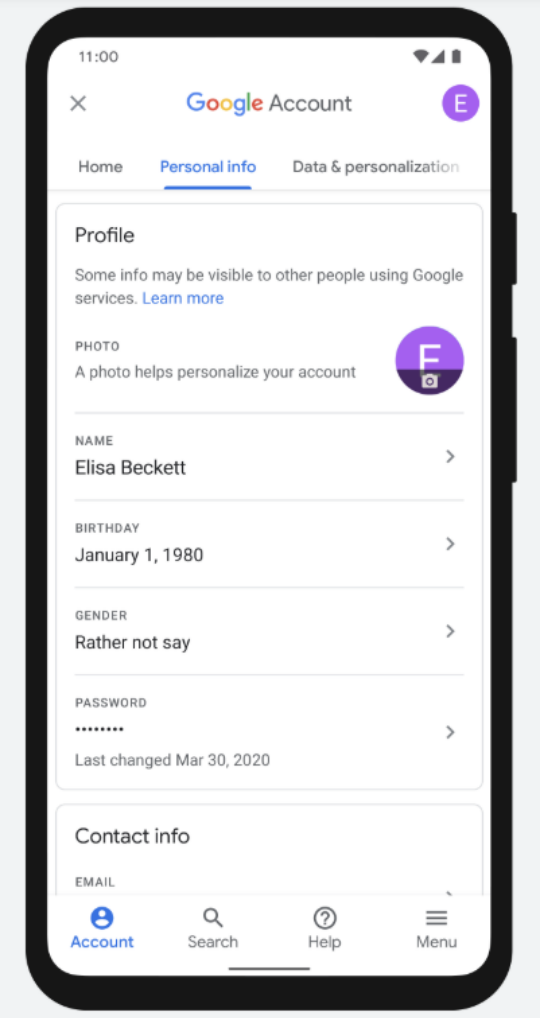
Claim No.	Accused Products			
	<p>See, e.g., US Payments Forum, <i>EMV Payment Tokenization Primer and Lessons Learned</i> at (June 2019 ver. 1.0) available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</p> <table><tr><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>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>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> <h2>5.0 Secure Limited-Use Key Storage</h2> <h3>5.1 Context</h3> <table><tr><td>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).</td></tr></table> <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>	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.	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).
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.			
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).				

Claim No.	Accused Products
	<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>  <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>

Claim No.	Accused Products
<p>6. The method of claim 5, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, bases the limited-use payment information (<i>e.g.</i>, as identified above) is based on at least one secret information (<i>e.g.</i>, keys) shared by both the electronic device and the payment processing authority (<i>e.g.</i>, on information and belief, device-specific information (<i>e.g.</i>, phone number, serial number, IMEI, etc.), issuer secrets, selected payment account information (<i>e.g.</i>, the DPAN, associated expiration date, or keys), or, user information (<i>e.g.</i>, name, phone number, password, email address)).</p> <p>5.0 Secure Limited-Use Key Storage</p> <p>5.1 Context</p> <div data-bbox="447 540 1392 675" style="border: 2px solid red; padding: 5px;"> <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> </div> <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><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>Add new card</p> <hr/> <p>With the Google Wallet app ^</p> <ol style="list-style-type: none"> 1. Open the Google Wallet app . 2. At the bottom, tap Add to Wallet . 3. Tap Payment card. <ul style="list-style-type: none"> • Any cards you saved to your Google Account are shown. 4. Tap New credit or debit card. <ul style="list-style-type: none"> • To add a card, use your camera or tap Enter details manually. 5. At the bottom, tap Save and continue.

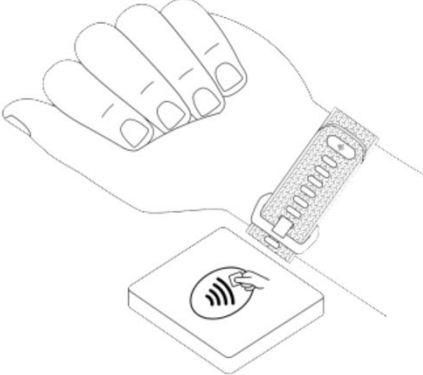
Claim No.	Accused Products
	<p>See, e.g., <i>Add a new debit or credit card</i>, Google Wallet Help, https://support.google.com/wallet/answer/12058983; <i>Make contactless payments with Google Pixel Watch</i>, Google Pixel Watch Help, https://support.google.com/googlepixelwatch/answer/12661007.</p> <p>Key Google Pay UX flows</p> <p>Cards can be added to Google Pay either through Google Wallet surfaces or an issuer's mobile banking app using the Push Provisioning API. Google Wallet app surfaces let users to enter their card details in multiple ways, including autofilling the details using a card already stored on file, OCR scanning, and manual entry.</p> <div>  <div> <div>Card on File</div> <div>OCR Scanning</div> <div>Manual entry</div> </div> </div> <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.</p>

Claim No.	Accused Products
	<p data-bbox="449 199 911 232">Add a card to your Google Wallet</p> <div data-bbox="449 245 858 561">  </div> <p data-bbox="926 245 1230 269">Add a credit or debit card</p> <p data-bbox="926 297 1545 321">If you add a card to your watch, you don't need your phone to pay.</p> <ol data-bbox="926 342 1646 472" style="list-style-type: none"> 1. On your smartwatch, open the Google Wallet app 🇵🇸. 2. Tap Get started. 3. Set up screen lock if you haven't already. 4. On your phone, follow the instructions to add a Suica, credit, or debit card. <p data-bbox="926 496 968 521">Tip:</p> <ul data-bbox="926 542 1675 566" style="list-style-type: none"> • This only adds a card to the Google Wallet app on your watch, not your phone. <p data-bbox="449 570 1919 626"><i>See, e.g., Make contactless payments with Google Pixel Watch, Google, https://support.google.com/googlepixelwatch/answer/12661007?hl=en.</i></p> <p data-bbox="449 667 1079 699">Add a Google or other account to your phone</p> <ol data-bbox="449 721 1331 1037" style="list-style-type: none"> 1. Open your device's Settings app. 2. Tap Passwords & accounts. 3. Under "Accounts," tap Add account. 4. Tap the type of account you want to add. <ul data-bbox="491 862 1331 1037" style="list-style-type: none"> • To add your Google Account, tap Google. When you sign in with a Google Account, the email, contacts, calendar events, and other data associated with that account automatically sync with your device. • To add your Google Meet account, tap Meet. When you sign in with your Meet account, you can make and receive video calls, create meetings, and call devices linked to your Home. <p data-bbox="449 1049 1835 1146"><i>See, e.g., Add or remove Google & other accounts on your Pixel phone, Pixel Phone Help, https://support.google.com/pixelphone/answer/2840815; Fix account and password issues for Pixel Watch, Google Pixel Watch Help, https://support.google.com/googlepixelwatch/answer/13579196.</i></p> <div data-bbox="449 1170 831 1232" style="border: 2px solid red; padding: 2px;"> <p data-bbox="464 1187 800 1211">Find your phone's IMEI numbers</p> </div> <p data-bbox="491 1252 858 1276">To find your phone's IMEI numbers:</p> <ul data-bbox="491 1300 894 1406" style="list-style-type: none"> • Check your phone's Settings app. <ol data-bbox="533 1341 894 1406" style="list-style-type: none"> 1. Tap About phone. 2. Scroll down until you find "IMEI."

Claim No.	Accused Products
	<div></div> <div><p>In your Watch settings</p><ol style="list-style-type: none">1. On Google Pixel Watch, swipe down > tap Settings ⚙️.2. Tap System > About.3. Swipe down to find your IMEI and serial numbers.</div> <p>See, e.g., Find your device serial number, Google Store Help, https://support.google.com/store/answer/3333000; Manage your Google Account, https://guidebooks.google.com/android/changesettingspermissions/manageyourgoogleaccountsettings.</p>

Claim No.	Accused Products
	<p>Add or switch accounts on your watch</p> <ol style="list-style-type: none"> 1. If you can't see your screen, wake up the watch. 2. To wake up your watch, from the watch face, slide down. 3. Tap Settings ⚙️ > Account and Backup > Google Account. <ul style="list-style-type: none"> • On Wear 2: Tap Settings ⚙️ > Personalization. • To add an account: Tap Accounts 👤 > Add Google Account. • To switch accounts: Tap Accounts 👤 and choose a different account. <p>Your watch uses the Google Account that you set up when you first connected your watch. You can have multiple Google accounts on both your watch and phone.</p> <p><i>See, e.g., Use Google Accounts on your watch, https://support.google.com/wearos/answer/7294653 (Last visited December 4, 2024).</i></p>
<p>7. The method of claim 1, wherein the priming operation comprises bringing the electronic device within receiving proximity of an NFC recipient.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch receives a priming operation comprising bringing the electronic device within receiving proximity of an NFC recipient (<i>e.g.</i>, “hold the back of your phone to the payment reader”).</p> <p><i>See supra</i> limitation 1[a].</p>

Claim No.	Accused Products
	<div data-bbox="449 199 709 764">  </div> <div data-bbox="726 699 1675 760" style="border: 2px solid red; padding: 5px;"> <p>Step 2: Hold the back of your phone to the payment reader</p> </div> <p data-bbox="491 800 667 824">NFC Tap (success)</p> <p data-bbox="730 776 1654 813">When you're done paying, a blue tick will appear on the screen.</p> <p data-bbox="443 862 1759 959">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="449 995 1018 1317">  </div> <p data-bbox="443 1325 1759 1422">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>8[a]: The method of claim 7, wherein said readying said device to perform a payment transaction comprises: identifying said proximity NFC recipient is an NFC payment facility;</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, on information and belief, readies said device to perform a payment transaction by identifying said proximity NFC recipient (e.g., as identified above) is an NFC payment facility.</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>
<p>8[b]: successfully validating the identified user as authorized to perform the payment</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, successfully validates the identified user as authorized to perform the payment transaction via said electronic device.</p> <p>See <i>supra</i> limitation 1[f].</p>

Claim No.	Accused Products
transaction via said electronic device; and	<p>Unlock your Android device to verify it's you</p> <p>To help protect your account, we may ask you to verify it's you. You can easily verify it's you through simple ways that unlock your Android device.</p> <p>Screen lock options</p> <p>If you've set up a screen lock on your Android device, you can use it to verify it's you. Screen lock options include:</p> <ul style="list-style-type: none">• Pattern: Draw a simple pattern with your finger.• Pin: Enter 4 or more numbers.• Password: Enter a combination of 4 or more letters, numbers, or characters.• Fingerprint: Touch your finger to a sensor. <p>See, e.g., <i>Google Account Help</i>, https://support.google.com/accounts/answer/9395014?hl=en.</p> <p>Google Pixel Watch - Unlock the Device</p> <p>1. From the watch screen, press the Crown button to open the apps screen.</p>  <p>2. Swipe up on the Home Screen.</p> <p>3. Do one of the following:</p> <ul style="list-style-type: none">• Enter the 4-digit PIN.• Draw the unlock pattern. <p>See, e.g., <i>Google Pixel Watch - Unlock the Device</i>, https://www.verizon.com/support/knowledge-base-303380/ (Last visited December 4, 2024).</p> <p>Why should I use the device lock on my Fitbit device?</p> <p>To help keep your Fitbit device secure, turn on the device lock in the Fitbit app. You'll be prompted to enter a personal 4-digit PIN code to unlock your device. If you set up Google Wallet, the device lock is turned on automatically and you're prompted to set a code.</p>

Claim No.	Accused Products
	<p>See, e.g., <i>How do I use the device lock on my Fitbit device?</i> https://support.google.com/fitbit/answer/14236813 (Last visited December 4, 2024).</p> <p>like Samsung Wallet. In addition, Fitbit Sense 2 and Versa 4 users can make contactless payments anywhere Google Pay is accepted by accessing their stored credit or debit cards via the Google Wallet app on their watch.</p> <p>See, e.g., <i>Google Wallet Is Finally Here For The Fitbit Sense 2 & Versa 4</i> (November 17, 2022), https://screenrant.com/google-wallet-fitbit-sense-2-versa-4/ (Last visited December 4, 2024).</p>
<p>8[c]: receiving a user approval for performing the payment transaction.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, receives a user approval for performing the payment transaction (e.g., double-clicking the crown button or selecting a payment method and authenticating with passcode, password, face unlock, or fingerprint).</p> <p>See <i>supra</i> limitation 1[f].</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> <div data-bbox="443 1015 898 1239" style="border: 2px solid red; padding: 10px;"> <ul style="list-style-type: none"> • PIN • Pattern • Password • Class 3 biometric unlock </div> <p>See, e.g., <i>Verify it's you to make a purchase</i>, https://support.google.com/wallet/answer/12059519?hl=en.</p> <h3>7.3.10. Biometric Sensors</h3>

Claim No.	Accused Products
	<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; background-color: #f9f9f9; padding: 10px; margin: 10px 0;"> <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
	<div>Unlock your Pixel phone with your face</div> <div><h3>How Face Unlock works</h3><p>You can create a unique model of your face to unlock your Pixel phone with Face Unlock. Face Unlock is available on Pixel 4 and Pixel 7 or later Pixel phones, including Pixel Fold. To create this face model during setup, you'll take images of your face from different angles.</p><p>When you use Face Unlock, face images are used to update your face model so that, over time, your phone can recognize your face better in more scenarios. The face images used to create your face model aren't stored, but the face model is stored securely on your phone and never leaves the phone. All processing occurs securely on your phone.</p><p>When you enroll in Face Unlock, the face model is used only for Face Unlock and isn't shared with any other Google services or apps.</p><p>See, e.g., <i>Unlock your Pixel Phone with your face</i>, https://support.google.com/pixelphone/answer/9517039?hl=en.</p><h3>How to unlock your Pixel phone with your fingerprint</h3><p>If your phone has a fingerprint sensor, either on the display or on the back of your device, you can use your fingerprint to unlock your phone, authorize purchases, and unlock certain apps.</p><p>Learn how to set up Fingerprint Unlock on your Pixel phone with our step-by-step tutorial .</p><p>See, e.g., <i>How to unlock your Pixel phone with your fingerprint</i>, https://support.google.com/pixelphone/answer/6285273.</p><h3>Set screen lock on your Pixel phone</h3><p>You can set up a screen lock to help secure your Android phone or tablet. Each time you turn on your device or wake up the screen, you'll be asked to unlock your device, usually with a PIN, pattern, or password. On some devices, you can unlock with your fingerprint or face.</p></div>

Claim No.	Accused Products
	<p>Standard locks</p> <ul style="list-style-type: none"> • PIN: Enter 4 or more numbers, but a 6 digit PIN is recommended for added security. Longer PINs tend to be more secure. • Pattern: Draw a simple pattern with your finger. • Password: Enter 4 or more letters or numbers. A strong password is the most secure screen lock option. <p>See, e.g., Set screen lock on your Pixel phone, https://support.google.com/pixelphone/answer/2819522?hl=en.</p> <p>Google Pixel Watch - Unlock the Device</p> <p>1. From the watch screen, press the Crown button to open the apps screen.</p>  <p>2. Swipe up on the Home Screen.</p> <p>3. Do one of the following:</p> <ul style="list-style-type: none"> • Enter the 4-digit PIN. • Draw the unlock pattern. <p>See, e.g., Google Pixel Watch – Unlock the Device, https://www.verizon.com/support/knowledge-base-303380/.</p> <p>Why should I use the device lock on my Fitbit device?</p> <p>To help keep your Fitbit device secure, turn on the device lock in the Fitbit app. You'll be prompted to enter a personal 4-digit PIN code to unlock your device. If you set up Google Wallet, the device lock is turned on automatically and you're prompted to set a code.</p> <p>See, e.g., How do I use the device lock on my Fitbit device? https://support.google.com/fitbit/answer/14236813 (Last visited December 4, 2024).</p>
9[a]: The method of claim 8, wherein said user	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, receives a user approval for performing a payment transaction by displaying a request for user input at said electronic device, for both said

Claim No.	Accused Products
approval for performing a payment transaction comprises displaying a request for user input at said electronic device, for both said identifying and said user approval of said payment transaction, and further comprising:	<p>identifying and said user approval of said payment transaction</p> <p><i>See supra</i> limitation 1[f] (e.g., prompting for double-clicking the crown button or selecting a payment method and authenticating with passcode, password, face unlock, or fingerprint).</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> <p>1. Double-press the crown.</p> <p>2. Your default card will appear on the screen.</p> <p>3. If you want to pay with a different card, swipe until you find the card you want to use.</p> <p>4. Hold your Pixel Watch near the payment terminal.</p> <p>5. Once the payment has been completed successfully, you will hear a chime and a checkmark appears on your watch.</p> <p><i>See, e.g., 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> <p>1. If prompted enter your 4-digit device PIN code. Your default card appears on the screen.</p> <div data-bbox="487 995 865 1214" data-label="Image"> </div> <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>
9[b]: the processor identifying that said user input matches a known authorized user of the	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, uses a processor (e.g., as identified above) to identify that said user input matches a known authorized user of the electronic device, before said readying said device to perform a payment transaction.

Claim No.	Accused Products
electronic device, before said readying said device to perform a payment transaction; and,	<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>See, e.g., <i>Verify it's you to make a purchase</i>, https://support.google.com/wallet/answer/12059519?hl=en.</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. Both Class 2 and Class 3 biometrics get additional capabilities as detailed below.</p> <p>See, e.g., <i>Android 15 Compatibility Definition</i>, 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> <h2>Unlock your Pixel phone with your face</h2> <h3>How Face Unlock works</h3> <p>You can create a unique model of your face to unlock your Pixel phone with Face Unlock. Face Unlock is available on Pixel 4 and Pixel 7 or later Pixel phones, including Pixel Fold. To create this face model during setup, you'll take images of your face from different angles.</p> <p>When you use Face Unlock, face images are used to update your face model so that, over time, your phone can recognize your face better in more scenarios. The face images used to create your face model aren't stored, but the face model is stored securely on your phone and never leaves the phone. All processing occurs securely on your phone.</p> <p>When you enroll in Face Unlock, the face model is used only for Face Unlock and isn't shared with any other Google services or apps.</p> <p>See, e.g., <i>Unlock your Pixel Phone with your face</i>, https://support.google.com/pixelphone/answer/9517039?hl=en.</p>

Claim No.	Accused Products
	<h2>How to unlock your Pixel phone with your fingerprint</h2> <p>If your phone has a fingerprint sensor, either on the display or on the back of your device, you can use your fingerprint to unlock your phone, authorize purchases, and unlock certain apps.</p> <p>Learn how to set up Fingerprint Unlock on your Pixel phone with our step-by-step tutorial .</p> <p><i>See, e.g., How to unlock your Pixel phone with your fingerprint, https://support.google.com/pixelphone/answer/6285273.</i></p> <h2>Set screen lock on your Pixel phone</h2> <p>You can set up a screen lock to help secure your Android phone or tablet. Each time you turn on your device or wake up the screen, you’ll be asked to unlock your device, usually with a PIN, pattern, or password. On some devices, you can unlock with your fingerprint or face.</p> <h3>Standard locks</h3> <ul style="list-style-type: none">• PIN: Enter 4 or more numbers, but a 6 digit PIN is recommended for added security. Longer PINs tend to be more secure.• Pattern: Draw a simple pattern with your finger.• Password: Enter 4 or more letters or numbers. A strong password is the most secure screen lock option. <p><i>See, e.g., Set screen lock on your Pixel phone, https://support.google.com/pixelphone/answer/2819522?hl=en.</i></p>

Claim No.	Accused Products
	<p>Google Pixel Watch - Unlock the Device</p> <p>1. From the watch screen, press the Crown button to open the apps screen.</p>  <p>2. Swipe up on the Home Screen.</p> <p>3. Do one of the following:</p> <ul style="list-style-type: none"> • Enter the 4-digit PIN. • Draw the unlock pattern. <p>See, e.g., Google Pixel Watch – Unlock the Device, https://www.verizon.com/support/knowledge-base-303380/.</p> <p>Why should I use the device lock on my Fitbit device? ^</p> <p>To help keep your Fitbit device secure, turn on the device lock in the Fitbit app. You'll be prompted to enter a personal 4-digit PIN code to unlock your device. If you set up Google Wallet, the device lock is turned on automatically and you're prompted to set a code.</p> <p>See, e.g., How do I use the device lock on my Fitbit device? https://support.google.com/fitbit/answer/14236813 (Last visited December 4, 2024).</p>
<p>9[c]: disallowing the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, disallows (e.g., if fingerprint isn't recognized) the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed.</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>See, e.g., <i>Verify it's you to make a purchase</i>, https://support.google.com/wallet/answer/12059519?hl=en.</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. Both Class 2 and Class 3 biometrics get additional capabilities as detailed below.</p> <p>See, e.g., <i>Android 15 Compatibility Definition</i>, https://source.android.com/docs/compatibility/15/android-15-cdd.</p>

Claim No.	Accused Products
	<div data-bbox="457 203 1873 235"> <div>BIOMETRIC_STRONG</div> <div>Added in API level 30</div> </div> <div data-bbox="457 300 1873 414"> <pre>public static final int BIOMETRIC_STRONG</pre> </div> <div data-bbox="457 462 1785 544"> <div>Any biometric (e.g. fingerprint, iris, or face)</div> <div>on the device that meets or exceeds the requirements for Class 3 (formerly Strong), as defined by the Android CDD.</div> </div> <div data-bbox="457 576 1507 609"> <div>This corresponds to</div> <div>KeyProperties.AUTH_BIOMETRIC_STRONG</div> <div>during key generation.</div> </div> <div data-bbox="443 625 1974 698"> <div>See, e.g., BiometricManager.Authenticators , Android Developers,</div> <div>https://developer.android.com/reference/android/hardware/biometrics/BiometricManager.Authenticators#BIOMETRIC_STRONG.</div> </div> <div data-bbox="457 738 1367 803"> <h2>Unlock your Pixel phone with your face</h2> </div> <div data-bbox="457 852 879 901"> <h3>How Face Unlock works</h3> </div> <div data-bbox="457 917 1606 1031"> <p>You can create a unique model of your face to unlock your Pixel phone with Face Unlock. Face Unlock is available on Pixel 4 and Pixel 7 or later Pixel phones, including Pixel Fold. To create this face model during setup, you'll take images of your face from different angles.</p> </div> <div data-bbox="457 1055 1596 1209"> <p>When you use Face Unlock, face images are used to update your face model so that, over time, your phone can recognize your face better in more scenarios. The face images used to create your face model aren't stored, but the face model is stored securely on your phone and never leaves the phone. All processing occurs securely on your phone.</p> </div> <div data-bbox="457 1234 1566 1307"> <p>When you enroll in Face Unlock, the face model is used only for Face Unlock and isn't shared with any other Google services or apps.</p> </div> <div data-bbox="443 1315 1778 1356"> <div>See, e.g., <i>Unlock your Pixel Phone with your face</i>,</div> <div>https://support.google.com/pixelphone/answer/9517039?hl=en.</div> </div>

Claim No.	Accused Products
	<h2>How to unlock your Pixel phone with your fingerprint</h2> <p>If your phone has a fingerprint sensor, either on the display or on the back of your device, you can use your fingerprint to unlock your phone, authorize purchases, and unlock certain apps.</p> <p>Learn how to set up Fingerprint Unlock on your Pixel phone with our step-by-step tutorial .</p> <p>See, e.g., <i>How to unlock your Pixel phone with your fingerprint</i>, https://support.google.com/pixelphone/answer/6285273.</p> <p>Authorize payments or unlock apps</p> <div><p>If a message asks you to scan your fingerprint, follow its instructions. Your fingerprint information isn't shared with the app.</p><p>[...]</p></div> <h2>About fingerprint security</h2> <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., <i>How to unlock your Pixel phone with your fingerprint</i>, https://support.google.com/pixelphone/answer/6285273.</p>

Claim No.	Accused Products
	<p>Set screen lock on your Pixel phone</p> <p>You can set up a screen lock to help secure your Android phone or tablet. Each time you turn on your device or wake up the screen, you’ll be asked to unlock your device, usually with a PIN, pattern, or password. On some devices, you can unlock with your fingerprint or face.</p> <p>Standard locks</p> <ul style="list-style-type: none"> • PIN: Enter 4 or more numbers, but a 6 digit PIN is recommended for added security. Longer PINs tend to be more secure. • Pattern: Draw a simple pattern with your finger. • Password: Enter 4 or more letters or numbers. A strong password is the most secure screen lock option. <p>See, e.g., <i>Set screen lock on your Pixel phone</i>, https://support.google.com/pixelphone/answer/2819522?hl=en.</p> <p>Google Pixel Watch - Unlock the Device</p> <p>1. From the watch screen, press the Crown button to open the apps screen.</p>  <p>2. Swipe up on the Home Screen.</p> <p>3. Do one of the following:</p> <ul style="list-style-type: none"> • Enter the 4-digit PIN. • Draw the unlock pattern. <p>See, e.g., <i>Google Pixel Watch – Unlock the Device</i>, https://www.verizon.com/support/knowledge-base-303380/.</p>

Claim No.	Accused Products
	<p data-bbox="472 203 1249 235">Why should I use the device lock on my Fitbit device? ^</p> <p data-bbox="508 292 1816 422">To help keep your Fitbit device secure, turn on the device lock in the Fitbit app. You'll be prompted to enter a personal 4-digit PIN code to unlock your device. If you set up Google Wallet, the device lock is turned on automatically and you're prompted to set a code.</p> <p data-bbox="445 451 1894 511"><i>See, e.g., How do I use the device lock on my Fitbit device?</i> https://support.google.com/fitbit/answer/14236813 (Last visited December 4, 2024).</p>
<p data-bbox="100 522 432 1117">10. The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between: firstly, a user input received via at least one of a set of user input sensors of the electronic device; and, secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device.</p>	<p data-bbox="445 522 1990 649">A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, successfully validating the identified user comprises the processor successfully determining a match between: firstly, a user input received via at least one of a set of user input sensors of the electronic device; and, secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device.</p> <p data-bbox="445 690 1375 717"><i>See supra</i> limitation 1[f] (e.g., passcode, password, face unlock, or fingerprint).</p> <h2 data-bbox="478 760 1432 824">Verify it's you to make a purchase</h2> <p data-bbox="478 852 1843 933">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="478 974 1365 1006">You can verify it's you in Google Wallet with several methods:</p> <ul data-bbox="478 1047 871 1247" style="list-style-type: none"> • PIN • Pattern • Password • Class 3 biometric unlock <p data-bbox="445 1274 1659 1302"><i>See, e.g., Verify it's you to make a purchase,</i> https://support.google.com/wallet/answer/12059519?hl=en.</p> <h3 data-bbox="462 1351 871 1383">7.3.10. Biometric Sensors</h3>

Claim No.	Accused Products
	<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="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc; margin: 10px 0;"> <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
	<h2>Unlock your Pixel phone with your face</h2> <h3>How Face Unlock works</h3> <p>You can create a unique model of your face to unlock your Pixel phone with Face Unlock. Face Unlock is available on Pixel 4 and Pixel 7 or later Pixel phones, including Pixel Fold. To create this face model during setup, you'll take images of your face from different angles.</p> <p>When you use Face Unlock, face images are used to update your face model so that, over time, your phone can recognize your face better in more scenarios. The face images used to create your face model aren't stored, but the face model is stored securely on your phone and never leaves the phone. All processing occurs securely on your phone.</p> <p>When you enroll in Face Unlock, the face model is used only for Face Unlock and isn't shared with any other Google services or apps.</p> <p><i>See, e.g., Unlock your Pixel Phone with your face, https://support.google.com/pixelphone/answer/9517039?hl=en.</i></p> <h2>How to unlock your Pixel phone with your fingerprint</h2> <p>If your phone has a fingerprint sensor, either on the display or on the back of your device, you can use your fingerprint to unlock your phone, authorize purchases, and unlock certain apps.</p> <p>Learn how to set up Fingerprint Unlock on your Pixel phone with our step-by-step tutorial .</p> <p><i>See, e.g., How to unlock your Pixel phone with your fingerprint, https://support.google.com/pixelphone/answer/6285273.</i></p> <h2>Set screen lock on your Pixel phone</h2> <p>You can set up a screen lock to help secure your Android phone or tablet. Each time you turn on your device or wake up the screen, you'll be asked to unlock your device, usually with a PIN, pattern, or password. On some devices, you can unlock with your fingerprint or face.</p>

Claim No.	Accused Products
	<p>Standard locks</p> <ul style="list-style-type: none"> • PIN: Enter 4 or more numbers, but a 6 digit PIN is recommended for added security. Longer PINs tend to be more secure. • Pattern: Draw a simple pattern with your finger. • Password: Enter 4 or more letters or numbers. A strong password is the most secure screen lock option. <p>See, e.g., Set screen lock on your Pixel phone, https://support.google.com/pixelphone/answer/2819522?hl=en.</p> <p>Google Pixel Watch - Unlock the Device</p> <p>1. From the watch screen, press the Crown button to open the apps screen.</p>  <p>2. Swipe up on the Home Screen.</p> <p>3. Do one of the following:</p> <ul style="list-style-type: none"> • Enter the 4-digit PIN. • Draw the unlock pattern. <p>See, e.g., Google Pixel Watch – Unlock the Device, https://www.verizon.com/support/knowledge-base-303380/.</p> <p>Why should I use the device lock on my Fitbit device?</p> <p>To help keep your Fitbit device secure, turn on the device lock in the Fitbit app. You'll be prompted to enter a personal 4-digit PIN code to unlock your device. If you set up Google Wallet, the device lock is turned on automatically and you're prompted to set a code.</p> <p>See, e.g., How do I use the device lock on my Fitbit device? https://support.google.com/fitbit/answer/14236813 (Last visited December 4, 2024).</p>

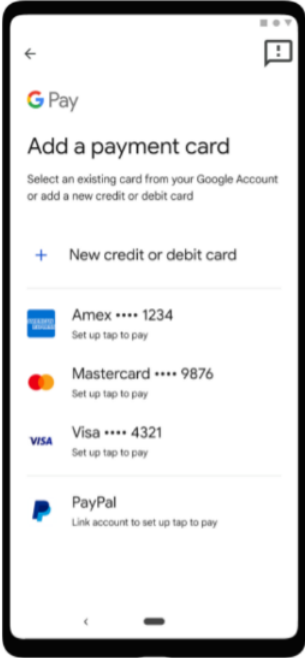
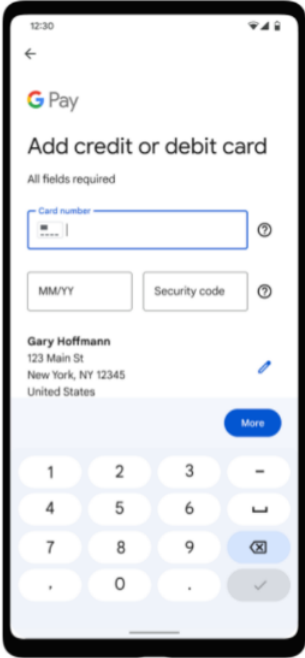
Claim No.	Accused Products
	<p>like Samsung Wallet. In addition, Fitbit Sense 2 and Versa 4 users can make contactless payments anywhere Google Pay is accepted by accessing their stored credit or debit cards via the Google Wallet app on their watch.</p> <p><i>See, e.g., Google Wallet Is Finally Here For The Fitbit Sense 2 & Versa 4</i> (November 17, 2022), https://screenrant.com/google-wallet-fitbit-sense-2-versa-4/ (Last visited December 4, 2024).</p>
11. The method of claim 10, wherein said user input received via at least one of a set of user input sensors of the electronic device comprises a passcode entry sequence performed by a user input via the touch-screen display.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, compares a user input received via at least one of a set of user input sensors of the electronic device comprises a passcode entry sequence performed by a user input via the touch-screen display</p> <p><i>See supra</i> limitation 1[f] (e.g., PIN, pattern, passcode entry).</p>
12. The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise known user biometric touch characteristics.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, compares a predetermined user characteristics stored within the electronic device comprising known user biometric touch characteristics.</p> <p><i>See supra</i> limitation 1[f] (e.g., fingerprint).</p>
13. The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user touch gesture.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, compares a predetermined user characteristics stored within the electronic device comprising a known user touch gesture.</p> <p><i>See supra</i> limitation 1[f] (e.g., PIN, pattern, passcode entry).</p>
15. The method of claim 1, wherein the input comprising a priming operation is a user input.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, receives an input wherein the input comprises a priming operation is a user input (e.g., activating Google Pay, e.g., by double clicking the crown button).</p> <p><i>See supra</i> limitation 1[a].</p>

Claim No.	Accused Products
16[a]: The method of claim 15, wherein said readying said device to perform a payment transaction comprises: successfully identifying said identified user from said user input; and,	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, readies said device to perform a payment transaction by successfully identifying said identified user from said user input. <i>See supra</i> limitation 1[f].
16[b]: wherein said user input further comprises a user approval for performing the payment transaction received from said identified user; and,	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, receives a user input comprising a user approval for performing the payment transaction received from said identified user. <i>See supra</i> limitation 1[f], claims 8 and 9.
16[c]: wherein said successfully identifying further comprises said electronic device validating an authorized user of said electronic device by comparing a user-touch input received via a touch input sensor on the electronic device with a recognized valid user-touch, stored in a memory of the electronic device; and,	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, successfully identifies said identified user further comprises said electronic device validating an authorized user of said electronic device by comparing a user-touch input received via a touch input sensor on the electronic device with a recognized valid user-touch, stored in a memory (e.g., a memory, flash, memory of secure element, memory on a SIM/eSIM) of the electronic device. <i>See supra</i> limitation 1[f] (e.g., fingerprint).
16[d]: wherein said user approval for performing the payment transaction further comprises: visually presenting information of the payment transaction on the touch screen display of said electronic device;	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, receives a user input comprising a user approval for performing the payment transaction that further comprises visually presenting information of the payment transaction on the touch screen display of said electronic device. <i>See supra</i> limitations 1[f], 1[h].

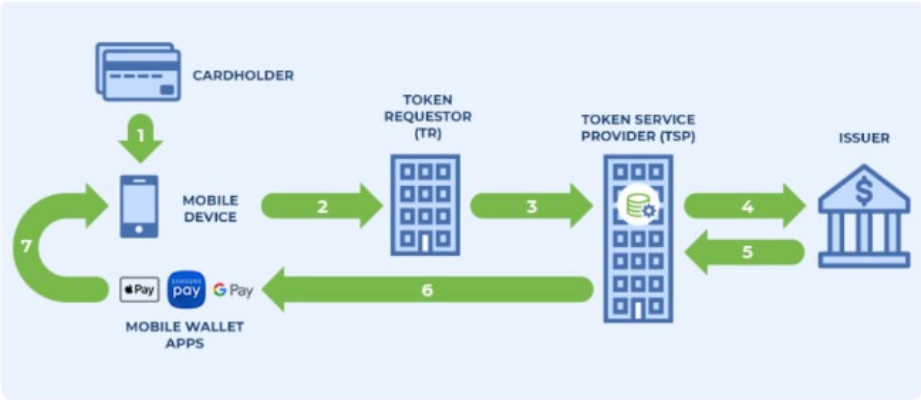
Claim No.	Accused Products
16[e]: visually presenting a request for user approval of the payment transaction via touch input at said electronic device; and,	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, visually presents a request for user approval of the payment transaction via touch input at said electronic device. <i>See supra</i> limitations 1[f], 1[h].
16[f]: subsequent to receiving a user-touch input from an identified user, approving performance of said payment transaction via said electronic device.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, subsequent to receiving a user-touch input from an identified user, approves performance of said payment transaction via said electronic device <i>See supra</i> limitations 1[f], 1[h].
17. The method of claim 1, further comprising: prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and, in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, prior to the priming operation, transmits the issued payment information (<i>e.g.</i> , as discussed above) for receipt by a payment processing authority; and, in response to said transmitting issued payment information, receives a static device account information (<i>e.g.</i> , a DPAN) and associated expiration date and key(s)) that is unique to the electronic device. <i>See supra</i> claim 3.
18[a]: The method of claim 17 further comprising: combining said limited-use payment information and said static device account information, to produce a combined payment information;	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, combines said limited-use payment information (<i>e.g.</i> , as described above) and said static device account information (<i>e.g.</i> , as described above), to produce a combined payment information (<i>e.g.</i> , DPAN and dynamic cryptogram). <i>See supra</i> limitation 4[a].
18[b]: transmitting said combined payment information, in place of the issued payment account information said NFC	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, transmits said combined payment information (<i>e.g.</i> , a combination including the dynamic cryptogram or dynamic security code, or both, with the DPAN, in place of the issued payment account information (<i>e.g.</i> , as identified above), via said NFC for receipt by an NFC recipient (<i>e.g.</i> , as identified above).

Claim No.	Accused Products
interface for receipt by an NFC recipient; and	<i>See supra</i> limitations 1[k], 1[l].
18[c]: receiving, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, receive, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction (<i>e.g.</i>, blue tick, or transaction confirmation).</p> <p><i>See supra</i> limitations 1[m].</p>
19. The method of claim 18, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, dynamically generates the limited-use payment information (<i>e.g.</i>, as identified above) based on payment processing authority secret information (<i>e.g.</i>, key).</p> <p><i>See supra</i> claim 5.</p>
20. The method of claim 19, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, bases the limited-use payment information (<i>e.g.</i>, as identified above) is based on at least one secret information shared by both the electronic device and the payment processing authority (<i>e.g.</i>, on information and belief information associated with the electronic device (<i>e.g.</i>, a transaction-unique value or IMEI), information associated with the selected payment account (<i>e.g.</i>, the DPAN, or keys), or user information (<i>e.g.</i>, as identified above)).</p> <p><i>See supra</i> claim 6.</p>
21. The method of claim 17, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, dynamically generates the limited-use payment information (<i>e.g.</i>, as identified above) based on payment processing authority secret information (<i>e.g.</i>, key).</p> <p><i>See supra</i> claim 5.</p>

Claim No.	Accused Products
<p>22. The method of claim 21, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, bases the limited-use payment information (<i>e.g.</i>, as identified above) is based on at least one secret information shared by both the electronic device and the payment processing authority (<i>e.g.</i>, on information and belief information associated with the electronic device (<i>e.g.</i>, a transaction-unique value or IMEI), information associated with the selected payment account (<i>e.g.</i>, the DPAN, or keys), or user information (<i>e.g.</i>, as identified above)).</p> <p><i>See supra</i> claim 6.</p>
<p>23. The method of claim 1, further comprising: prior to the priming operation, transmitting the issued payment information, user information and device-specific information; and, in response to transmitting said issued payment information, user information and device-specific information, receiving a payment processing authority supplied secret information.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, prior to the priming operation, transmits the issued payment information (<i>e.g.</i>, as discussed above), user information (<i>e.g.</i>, as identified above), and, on information and belief, device specific information (<i>e.g.</i>, phone number, serial number, IMEI, etc.), and, in response to transmitting said issued payment information (<i>e.g.</i>, as discussed above), user information, and device-specific information that is unique to the electronic device, receives a payment processing authority supplied secret information (<i>e.g.</i>, a DPAN and associated expiration date and key(s), issuer secrets).</p> <p><i>See supra</i> claim 3.</p> <div data-bbox="457 776 1402 1472"> <h2>Add a debit or credit card to the Google Wallet app</h2> <p>You can add a supported card to Google Wallet to pay in stores with your phone or smartwatch.</p> <h3>Add new card</h3> <hr/> <p>With the Google Wallet app </p> <ol style="list-style-type: none"> 1. Open the Google Wallet app . 2. At the bottom, tap Add to Wallet . 3. Tap Payment card. <ul style="list-style-type: none"> • Any cards you saved to your Google Account are shown. 4. Tap New credit or debit card. <ul style="list-style-type: none"> • To add a card, use your camera or tap Enter details manually. 5. At the bottom, tap Save and continue. 6. Read the Issuer Terms and tap Accept. 7. If you're asked to verify your payment method, choose an option from the list. Learn how to verify your payment method. </div>

Claim No.	Accused Products
	<p>See, e.g., <i>Add a new debit or credit card</i>, Google Wallet Help, https://support.google.com/wallet/answer/12058983; <i>Make contactless payments with Google Pixel Watch</i>, Google Pixel Watch Help, https://support.google.com/googlepixelwatch/answer/12661007.</p> <p>Key Google Pay UX flows</p> <p>Cards can be added to Google Pay either through Google Wallet surfaces or an issuer's mobile banking app using the Push Provisioning API. Google Wallet app surfaces let users to enter their card details in multiple ways, including autofilling the details using a card already stored on file, OCR scanning, and manual entry.</p> <div><div><p>Card on File</p></div><div><p>OCR Scanning</p></div><div><p>Manual entry</p></div></div> <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.</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>
24. The method of claim 23 wherein said payment processing authority supplied secret information comprises static device account information.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, receives payment processing authority supplied secret information that comprises static device account information (e.g., a DPAN and associated expiration date and key(s)).</p> <p><i>See supra</i> claim 3.</p>
25. The method of claim 24 wherein said static device account information comprises a static device account number and a static device-specific expiration date.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, receives payment processing authority supplied secret information that comprises static device account information that comprises a static device account number and a static device-specific expiration date (e.g., a DPAN and associated expiration date).</p> <p><i>See supra</i> claim 3.</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"> 1. The cardholder uses a device that supports the digital wallet application and registers a card, entering the data into the application. 2. The application sends the data to a <i>Token Requestor</i> (TR). 3. The TR sends the data to the <i>Token Service Provider</i> (TSP) with which it is registered and makes a registration request for a new token. 4. The TSP verifies the data with the card issuer. 5. If everything is correct, the TSP registers the PAN and links it to a new token in a secure database (<i>Token Vault</i>). Along with the TR Identifier, the token expiration date, and a number of additional security features called <i>Token Domain</i>, including restrictions on the use of the new token on certain channels, use by a particular merchant, limitation on the number of permitted uses, and verification of the cryptogram. 6. The TSP notifies the application of the newly generated token. 7. The application stores the generated token (<i>Device Account Number</i> (DAN) for Apple Pay or Digitized PAN (DPAN) for Samsung Pay) in a secure location (Secure Element (SE) or Host Card Emulation (HCE)).  <p>Figure 1. Payment token creation request diagram</p> <p>See, e.g., <i>Mobile payments with digital wallets and tokenization: How Google Pay, Google 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-Google-pay-samsung-pay-protect-your-card-details (captured May 9, 2024).</p>

Claim No.	Accused Products
26. The method of claim 25 wherein the static device account number is associated with the selected issued payment account on said electronic device.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, receives payment processing authority supplied secret information that comprises static device account information (<i>e.g.</i> , a DPAN and associated expiration date and key(s) associated with the issued payment information). <i>See supra</i> claim 3.
27. The method of claim 1, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, dynamically generates the limited-use payment information (<i>e.g.</i> , as identified above) based on payment processing authority secret information (<i>e.g.</i> , key). <i>See supra</i> claim 5.
28[a]: The method of claim 27 wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority; and	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, bases the limited-use payment information (<i>e.g.</i> , as identified above) is based on at least one secret information shared by both the electronic device and the payment processing authority (<i>e.g.</i> , as identified above). <i>See supra</i> claim 6.
28[b]: further wherein the at least one secret information is not exchanged when performing the payment transaction.	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone or smartwatch, on information and belief, does not exchange the at least one secret information shared by both the electronic device and the payment processing authority (<i>e.g.</i> , as identified above) when performing the payment transaction (<i>e.g.</i> , as a security feature to render the exchanged information useless if intercepted). <i>See supra</i> claim 6.

II. Claim 29 and Dependent Claims 30-38

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
29[Pre]: A system for completing a payment transaction, the system comprising:	To the extent the preamble is limiting, a Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, is a system for completing a payment transaction. <i>See supra</i> limitation 1[Pre].
29[a]: an electronic device operable to receive a priming operation, wherein the priming operation is operable to ready said device for performing a payment transaction by an identified user, and,	A Google Pay- and/or Google Wallet-enabled computing device, such as a smartphone or smartwatch (See 1[Pre]), is an electronic device that receives a priming operation (<i>e.g.</i> , activating Google Pay, <i>e.g.</i> , by double clicking the crown button or bringing device near an NFC field), wherein the priming operation is operable to ready said device for performing a payment transaction by an identified user (<i>e.g.</i> , user authenticates with passcode, password, face unlock, or fingerprint). <i>See supra</i> limitations 1[a], 1[b], and 1[f].
29[b]: wherein the electronic device further comprises: a processor;	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i> , processor or coprocessor, processor of secure element, processor of eSIM/SIM, or combination of the same). <i>See supra</i> limitation 1[c].
29[c]: a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; and,	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a near field communications (NFC) interface coupled to the processor and operable to receive a payment request (<i>e.g.</i> , from the merchant payment terminal) associated with the payment transaction <i>See supra</i> limitation 1[e] and 1[g].
29[d]: a touch-screen display coupled to the processor, and	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a touch-screen display coupled to the processor. <i>See supra</i> limitation 1[d].
29[e]: wherein the electronic device is operable to cause the display of information reflecting device-readiness, the payment request, and an image representing at least one selected issued payment account;	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, causes the display of information reflecting device-readiness (<i>e.g.</i> , direction to “Hold to Reader”), the payment request (<i>e.g.</i> , direction to “Hold to Reader”), and an image representing at least one selected issued payment account (<i>e.g.</i> , a view of the default card or another user-selected payment method). <i>See supra</i> limitation 1[h].

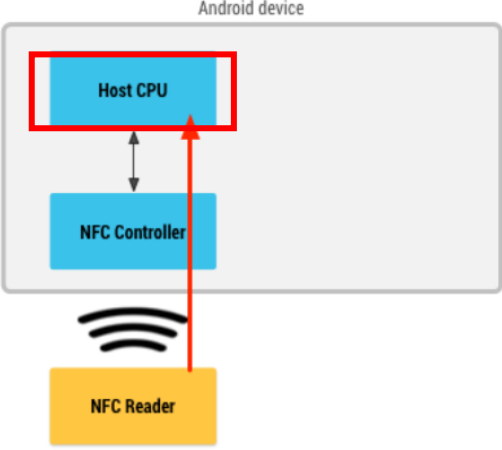
Claim No.	Google Pay- and/or Google Wallet-enabled computing device		
29[f]: wherein the electronic device is operable to dynamically generate limited-use payment information based on a sequential counter count from the electronic device;	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, dynamically generate limited-use payment information (e.g., dynamic cryptogram, transaction cryptogram, application cryptogram, or any combination of the same) based on a sequential counter count from the electronic device (e.g., transaction-unique value).</p> <p><i>See supra</i> limitations 1[i] and 1[j].</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><i>See, e.g.,</i> 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><i>See, e.g.,</i> 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><i>See, e.g.,</i> 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.		
29[g]: wherein the electronic device is operable to store a static device-specific user account information;	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, stores (e.g., in the secure element and/or Host-based Card Emulation (“HCE”)) a static device-specific user account information (e.g., the DPAN).</p> <p><i>See supra</i> claim 3.</p>		

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
	<p>What device tokens are</p> <p>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>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><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> <p>12) Will the DPAN be stored encrypted along with the LUK in the service layer’s sqlite database?</p> <p>Yes. Each TSP provides a payment bundle which includes static data like the token and dynamic data like the keys. The bundle data is stored encrypted on the device.</p> <p><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.</i></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>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
	<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 User->>Google: User accepts Google Pay ToS Google->>TSP: checkEligibility() TSP-->>Issuer: checkEligibility() Issuer-->>TSP: Success TSP-->>Google: Success (card metadata, Issuer ToS, card art) Google->>User: Present issuer ToS User->>Google: ToS accpeted Google->>TSP: tokenize(risk signals, provisioning data) TSP->>Issuer: tokenize(risk signals, provisioning data) Issuer-->>TSP: idvOutcome(approved, declined,challenge) TSP-->>Google: idvOutcome(approved, declined,challenge) Google-->>User: idvOutcome(approved, declined,challenge) 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.</p>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
	<div> <div>In general terms, the process for registering a card in a mobile wallet is as follows: [. . .]</div> <div> <div>6. The TSP notifies the application of the newly generated token.</div> <div> <div>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)).</div> <div> <p>The diagram illustrates the tokenization process flow involving five main entities: CARDHOLDER, MOBILE DEVICE, TOKEN REQUESTOR (TR), TOKEN SERVICE PROVIDER (TSP), and ISSUER. The process is numbered 1 through 6. Step 1 shows the CARDHOLDER interacting with the MOBILE DEVICE. Step 2 shows the MOBILE DEVICE sending a request to the TOKEN REQUESTOR (TR). Step 3 shows the TR sending a request to the TOKEN SERVICE PROVIDER (TSP). Step 4 shows the TSP sending a response to the ISSUER. Step 5 shows the ISSUER sending a response back to the TSP. Step 6 shows the TSP sending a response back to the MOBILE DEVICE. A red box highlights step 7, which is a curved arrow indicating the MOBILE DEVICE storing the token in the MOBILE WALLET APPS.</p> </div> </div> </div> <div> <div>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.</div> <div> <div>5. End-to-End EMV Payment Tokenization Flows</div> <div> <div>This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):</div> <div> <div> <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> </div> </div> </div></div>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
	<div data-bbox="451 186 1491 698"> <p>Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet</p> <p><i>See, e.g., US Payments Forum, EMV Payment Tokenization Primer and Lessons Learned at 12 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</i></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> </div>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
	<p data-bbox="457 199 1402 264">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 data-bbox="457 272 779 297">5.1.3.4 Token Provisioning</p> <p data-bbox="457 313 1392 370">Token Provisioning is the process of delivering a Payment Token and related data to the Token Location.</p> <p data-bbox="457 394 1392 516">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 data-bbox="457 524 1980 589">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/.</p> <p data-bbox="457 605 930 638">Host-based card emulation</p> <p data-bbox="457 670 1738 735">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> <div data-bbox="468 743 966 1190">  <p>The diagram shows an Android device (grey box) containing a Host CPU (blue box) and an NFC Controller (blue box). The Host CPU and NFC Controller are connected by a double-headed arrow. Below the device is an NFC Reader (yellow box) with a red arrow pointing up to the Host CPU. A black curved arrow points from the NFC Controller to the Host CPU, indicating data flow.</p> </div> <p data-bbox="457 1206 1003 1230">Figure 2. NFC card emulation without a secure element.</p> <p data-bbox="457 1263 1707 1295">See, e.g., <i>Host-based card emulation overview</i>, https://developer.android.com/develop/connectivity/nfc/hce.</p> <ul data-bbox="457 1344 1864 1417" 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 data-bbox="457 1433 1455 1466">See, e.g., <i>Fitbit Pay FAQ</i>, https://developers.google.com/pay/issuers/support/fitbit-faq.</p>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
29[h]: wherein the electronic device is operable to transmit a combination of said dynamically generated limited-use payment information and said static device-specific user account information to an NFC recipient via, said NFC interface for use in connection with payment transaction in place of information associated with said selected issued payment account;	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, transmits a combination of said dynamically generated limited-use payment information (<i>e.g.</i>, as identified above) and said static device-specific user account information (<i>e.g.</i>, as identified above) to an NFC recipient (<i>e.g.</i>, a contactless reader) via, said NFC interface for use in connection with payment transaction in place of information associated with said selected issued payment account (<i>e.g.</i>, PAN or associated expiration date or CVV).</p> <p><i>See supra</i> limitations 1[k] and 1[l] and claim 3.</p>
29[i]: wherein the electronic device is operable, subsequent to transmission of said combination, to receive a status information reflecting a status of said payment transaction; and, wherein the touch-screen display is operable to display as indication of said status information.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, subsequent to transmission of said combination, to receive a status information reflecting a status of said payment transaction; and, wherein the touch-screen display is operable to display as indication of said status information.</p> <p><i>See supra</i> limitation 1[m].</p>
30. The system of claim 29, wherein the dynamically generated limited-use payment information comprises a cryptogram number.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, dynamically generates limited-use payment information (<i>e.g.</i>, as identified above) comprising a cryptogram number (<i>e.g.</i>, dynamic cryptogram, transaction cryptogram, application cryptogram).</p> <p><i>See supra</i> claim 2.</p>
31. The system of claim 29, wherein the device-specific user account information comprises static device account information.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, receives device-specific user account information comprising static device account information (<i>e.g.</i>, a DPAN and associated expiration date and key(s)).</p> <p><i>See supra</i> claim 3.</p>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device		
32. The system of claim 31, wherein the static device account information comprises a static device account number that is unique to the electronic device.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, receives static device account information comprising a static device account number that is unique to the electronic device (<i>e.g.</i> , a DPAN). <i>See supra</i> claim 3.		
33. The system of claim 32 wherein the static device account information further comprises a static device account expiration date.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, receives the static device account information further comprising a static device account expiration date. <i>See supra</i> claim 25.		
34. The system of claim 32 wherein the sequential counter count is changed per payment transaction.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, dynamically generates limited-use payment information (<i>e.g.</i> , as identified above) based on a sequential counter count that is changed per payment transaction (<i>e.g.</i> , transaction-unique value). <i>See supra</i> limitation 1[j]. 3. Tokenization Use Case Scenarios Payment tokenization can be implemented in a variety of environments and use cases: <ul style="list-style-type: none"> • In-store EMV contactless payments with device-centric³ digital wallets (<i>e.g.</i>, Apple Pay, Google Pay, Samsung Pay) <i>See, e.g.</i> , 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 . <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> <i>See, e.g.</i> , EMVCo, <i>EMV Payment Tokenisation Specification – Technical Framework</i> at 10 (June 2019 ver. 2.1).	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.	Google Pay- and/or Google Wallet-enabled computing device
	<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>35. The system of claim 34 wherein the electronic device is operable to transmit issued payment account information and in response thereto, to receive the static device account information.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, transmits issued payment account information (e.g., the PAN or associated expiration date or CVV) and in response thereto, to receive the static device account information (e.g., as described above).</p> <p><i>See supra</i> claim 3.</p>
<p>36. The system of claim 29 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on a shared information: from said user, information associated with said electronic device, information associated with said selected, issued payment account, and at least one secret; and, wherein said shared information is shared by both the electronic device and a payment processing authority.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, dynamically generates the limited-use payment information (e.g., as identified above) based on a shared information: from said user (e.g., account information, birth date, etc.), information associated with said electronic device (e.g., phone number, serial number, IMEI, etc.), information associated with said selected, issued payment account (e.g., the DPAN, or keys), and at least one secret (e.g., keys); and, wherein said shared information is shared by both the electronic device and a payment processing authority.</p> <p><i>See supra</i> claim 6.</p>

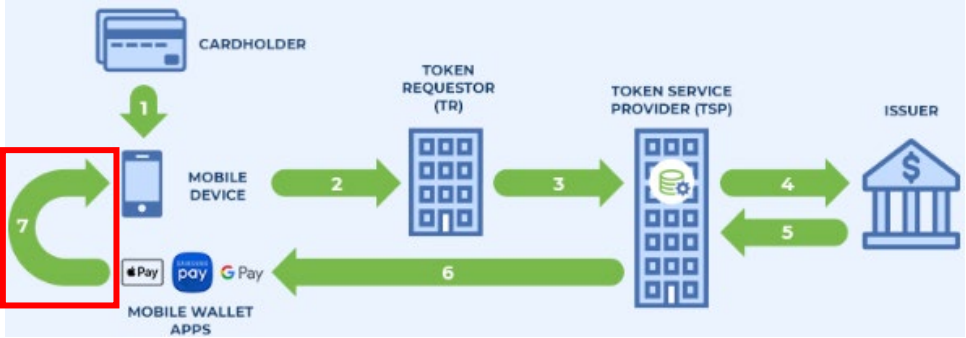
Claim No.	Google Pay- and/or Google Wallet-enabled computing device
37. The system of claim 36 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, dynamically generates the limited-use payment information (<i>e.g.</i>, as identified above) based on payment processing authority secrets (<i>e.g.</i>, key).</p> <p><i>See supra</i> claim 5.</p>
38. The system of claim 29 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, dynamically generates the limited-use payment information (<i>e.g.</i>, as identified above) based on payment processing authority secrets (<i>e.g.</i>, key).</p> <p><i>See supra</i> claim 5.</p>

III. Claim 39 and Dependent Claims 40–53, 55

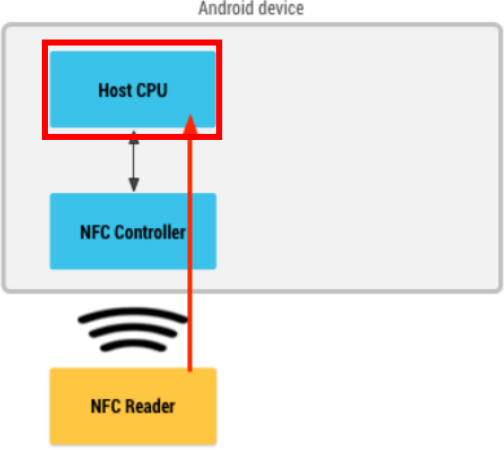
Claim No.	Google Pay- and/or Google Wallet-enabled computing device
39[Pre]: An electronic device for completing a payment transaction, the electronic device comprising:	To the extent the preamble is limiting, a Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, is an electronic device for completing a payment transaction. <i>See supra</i> limitations 1[pre], 1[b].
39[a]: a processor;	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i> , processor or coprocessor or processor of secure element or processor of eSIM/SIM or combination of the same). <i>See supra</i> limitation 1[c].
39[b]: a memory coupled to the processor, wherein the memory is operable to store information associated with use of an issued payment account and wherein the payment authority information comprises a secret information;	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a memory (<i>e.g.</i>, memory, memory of secure element, memory of eSIM/SIM, or host CPU) coupled to the processor, wherein the memory is operable to store information associated with use of an issued payment account (<i>e.g.</i>, DPAN and associated expiration date and key(s)), and wherein the payment authority information comprises a secret information (<i>e.g.</i>, keys).</p> <p>What device tokens are</p> <p>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>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><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> <p>12) Will the DPAN be stored encrypted along with the LUK in the service layer’s sqlite database?</p> <p>Yes. Each TSP provides a payment bundle which includes static data like the token and dynamic data like the keys. The bundle data is stored encrypted on the device.</p> <p><i>See, e.g., Google, 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.</p>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
	<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>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
	<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 User->>Google: User accepts Google Pay ToS Google->>TSP: checkEligibility() TSP->>Issuer: checkEligibility() Issuer-->>TSP: Success TSP-->>Google: Success (card metadata, Issuer ToS, card art) Google->>User: Present issuer ToS User->>Google: ToS accpeted Google->>TSP: tokenize(risk signals, provisioning data) TSP->>Issuer: tokenize(risk signals, provisioning data) Issuer-->>TSP: idvOutcome(approved, declined, challenge) TSP-->>Google: idvOutcome(approved, declined, challenge) Google->>User: idvOutcome(approved, declined, challenge) 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.</p>

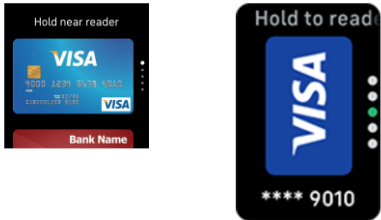
Claim No.	Google Pay- and/or Google Wallet-enabled computing device
	<p>In general terms, the process for registering a card in a mobile wallet is as follows: [. . .]</p> <p>6. The TSP notifies the application of the newly generated token.</p> <p>7. The application stores the generated token (<i>Device 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>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>3.1 In-Store EMV Contactless Payments with Device-Centric Digital Wallets</h3> <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> <h2>5. End-to-End EMV Payment Tokenization Flows</h2> <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.	Google Pay- and/or Google Wallet-enabled computing device
	<div data-bbox="451 186 1491 698"> <p>Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet</p> <p><i>See, e.g., US Payments Forum, EMV Payment Tokenization Primer and Lessons Learned at 12 (June 2019), available at https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf.</i></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> </div>

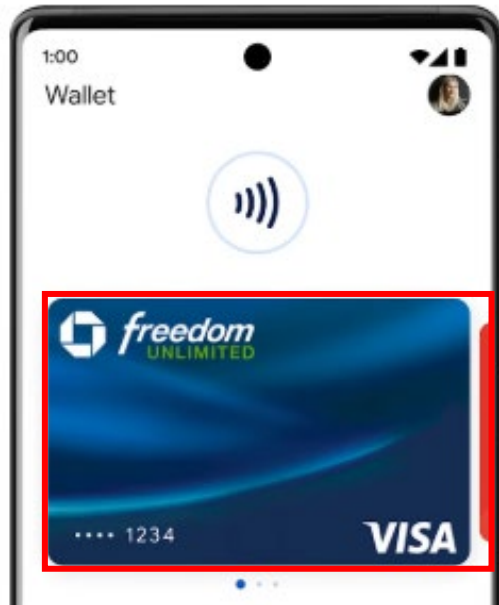
Claim No.	Google Pay- and/or Google Wallet-enabled computing device
	<p data-bbox="457 199 1402 264">Tokens SHALL only be issued through the response to a Token Request from a registered Token Requestor with a valid Token Requestor ID.</p> <p data-bbox="457 272 779 297">5.1.3.4 Token Provisioning</p> <p data-bbox="457 313 1392 370">Token Provisioning is the process of delivering a Payment Token and related data to the Token Location.</p> <p data-bbox="457 394 1392 516">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 data-bbox="457 524 1982 581"><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 data-bbox="457 597 932 638">Host-based card emulation</p> <p data-bbox="457 670 1738 735">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> <div data-bbox="468 743 968 1190">  <p>The diagram shows an 'Android device' box containing a 'Host CPU' box and an 'NFC Controller' box. The 'Host CPU' box is highlighted with a red border. A double-headed arrow connects the 'Host CPU' and 'NFC Controller' boxes. Below the 'Android device' box is an 'NFC Reader' box. A red arrow points from the 'NFC Reader' box up to the 'Host CPU' box, passing through the 'NFC Controller' box. There are also three curved lines representing an antenna between the 'NFC Controller' and the 'NFC Reader'.</p> </div> <p data-bbox="457 1206 1003 1230">Figure 2. NFC card emulation without a secure element.</p> <p data-bbox="457 1263 1707 1295"><i>See, e.g., Host-based card emulation overview, https://developer.android.com/develop/connectivity/nfc/hce.</i></p> <ul data-bbox="457 1344 1860 1417" 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 data-bbox="457 1433 1455 1466"><i>See, e.g., Fitbit Pay FAQ, https://developers.google.com/pay/issuers/support/fitbit-faq.</i></p>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
39[c]: a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction (e.g., from the merchant payment terminal).</p> <p><i>See supra</i> limitations 1[e], 1[g].</p>
39[d]: a user interface coupled to the processor;	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a user interface coupled to the processor (e.g., display).</p> <p><i>See supra</i> limitation 1[d].</p>
39[e]: a user input device coupled to the processor; and,	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a user input device (e.g., touchscreen (e.g., for passcode, password), biometric sensors (e.g., for face unlock, fingerprint)) coupled to the processor (e.g., as identified above).</p> <p><i>See supra</i> limitation 1[f].</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><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>

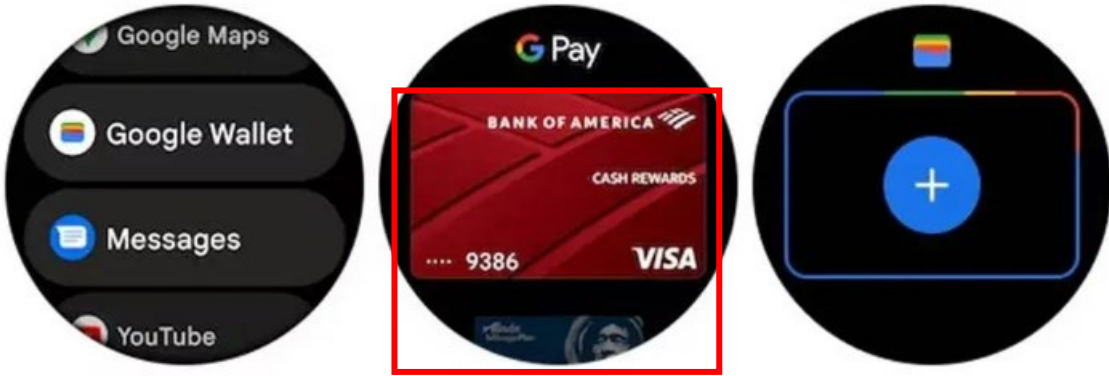
Claim No.	Google Pay- and/or Google Wallet-enabled computing device
	<p>7.3.10. Biometric Sensors</p> <p>Biometric sensors can be classified as Class 3 (formerly Strong), Class 2 (formerly Weak), or Class 1 (formerly Convenience) based on their spoof and imposter acceptance rates, and on the security 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; background-color: #f9f9f9; padding: 10px; margin: 10px 0;"> <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.	Google Pay- and/or Google Wallet-enabled computing device
	<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> <p>1. Double-press the crown.</p> <p>2. Your default card will appear on the screen.</p> <p>3. If you want to pay with a different card, swipe until you find the card you want to use.</p> <p>4. Hold your Pixel Watch near the payment terminal.</p> <p>5. Once the payment has been completed successfully, you will hear a chime and a checkmark appears on your watch.</p> <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> <p>1. If prompted enter your 4-digit device PIN code. Your default card appears on the screen.</p> <div data-bbox="491 863 869 1081">  </div> <p>2. To pay with your default card, hold your wrist near the payment terminal. To pay with a different card:</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.	Google Pay- and/or Google Wallet-enabled computing device
39[f]: wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i>, as identified above) that, responsive to a priming operation (<i>e.g.</i>, activating Google Pay, <i>e.g.</i>, by double clicking the crown button or bringing device near an NFC field), wherein the priming operation is operable to ready the device to perform the payment transaction.</p> <p><i>See supra</i> limitations 1[a], 1[f].</p>
39[g]: cause the display of information associated with the payment request; cause the display of an image representing at least one user-selectable issued payment account; and,	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i>, as identified above) that, responsive to a priming operation (<i>e.g.</i>, as identified above) causes the display of information associated with the payment request (<i>e.g.</i>, direction to “Hold to Reader”) and causes the display of an image representing at least one user-selectable issued payment account (<i>e.g.</i>, a view of the default card or another user-selected payment method).</p> <p><i>See supra</i> limitation 1[h].</p>



See, e.g., Molly McHugh-Johnson, *Ask a Techspert: How do digital wallets work?*, Google – The Keyword (May 11, 2022), <https://blog.google/products/android/ask-a-techspert-google-wallet/>.

Claim No.	Google Pay- and/or Google Wallet-enabled computing device		
	 <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>		
<p>39[h]: dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and secret information associated with a selected issued payment account; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (e.g., as identified above) that, responsive to a priming operation (e.g., as identified above), dynamically generates a limited-use payment information (e.g., dynamic cryptogram, transaction cryptogram, application cryptogram, or any combination including the same) based on a per-transaction sequential parameter originating from the electronic device (e.g., transaction-unique value), and secret information associated with a selected issued payment account (e.g., key).</p> <p>See <i>supra</i> limitations 1[i], 1[j] and claims 3, 5.</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" data-bbox="451 1263 1451 1425"> <tr> <td data-bbox="451 1263 674 1425">Token Cryptogram</td><td data-bbox="674 1263 1451 1425">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.	Google Pay- and/or Google Wallet-enabled computing device
	<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>39[i]: cause the transmission, via said NFC interface, a payment information combination comprising the dynamically generated limited-use payment information and said payment authority information, for receipt by an NFC recipient;</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (e.g., as identified above) that, responsive to a priming operation (e.g., as identified above), causes the transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information (e.g., as identified above) and said payment authority information (e.g., as identified above), for receipt by an NFC recipient (e.g., a contactless reader).</p> <p><i>See supra</i> limitations 1[k], 1[l], 4[a], and 4[b].</p>
<p>39[j]: wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the status information.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes an NFC interface that in response to transmitting said payment information combination (e.g., as identified above), receives status information reflecting a transaction processing status of said payment transaction (e.g., transaction confirmation); and wherein the user interface (e.g., as identified above) is operable to provide an indication of the status information (e.g., blue tick, check mark or transaction confirmation notification).</p> <p><i>See supra</i> limitation 1[m].</p>
<p>40. The device of claim 39 wherein the payment authority information comprises information that is unique to the electronic device.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, stores payment authority information that is unique to the electronic device (e.g., DPAN).</p> <p><i>See supra</i> claim 3.</p>

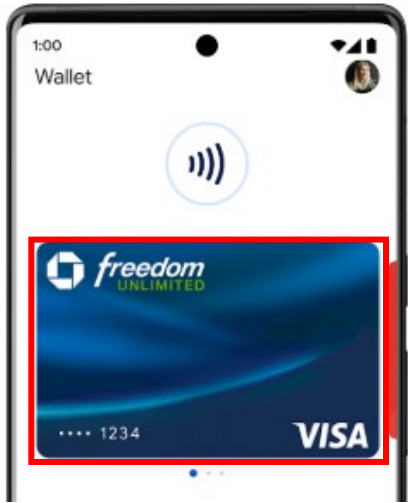
Claim No.	Google Pay- and/or Google Wallet-enabled computing device
41. The device of claim 39 wherein the payment authority information comprises a secret information shared by both the electronic device and a payment processing authority.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, stores payment authority information that comprises a secret information shared by both the electronic device and a payment processing authority (e.g., the DPAN, associated expiration date, or keys). <i>See supra</i> claim 6.
42. The device of claim 41 wherein the processing authority information comprises a static device account number.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, stores processing authority information that comprises a static device account number (e.g., DPAN). <i>See supra</i> claim 3.
43. The device of claim 42 wherein the processing authority information further comprises a static device account expiration date.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, stores processing authority information that comprises a static device account expiration date (e.g., an expiration date associated with the DPAN). <i>See supra</i> claim 25.
44. The device of claim 39 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the processing authority information.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (e.g., as identified above) that causes the transmission (e.g., the NFC interface) of issued payment account information (e.g., PAN or associated expiration date or CVV) and in response thereto, to receive the processing authority information (e.g., as identified above). <i>See supra</i> limitation 1[c] and claim 3.
45[a]: The device of claim 39 wherein the dynamically generated limited-use payment information comprises a cryptogram number, and	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, dynamically generates limited-use payment information comprising a cryptogram number (e.g., dynamic cryptogram, transaction cryptogram, application cryptogram) <i>See supra</i> claim 2.

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
45[b]: further wherein the processor is operable to cause transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information and at least a portion of said payment authority information in connection with the payment transaction in place of at least a portion of the payment information associated with said selected issued payment account.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i>, as identified above) that causes transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information (<i>e.g.</i>, as identified above) and at least a portion of said payment authority information (<i>e.g.</i>, as identified above) in connection with the payment transaction in place of at least a portion of the payment information associated with said selected issued payment account (<i>e.g.</i>, PAN or associated expiration date or CVV).</p> <p><i>See supra</i> limitations 1[j], 1[k], 1[l] and claim 5.</p>
46. The device of claim 45 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the processing authority information.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i>, as identified above) that cause the transmission of issued payment account information (<i>e.g.</i>, as identified above) and in response thereto, receive the processing authority information (<i>e.g.</i>, as identified above).</p> <p><i>See supra</i> claim 3.</p>
47. The device of claim 46 wherein the processing authority information comprises a static device account number.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, stores processing authority information that comprises a static device account number (<i>e.g.</i>, DPAN).</p> <p><i>See supra</i> claims 3.</p>
48. The device of claim 47 wherein the processing authority information further comprises a static device account expiration date.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, stores processing authority information that comprises a static device account expiration date (<i>e.g.</i>, an expiration date associated with the DPAN).</p> <p><i>See supra</i> claim 25.</p>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
<p>49. The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch panel.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a user interface comprising a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor (<i>e.g.</i>, as identified above) is operable to identify an authorized user by validating a valid user passcode input to the touch panel.</p> <p><i>See supra</i> limitations 1[d], 1[f] (<i>e.g.</i>, passcode entry).</p>
<p>50. The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response thereto.</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a user interface comprising a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor (<i>e.g.</i>, as identified above) is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response thereto.</p> <p><i>See supra</i> limitations 1[d], 1[f] (<i>e.g.</i>, PIN, password entry).</p>
<p>51. The device of claim 39, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor (<i>e.g.</i>, as identified above) is operable to identify an authorized user by biometric sensing of a continuous user touch.</p> <p><i>See supra</i> limitations 1[d], 1[f] (<i>e.g.</i>, wrist detection).</p>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
by biometric sensing of a continuous user touch.	<div data-bbox="457 198 1713 315" style="border: 2px solid red; padding: 5px;"> <p>On supported devices that run Wear OS 5 or higher, the system detects whether the user is wearing the device on their wrist. If the user turns off wrist detection and then takes the device off of their wrist, the system keeps the device unlocked for a longer period of time than it would otherwise.</p> </div> <p>If your app requires a higher level of security—such as when displaying potentially sensitive or private data—first check whether wrist detection is enabled:</p> <div data-bbox="457 444 1675 574" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>val wristDetectionEnabled = isWristDetectionAutoLockingEnabled(applicationContext)</pre> </div> <p>If the return value of this method is <code>false</code>, prompt the user to sign into an account in your app before displaying user-specific content.</p> <p><i>See, e.g., Authentication of wearables</i>, https://developer.android.com/training/wearables/apps/auth-wear.</p>
52. The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch panel.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a user interface comprising a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor (<i>e.g.</i>, as identified above) is operable to identify an authorized user by biometric sensing of a user touch at the touch panel.</p> <p><i>See supra</i> limitations 1[d], 1[f] (<i>e.g.</i>, a fingerprint).</p>
53. The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a user interface comprising a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor (<i>e.g.</i>, as identified above) is operable to identify an authorized user by biometric recognition of a valid user identification.</p> <p><i>See supra</i> limitations 1[d], 1[f] (<i>e.g.</i>, face unlock, fingerprint, wrist detection, or Class 3 biometric unlock).</p>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
biometric recognition of a valid user identification.	<p data-bbox="443 196 1115 245">Verify it’s you to make a purchase</p> <p data-bbox="443 261 1402 321">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="443 342 1066 370">You can verify it’s you in Google Wallet with several methods:</p> <div data-bbox="443 386 858 544" style="border: 2px solid red; padding: 5px;"> <ul style="list-style-type: none"> <li data-bbox="443 394 506 418">• PIN <li data-bbox="443 435 548 459">• Pattern <li data-bbox="443 475 569 500">• Password <li data-bbox="443 516 716 540">• Class 3 biometric unlock </div> <p data-bbox="443 565 1388 625">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="443 630 1997 792"><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> <p data-bbox="443 841 877 873">7.3.10. Biometric Sensors</p> <p data-bbox="443 894 1858 1117">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 data-bbox="443 1138 1598 1166">Both Class 2 and Class 3 biometrics get additional capabilities as detailed below.</p> <p data-bbox="443 1182 1766 1205"><i>See, e.g.,</i> Android 15 Compatibility Definition, https://source.android.com/docs/compatibility/15/android-15-cdd.</p>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
	<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 KeyProperties.AUTH_BIOMETRIC_STRONG 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>
<p>55[a]: The device of claim 39, wherein the processor is operable to: receive a user-selection of an issued payment account presented on the user interface, received the user input device coupled to the processor, and</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (e.g., as identified above) that receives a user-selection of an issued payment account (e.g., by confirming use of the default card or selecting a card other than the default) presented on the user interface, received via the user input device (e.g., touchscreen panel) coupled to the processor.</p> <p>See <i>supra</i> limitation 1[h].</p> <div style="text-align: center;">  </div> <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>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
	 <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>
55[b]: responsive thereto, select from the memory a specific processing authority information corresponding to the user-selected issued payment account information, and	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (e.g., as identified above), that selects from the memory (e.g., as identified above) a specific processing authority information (e.g., the DPAN and associated expiration date and key(s)) corresponding to the user-selected issued payment account information.</p> <p>See <i>supra</i> limitation 1[h], 1[k], claim 3.</p> <ol style="list-style-type: none"> 5. If everything is correct, the TSP registers the PAN and links it to a new token in a secure database (<i>Token Vault</i>). Along with the TR Identifier, the token expiration date, and a number of additional security features called <i>Token Domain</i>, including restrictions on the use of the new token on certain channels, use by a particular merchant, limitation on the number of permitted uses, and verification of the cryptogram. 6. The TSP notifies the application of the newly generated token. 7. The application stores the generated token (<i>Device Account Number</i> (DAN) for Apple Pay or Digitized PAN (DPAN) for Samsung Pay) in a secure location (Secure Element (SE) or Host Card Emulation (HCE)).

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
	<div data-bbox="447 196 1400 526"> <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. </div> <div data-bbox="447 878 1293 922" 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="447 922 1400 1450"> </div>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
	<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), <i>available at</i> https://web.archive.org/web/20240509123131/https://www.advantio.com/blog/heres-how-google-pay-apple-pay-samsung-pay-protect-your-card-details .
55[c]: use at least a portion of said specific processing authority information in place of at least a portion of the issued payment account information to generate a combined payment information to complete a payment transaction per the input user-selection.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, uses at least a portion of said specific processing authority information (<i>e.g.</i>, as identified above) in place of at least a portion of the issued payment account information to generate a combined payment information (<i>e.g.</i>, a combination including the dynamic cryptogram, transaction cryptogram, or application cryptogram, with the DPAN) to complete a payment transaction per the input user-selection (<i>e.g.</i>, as identified above).</p> <p><i>See supra</i> limitations 1[i], 1[k], 4[a].</p>

IV. Claim 56 and Dependent Claims 57–70, 72

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
56[Pre]: An electronic device for completing a payment transaction, the electronic device comprising:	To the extent the preamble is limiting, a Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, is an electronic device for completing a payment transaction. <i>See supra</i> limitations 1[pre], 1[b].
56[a]: a processor;	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i> , processor or coprocessor or processor of secure element or processor of eSIM/SIM or combination of the same). <i>See supra</i> limitation 1[c].
56[b]: a memory coupled to the processor, wherein the memory stores a payment authority information associated with a user-selectable issued payment account, and wherein the payment authority information includes a secret information;	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a memory (<i>e.g.</i> , a system memory, memory of secure element, memory of eSIM/SIM, or host CPU) coupled to the processor, wherein the memory stores a payment authority information (<i>e.g.</i> , DPAN and associated expiration date and key(s)) associated with a user-selectable issued payment account (<i>e.g.</i> , by confirming use of the default card or selecting a card other than the default), and wherein the payment authority information includes a secret information (<i>e.g.</i> , keys). <i>See supra</i> limitations 1[h], 39[b].
56[c]: a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction (<i>e.g.</i> , from the merchant payment terminal). <i>See supra</i> limitations 1[e], 1[g].
56[d]: a user interface coupled to the processor;	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a user interface coupled to the processor (<i>e.g.</i> , display). <i>See supra</i> limitation 1[d].
56[e]: a user input device coupled to the processor; and,	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a user input device (<i>e.g.</i> , touchscreen (<i>e.g.</i> , for PIN, passcode, password), biometric sensors (<i>e.g.</i> , for face unlock, fingerprint, or wrist detection) coupled to the processor (<i>e.g.</i> , as identified above). <i>See supra</i> limitations 1[f], 39[e].

Claim No.	Google Pay- and/or Google Wallet-enabled computing device		
56[f]: wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i>, as identified above) that, responsive to a priming operation (<i>e.g.</i>, activating Google Pay, <i>e.g.</i>, by double clicking the crown button or bringing device near an NFC field), wherein the priming operation is operable to ready the device to perform the payment transaction.</p> <p><i>See supra</i> limitations 1[a], 1[f].</p>		
56[g]: cause the display of information associated with the payment request; cause the display of an image representing the user-selectable issued payment account; and,	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i>, as identified above) that responsive to a priming operation (<i>e.g.</i>, as identified above), causes the display of information associated with the payment request (<i>e.g.</i>, direction to “Hold to Reader”) and causes the display of an image representing at least one user-selectable issued payment account (<i>e.g.</i>, a view of the default card or another user-selected payment method).</p> <p><i>See supra</i> limitation 1[h].</p>		
56[h]: dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and the secret information associated with the user-selectable issued payment account; and,	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i>, as identified above) that, responsive to a priming operation (<i>e.g.</i>, as identified above), dynamically generates a limited-use payment information (<i>e.g.</i>, dynamic cryptogram, transaction cryptogram, application cryptogram, or any combination including the same) based on a per-transaction sequential parameter originating from the electronic device (<i>e.g.</i>, transaction-unique value), and the secret information associated with the user-selectable issued payment account (<i>e.g.</i>, limited-use key).</p> <p><i>See supra</i> limitations 1[i], 1[j] and claims 3, 5.</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 (<i>e.g.</i>, Apple Pay, Google Pay, Samsung Pay) <p><i>See, e.g.</i>, 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><i>See, e.g.</i>, 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.	Google Pay- and/or Google Wallet-enabled computing device
56[i]: cause the transmission, via said NFC interface, of a payment information combination comprising, the dynamically generated limited-use payment information and at least a portion of said payment authority information, for receipt by an NFC recipient;	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i>, as identified above) that, responsive to a priming operation (<i>e.g.</i>, as identified above), causes the transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information (<i>e.g.</i>, as identified above) and said payment authority information (<i>e.g.</i>, as identified above), for receipt by an NFC recipient (<i>e.g.</i>, a contactless reader).</p> <p><i>See supra</i> limitations 1[k], 1[l], 4[a], and 4[b].</p>
56[j]: wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the transaction status information.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes an NFC interface that, in response to transmitting said payment information combination (<i>e.g.</i>, as identified above), receives status information reflecting a transaction processing status of said payment transaction (<i>e.g.</i>, transaction confirmation); and wherein the user interface (<i>e.g.</i>, as identified above) is operable to provide an indication of the status information (<i>e.g.</i>, blue tick, check mark or transaction confirmation notification).</p> <p><i>See supra</i> limitation 1[m].</p>
57.: The device of claim 56, wherein the payment authority information comprises information that is unique to the electronic device.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, stores payment authority information comprises information that is unique to the electronic device (<i>e.g.</i>, DPAN).</p> <p><i>See supra</i> claim 3.</p>
58. The device of claim 57, wherein the payment authority information comprises a static device account number.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, stores payment authority information that comprises a static device account number (<i>e.g.</i>, DPAN).</p> <p><i>See supra</i> claim 3.</p>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
59. The device of claim 58, wherein the payment authority information further comprises a static device account expiration date.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, stores payment authority information that further comprises a static device account expiration date (<i>e.g.</i> , an expiration date associated with the DPAN). <i>See supra</i> claim 25.
60. The device of claim 56, wherein the secret information is shared by both the electronic device and a payment processing authority.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, stores secret information that is shared by both the electronic device and a payment processing authority (<i>e.g.</i> , the DPAN, associated expiration date, or keys). <i>See supra</i> claim 6.
61. The device of claim 56, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the payment authority information.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i> , as identified above) that is operable to cause the transmission (<i>e.g.</i> , via the NFC interface) of issued payment account information (<i>e.g.</i> , PAN or associated expiration date or CVV) and in response thereto, to receive the payment authority information (<i>e.g.</i> , as identified above). <i>See supra</i> limitation 1[c] and claim 3.
62. The device of claim 56, wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further payment information combination is used in place of at least a portion of fixed payment information associated with said user-selectable issued payment account.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i> , as identified above) that dynamically generates limited-use payment information comprising a cryptogram number (<i>e.g.</i> , dynamic cryptogram, transaction cryptogram, application cryptogram), and further the payment information combination (<i>e.g.</i> , as identified above) is used in place of at least a portion of fixed payment information (<i>e.g.</i> , the PAN or associated expiration or CVV) associated with said user-selectable issued payment account (<i>e.g.</i> , as identified above). <i>See supra</i> limitations 1[k] and claim 2.

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
63. The device of claim 62, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the payment authority information.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i> , as identified above) that is operable to cause the transmission (<i>e.g.</i> , via the NFC interface) of issued payment account information (<i>e.g.</i> , PAN or associated expiration date or CVV) and in response thereto, to receive the payment authority information (<i>e.g.</i> , as identified above). <i>See supra</i> limitation 1[c] and claim 3.
64. The device of claim 63, wherein the payment authority information comprises a static device account number.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, stores payment authority information that comprises a static device account number (<i>e.g.</i> , DPAN). <i>See supra</i> claims 3.
65. The device of claim 64, wherein the payment authority information further comprises a static device account expiration date.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, stores payment authority information that further comprises a static device account expiration date (<i>e.g.</i> , an expiration date associated with the DPAN). <i>See supra</i> claim 25.
66. The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch screen interface.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a user interface comprising a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is (<i>e.g.</i> , as identified above) operable to identify an authorized user by validating a valid user passcode input to the touch screen interface. <i>See supra</i> limitations 1[d], 1[f] (<i>e.g.</i> , PIN, pattern, passcode entry).
67. The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a user interface comprising a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor (<i>e.g.</i> , as identified above) is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response thereto. <i>See supra</i> limitations 1[d], 1[f] (<i>e.g.</i> , PIN, pattern, passcode entry).

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
display, and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response via said touch screen interface of the display.	
68. The device of claim 56, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user by biometric sensing of said user touch.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a user input device comprising a biometric sensor (<i>e.g.</i>, for fingerprint or wrist detection) operable to detect a user touch of said electronic device and wherein further the processor (<i>e.g.</i>, as identified above) is operable to identify an authorized user by biometric sensing of said user touch.</p> <p><i>See supra</i> limitations 1[d], 1[f] (<i>e.g.</i>, fingerprint or wrist detection).</p>
69. The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch screen interface.	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes user interface comprising a display and wherein said user input device comprises a touch screen interface of the display and wherein further the processor (<i>e.g.</i>, as identified above) is operable to identify an authorized user by biometric sensing of a user touch at the touch screen interface.</p> <p><i>See supra</i> limitations 1[d], 1[f] (<i>e.g.</i>, fingerprint).</p>
70. wherein said user input device comprises a touch input of the electronic device and wherein further the processor is operable to	<p>A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a user interface comprising a display and wherein the user input device comprises a touch input of the electronic device (<i>e.g.</i>, sensor for fingerprint or wrist detection) and wherein further the processor (<i>e.g.</i>, as identified above) is operable identify an authorized user by biometric recognition of a valid user identification via the touch input.</p>

Claim No.	Google Pay- and/or Google Wallet-enabled computing device
identify an authorized user by biometric recognition of a valid user identification via the touch input.	<i>See supra</i> limitations 1[d], 1[f] (<i>e.g.</i> , fingerprint, wrist detection).
72[a]: The device of claim 56, wherein the processor is operable to receive, via the user input device, a user-selection of said user-selectable issued payment account presented on the user interface, and	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i> , as identified above) that is operable to receive, via the user input device, a user-selection (<i>e.g.</i> , by confirming use of the default card or selecting a card other than the default) of said user-selectable issued payment account presented on the user interface (<i>e.g.</i> , as identified above). <i>See supra</i> limitation 1[h], 55[a].
72[b]: in response thereto, is further operable to select from memory the payment authority information corresponding to selected user-selectable issued payment account, and	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i> , as identified above) that is further operable to select from memory (<i>e.g.</i> , as identified above) the payment authority information (<i>e.g.</i> , the DPAN and associated expiration date and key(s)) corresponding to the selected user-selectable issued payment account. <i>See supra</i> limitation 1[h], 1[k], 55[b], claim 3.
72[c]: is further operable to use said payment information combination in place of at least a portion of fixed payment information associated with said selected user-selectable issued payment account.	A Google Pay- and/or Google Wallet-enabled computing device (See 1[Pre]), such as a smartphone or smartwatch, includes a processor (<i>e.g.</i> , as identified above) that is further operable to use said payment information combination (<i>e.g.</i> , as identified above) in place of at least a portion of fixed payment information (<i>e.g.</i> , PAN or associated expiration date or CVV) associated with said selected user-selectable issued payment account (<i>e.g.</i> , as identified above). <i>See supra</i> limitations 1[i], 1[k], 55[c], 4[a].

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 ’634 Patent and all processes employed by Defendant that practice the methods claimed by the ’634 Patent, consisting of at least products that support Google Pay (alone or with Google Wallet), including the following smartphones, smartwatches, and tablets¹, and other smartphones 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 system and NFC capability², and all variations (e.g., all colors and all storage capacities) of other smartphones that run on an Android operating system and have NFC capability.

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

¹ See, e.g., *Supported devices*, Google Pay (Jul. 19, 2024), <https://developers.google.com/pay/issuers/overview/supported-devices>.

² 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 A10e*	SM-A102U, SM-A102U1		BlackBerry Evolve X*	BBE100-1
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
Samsung Galaxy Z Fold*	SM-F900		BLU g44*	G1010WW

Product	Model Nos.		Product	Model Nos.
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
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

Product	Model Nos.		Product	Model Nos.
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
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

Product	Model Nos.		Product	Model Nos.
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
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

Product	Model Nos.		Product	Model Nos.
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
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

Product	Model Nos.		Product	Model Nos.
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
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

Product	Model Nos.		Product	Model Nos.
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
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,HTC6500LK
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

Product	Model Nos.		Product	Model Nos.
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
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_FLA-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

Product	Model Nos.		Product	Model Nos.
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
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

Product	Model Nos.		Product	Model Nos.
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
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

Product	Model Nos.		Product	Model Nos.
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
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
Ulefone Armor 25T Pro*	Ulefone Armor 25T Pro		Motorola Edge 30*	XT2203-1

Product	Model Nos.		Product	Model Nos.
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
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

Product	Model Nos.		Product	Model Nos.
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
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

Product	Model Nos.		Product	Model Nos.
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
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

Product	Model Nos.		Product	Model Nos.
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
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

Product	Model Nos.		Product	Model Nos.
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 and NFC capability.³

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

³ 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.
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
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 with NFC capability, and all variations (e.g., all sizes, all colors, all storage capacities, and connectivities) of other tablets that run on an Android operating system and have NFC capability.⁴

⁴ See, e.g., *Google Pixel Tablet technical specifications*, Google Pixel Tablet Help, <https://support.google.com/googlepixelttablet/answer/13555146?hl=en>.

CardWare Inc. v. Google LLC, Civil Action No. 7:24-cv-00278-DC-DTG
EXHIBIT F: Infringement Claim Chart for U.S. Patent No. 11,620,634 (“’634 Patent”)

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
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.