IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
MIDLAND/ODESSA DIVISION

CARDWARE INC.,	§	
	§	
Plaintiff	§	
	§	
v.	§	Civil Action No. 7:24-CV-00278-DC-DTG
	§	
GOOGLE LLC,	§	JURY TRIAL DEMANDED
	§	
Defendant.	§	
	§	
	§	

DEFENDANT GOOGLE LLC'S INVALIDITY CONTENTIONS

Pursuant to the Scheduling Order (Dkt. 48), and the Court's Standing Order Governing Patent Proceedings ("Standing Order"), Defendant Google LLC ("Google" or "Defendant"), hereby discloses these Supplemental Invalidity Contentions in the above-captioned case to CardWare Inc. ("CardWare" or "Plaintiff"). The Scheduling Order and Standing Order require:

> Defendant serves preliminary invalidity contentions in the form of (1) a chart setting forth where in the prior art references each element of the asserted claim(s) are found, (2) an identification of any limitations the Defendant contends are indefinite or lack written description under section 112, and (3) an identification of any claims the Defendant contends are directed to ineligible subject matter under section 101. Defendant shall also produce (1) all prior art referenced in the invalidity contentions, and (2) technical documents, including software where applicable, sufficient to show the operation of the accused product(s).

On February 13, 2025, CardWare served Google with Infringement Contentions alleging infringement of claims 1, 2, 4-23 of U.S. Patent No. 10,339,520 (the "'520 Patent"); claims 1-23 of U.S. Patent No. 10,810,579 (the "'579 Patent"); claims 1-30 of U.S. Patent No. 11,176,538 (the "'538 Patent"); and claims 1-3, 15-53, 55-70, and 72 of U.S. Patent No. 11,620,634 (the "'534 Patent") (collectively, the "Asserted Claims" of the "Asserted Patents"). *See* Plaintiff

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 1 of 156

CardWare Inc.'s Preliminary Contentions ("Infringement Contentions"). As discovery and possible third-party productions relevant to invalidity has not yet begun, Google reserves the right to supplement these Invalidity Contentions, including to add additional prior art, supporting evidence, and obviousness combinations.

As explained below and in the accompanying exhibits, incorporated by reference herein, Google contends that each of the claims asserted by CardWare is invalid under at least 35 U.S.C. §§ 102, 103, and/or 112 (pre-AIA and AIA). In its infringement contentions CardWare "contends that every asserted claim of each asserted patent is entitled to a priority date no later than March 15, 2013, the filing date of U.S. Provisional Application No. 61/794,891." Infringement Contentions at p. 2, which would mean that the Asserted Patents fall under pre- Leahy-Smith America Invents Act patent law ("pre-AIA") as their effective filing dates fall before March 16, 2013. Defendant does not concede that any or all of the Asserted Claims of the Asserted Patents are entitled to the alleged priority date or to pre-AIA treatment. However, most of the Asserted Claims lack written description support in *any* patent application, provisional or otherwise. CardWare is not entitled to the claimed priority date, then intervening prior art may exist, such as, for example, US Patent No. 11,164,176 to Ngo (the application for which was filed on December 19, 2014). Google reserves the right to supplement these invalidity contentions with such intervening prior art.

Defendant notes that it may challenge the priority date of the Asserted Claims of the Asserted Patents. Exemplary bases for challenging the claimed priority dates are set forth below.

Regarding the '520 patent, at least the following terms do not draw support from any incorporated provisional or non-provisional applications, and were added to the application for that issued as the '520 patent by a claim amendment dated December 11, 2018.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 2 of 156

- "wirelessly receiving a static device account number payment information for storage on the electronic device" (claim 1);
- "dynamically-generating a one-time limited-use numbers based on at least one of a set of information including: user-identifying information; user secrets; device information; device secrets; time; merchant; facility location; sequence count; payment information; account information; amount; and transaction information" (claim 1);
- "using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction" (claims 1, 10);
- "issuer provided payment information is communicated wirelessly; and, receiving wirelessly a static device account number payment information for storage on the electronic device" (claim 10);
- "recording a user selection from the user interface of the electronic device of a user selected account operation, wherein said user selected account operation is selected from a list of funds transfer operations" (claim 18); and
- "wherein said static and dynamic information is combined to perform the user selected ATM operation" (claim 18).

Thus, even assuming CardWare can prove they have written description support in any application, at least claims 1, 10, 18, and their dependents are entitled to a priority date no earlier than September 11, 2017, the filing date of patent application No. 15/701,261, which issued as the '520 patent.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 3 of 156

Regarding the ’579 Patent, at least the following terms do not draw support from any prior-filed provisional or non-provisional application:

- “receiving a request for a transaction payment at said electronic device via the NFC interface” (claim 1);
- “displaying, on the touch-screen display, images of: a card issuer payment method selection, including a last 4-digit partial number of a card issuer supplied account number of a payment card; a card logo; and other iconography of the payment card” (claim 1);
- “visually conveying a status of said transaction via a user-interface displayed on said touch-screen display” (claim 1);
- “receiving an input signal at an electronic device, the input signal corresponding to a request for payment of a transaction at said electronic device, via a recipient proximity communication request to an NFC interface of the electronic device” (claim 15);
- “displaying a summary of selectable payment account options at a touch-screen display user-interface of the electronic device” (claim 15);
- “displaying on said display at least one of a set of information comprising: transaction information; merchant information; a time; a location of the transaction; a payment bank logo; a card issuer icon; a payment card image; an amount” (claim 15);
- “receiving a user input providing for at least one transaction action, from a set of actions comprising: approving a transaction; denying a transaction; and adjusting a transaction” (claim 15);

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 4 of 156

- "an NFC interface operable to receive a transaction request when in proximity to an NFC recipient" (claim 19);
- "responsive to receiving an NFC transaction payment request, generating a limited-use payment information for use in place of card issuer payment information" (claim 19); and
- "wherein further the processor is operable to cause the display to visually convey a status of the transaction" (claim 19).

Claims 1 and 19 are original claims filed with the application, and claim 15 was amended on May 20, 2020, to include the features of a dependent claim. Thus, even assuming CardWare can prove they have written description support in any application, at least claims 1, 15, 19, and their dependents are entitled to a priority date no earlier than July 1, 2019 (the filing date of the application that issued as the '579 Patent).

Regarding the '538 Patent, at least the following terms do not draw support from any prior-filed provisional or non-provisional application:

- "receiving a request for a transaction payment at said electronic device via an NFC interface of the device" (claim 1);
- "displaying, on a display of the device, a transaction payment request and at least a portion of an original static issuer-supplied payment account information associated with a payment method, for a user selection in paying the payment request" (claim 1);
- "receiving information at said electronic device corresponding to a transaction status of the payment transaction, wherein such transaction status is at least partly dependent on validation of the transmitted complete device payment

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 5 of 156

information by a payment processor authority and a payment issuer authority" (claim 1);

- "visually conveying the transaction payment authorization status via a user-interface displayed on said display" (claim 1);
- "receiving an input signal at an electronic device, the input signal corresponding to a request for payment of an online payment transaction by said electronic device, via a wireless interface of the electronic device" (claim 19);
- "receiving a user input providing for at least one transaction authorization actions, from a set of actions including: approving a transaction, denying a transaction, selecting a user information, a payment amount adjustment, and selecting a transaction payment method" (claim 19); and
- "wherein further the processor is operable to receive an approval and a denial confirmation from an online payment facility of the complete device payment information, and cause the display to visually convey a status of the online purchase transaction" (claim 25).

Claims 1, 19, and 25 were added with the rest of the '538 Patent claims in a preliminary amendment on June 16, 2021. Thus, even assuming CardWare can prove they have written description support in any application, at least claims 1, 19, 25, and their dependents are entitled to a priority date no earlier than of October 20, 2020 (the filing date of the application that issued as the '538 Patent).

Regarding the '634 Patent, at least the following terms do not draw support from any prior-filed provisional or non-provisional application:

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 6 of 156

- "receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises:. . . a near field communications (NFC) interface coupled to the processor . . . receiving a payment request for the payment transaction at said electronic device;" (claim 1)
- "The method of claim 1, wherein the priming operation comprises bringing the electronic device within receiving proximity of an NFC recipient." (claim 7)
- "a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;" (claim 29)
- "a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction" (claim 39)
- "a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction" (claim 56)
- "displaying the status of said payment transaction via said touch-screen display." (claim 1)
- "displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account;" (claim 1)
- "displaying the status of said payment transaction via said touch-screen display" (claim 1)

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 7 of 156

- "visually presenting a request for user approval of the payment transaction via touch input at said electronic device" (claim 16)
- "wherein the touch-screen display is operable to display as indication of said status information." (claim 29)
- "wherein the user interface is operable to provide an indication of the transaction status information." (claim 56)
- "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." (claim 72)

Claims 1, 29, 16, 39, 56, and 72 were added with the rest of the '634 Patent claims in a preliminary amendment on April 22, 2022. Thus, even assuming CardWare can prove they have written description support in any application, at least claims 1, 29, 16, 39, 56, and 72 and their dependents are entitled to a priority date no earlier than of November 16,2021 (the filing date of the application that issued as the '634 Patent).

Defendant reserves the right to challenge the alleged priority date for any of the Asserted Claims and present herein prior art references that are applicable to pre-AIA and AIA treatment for certain Asserted Claims.

Likewise, should any application for one of the Asserted Patents contain or have contained at any time, a claim having an effective filing date of March 16, 2013, or later, or a specific reference under 35 U.S.C. §§ 120, 121, or 365(c), to any patent or application that contains or contained at any time such a claim, the AIA's provisions would apply to every claim to have issued from such an application. *See* AIA § 3(n)(1). As such, these invalidity contentions and the attached exhibits address invalidity and ineligibility under both pre-AIA and AIA patent

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 8 of 156

law. Unless stated otherwise, each citation to any of 35 U.S.C. section 101, 102, 103, and/or 112, shall be interpreted as referring to both the pre-AIA and AIA section(s).

For purposes of these Invalidity Contentions, Defendant identifies prior art references and provides element-by-element claim charts based, in part, on the implicit claim constructions advanced by Plaintiff in its Infringement Contentions. The citation of prior art herein and in the accompanying exhibits is not intended to reflect Defendant's claim construction positions, which will be disclosed in due course in accordance with the Scheduling Order (Dkt. 48), and may instead reflect Plaintiff's implicit (and potentially erroneous) claim constructions based on its Infringement Contentions. Nothing stated herein shall be treated as an admission or suggestion that Defendant agrees with Plaintiff regarding either the scope of any of the Asserted Claims or the claim constructions advanced in the Infringement Contentions. Moreover, nothing in these Invalidity Contentions shall be treated as an admission that Defendant's accused technology meets any limitations of the claims.

Defendant's Invalidity Contentions herein reflect Defendant's knowledge as of this early date in the present action. Defendant reserves the right, to the extent permitted by the Court and the applicable statutes and rules, to modify and/or supplement their Invalidity Contentions in response to becoming aware of additional prior art or information regarding prior art, including internal information regarding Google Wallet, any modification or supplementation of Plaintiff's Infringement Contentions, any claim construction by the Court, or as otherwise may be appropriate.

Defendant's Exhibits attached hereto cite to particular teachings and disclosures of the prior art as applied to features of the Asserted Claims. However, persons having ordinary skill in the art ("POSITA") generally view a prior disclosure in its entirety (e.g., view specific

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 9 of 156

disclosures in the context of the general disclosures), in the context of other publications, literature, products, and understanding and knowledge of such a person. As such, the cited portions of prior art identified herein are exemplary only. Defendant may rely on the entirety of the prior art references listed herein, including un-cited portions of those prior art references, and on other publications, systems, evidence, and expert testimony shedding light on those prior art references or the state of the art in general, including as aids in understanding and interpreting the cited portions, as providing context thereto, and as additional evidence that the prior art discloses a claim limitation.

Defendant may also rely on documents, systems, products, testimony, and other evidence to establish bases for, and motivations to make, combinations of or modifications to certain cited references that render the Asserted Claims obvious. Defendant may rely upon corroborating documents, products, testimony, and other evidence, including confidential and non-confidential Google materials regarding Google Wallet, materials obtained through further discovery, investigation, and third-party discovery of the prior art identified herein that describes the invalidating features identified in these contentions; evidence of the state of the art in the relevant time period (irrespective of whether such references themselves qualify as prior art to the Asserted Patents), including prior art listed on the face of the Asserted Patents and/or disclosed in the specification(s) (i.e., applicant admitted prior art); and/or expert testimony to provide context to or aid in understanding the cited portions of the identified prior art.

The references discussed in the Exhibits hereto disclose the elements of the Asserted Claims explicitly, inherently, and/or in combination with themselves or the knowledge of one skilled in the art at the time of filing. The references also may be relied upon to show the state of the art in the relevant time frame. To the extent the attached claim charts cite to a reference for

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 10 of 156

each element or limitation of an Asserted Claim, Defendant contends that such reference anticipates that claim or renders it obvious, either alone or in combination with other references. To the extent suggested obviousness combinations are included in the attached exhibits, they are provided in the alternative to Defendant's anticipation contentions and are not to be construed to suggest that any reference included in the combinations is not by itself anticipatory.

Pursuant to the Scheduling Order and the Standing Order, Defendant produces prior art referenced in the invalidity contentions, and technical documents, including software, sufficient to show the operation of the accused product(s) as identified by Plaintiff in its Infringement Contentions. Defendant will further supplement its document production should it later find additional prior art or obtain translations of previously produced art. To the extent any further proof is required as to internal functionality of Google Wallet as it operated prior on and before March 2013 to support Google's claim of invalidity, Google will produce during the course of case additional documents, source code, and other evidence under the Protective Order describing the operation of Google Wallet on and before March, 2013. This will include depositions and other discovery about Google Wallet taken in other actions regarding the Asserted Patents, including, but not limited to, CardWare's action against Samsung. Google will supplement these invalidity contentions with such information in accordance with the Scheduling Order and Standing Order. Much of the art identified in the attached Exhibits reflects common knowledge and the state of the art near the filing date of the Asserted Patent.

Each of the Asserted Claims[1] of the Asserted Patents is anticipated by and/or obvious in view of one or more items of prior art identified herein, alone or in combination. Specific

[1] For reasons analogous to those identified herein, Defendant contends all *non-asserted* claims of the Asserted Patent are invalid as anticipated and/or obvious in view of the prior art, patent ineligible subject matter, indefinite, not enabled, or not supported by the written description.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 11 of 156

examples of this anticipation and obviousness, along with the motivation to combine the selected prior art, are set forth in the attached Claim Charts (Exhibits A-01 through D-42) and Combinations Exhibit (Ex. I). The identification of obviousness combinations is not intended to be exhaustive, as there are many possible combinations of the references that one of ordinary skill in the art would have been motivated to make, and it is not practical to provide details of all such possible combinations, particularly at this early stage of the case.

The Scheduling Order (Dkt. 48) and the Standing Order contemplate that these Invalidity Contentions would be prepared and served in response to Plaintiff's Infringement Contentions. Defendant reserves the right to amend these Invalidity Contentions should Plaintiff amend its Infringement Contentions or its implicit claim constructions. Defendant also reserves the right to modify, amend, and/or supplement its Invalidity Contentions in light of positions that Plaintiff or its expert witnesses may assert concerning claim construction, infringement, and/or invalidity issues.[2] Defendant also reserves the right to modify, amend, and/or supplement its Invalidity Contentions in view of additional evidence, including third party evidence, produced in this matter in accordance with the Scheduling Order and Standing Order and/or as that information is produced in the ordinary course of discovery.

I. BACKGROUND AND STATE OF THE ART / SYSTEM PRIOR ART

A. Contactless Payments and Key Fobs

Contactless payment has been known since at least 1997. Exxon/Mobile, McDonalds and Bank of America launched contactless payment systems in the late 1990s and early 2000s. http://usatoday30.usatoday.com/tech/news/2001-05-29-mcdonalds-e-payments.htm,

[2] Defendant identifies and may rely upon references and arguments made in the following *inter partes* review petitions and related proceeding papers: IPR2023-00196, IPR2023-00210, IPR2023-00211, IPR2023-00219. Further, defendant may rely upon any *inter partes* or other ex parte proceeding brought against any Asserted Patent in the future.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 12 of 156

https://www.secureidnews.com/news-item/freedompay-makes-waves-in-contactless-payment/.

Exxon's system, known as SpeedPass, used RFID technology to transmit payment related data wirelessly from a key fob to a payment terminal. The key fobs included no printed user or account identifying information thereon:

Visa (discussed further below) provided key fobs to users as early as 2007 that were capable of facilitating contactless payments at Visa PayPass point of sale terminals:

> SAN FRANCISCO, September 26, 2007–Visa announced today the availability of the Visa Micro Tag, a new key fob payment device embedded with Visa payWave, Visa's contactless technology feature. The Visa Micro Tag is designed to easily attach to a key ring, and allows cardholders to pay by simply waving their Visa Micro Tag in front of a contactless payment terminal without the need to physically swipe or insert the device into a point-of-sale terminal.
>
> The Visa Micro Tag allows financial institutions to offer cardholders a companion device to an existing credit, debit or prepaid account. Designed to be small and durable, the Visa Micro Tag makes paying for purchases faster and more convenient.
>
> Visa Micro Tags display the Visa Brand Mark and contactless indicator. ***A Visa account number is not required to be embossed or printed on the device, providing an additional layer of security for consumers carrying a Visa Micro Tag in visible ways, such as on a keychain*** . . . .

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 13 of 156

> Cardholders making purchases with Visa payWave-enabled products enjoy additional layers of security because the payment device never leaves the customer's hand, can only be read at extremely close proximity to a reader, and submits a unique digital watermark to the Visa payment network for each transaction.

Visa Unveils New Contactless Payment Device – Visa Micro Tag, https://www.securetechalliance.org/visa-unveils-new-contactless-payment-device-visa-micro-tag/ (September 26, 2007) (emphasis added). *And see* Visa Pay Wave, which is discussed further below. MasterCard offered a similar key fob for use with MasterCard PayPass contactless terminals:

> MasterCard PayPass ® is a "contactless" payment solution that enables consumers simply to tap or wave their payment card or other payment device, such as a phone, ***key fob*** or wristband, on a specially equipped terminal.

MASTERCARD INC, FORM 10-K, (Annual Report), Filed 02/28/07 for the Period Ending 12/31/06, https://s25.q4cdn.com/479285134/files/doc_financials/2006/q4/658dd46b-769b-4c17-9e23-8ae0073ddc96.pdf, p. 14 (emphasis added). *See also*, KickStarter, *Simplify, Organize and Pay with Loop*; https://www.kickstarter.com/projects/loop/pay-with-loop:

Fob going into the Bumper.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 14 of 156

B. The PCI DSS, EMV and ISO Standards

By 2004, the Payment Card Industry Data Security Standard (PCI DSS) and the EMV (EuroPay, Mastercard, Visa) standards had been established. PCI DSS was focused on increasing controls around cardholder data to reduce credit card fraud. EMV concerned smart cards (chip cards), a/k/a integrated circuit (IC) cards, capable of storing data on integrated circuit chips embedded in the card. PCI DSS was implemented in the EMV environment to enhance credit card transaction security and fraud-reduction:

> This document compares and contrasts the current fraud-reduction capabilities of EMV within the security framework of the Payment Card Industry Data Security Standard (PCI DSS) and examines the rationale for why it remains necessary to implement PCI DSS in the EMV environments that exist today.

pci_dss_emv.pdf (pcisecuritystandards.org), https://listings.pcisecuritystandards.org/pdfs/pci_dss_emv.pdf (*PCI DSS Applicability in an EMV Environment, A Guidance Document,* Version 1, Release date: 5 October 2010). The ISO published standards on credit card numbering and contactless card structure, technology, operation and protocols well before 2013.

The original RFID protocol for contactless cards was ISO14443, including 14443-1, 14443-2, 14443-3, 14443-4. 14443-4[3], the latter being most relevant to programmers. (ISO15693 was for vicinity cards, like office access cards). ISO 14443 included a peer-to-peer mode where two NFC devices can talk to each other and engage in data exchange. An NFC specific "NFC forum" was created from ISO14443. NFC is also based on RFID. The NFC forum standardized the RFID/NFC protocol. in ISO18092 aka "NFCIP-1." This allowed implementation of RFID on

[3] Standing Document 1 (SD1): WG8 Projects (archive.org), https://web.archive.org/web/20110927044225/http://wg8.de/sd1.html#14443 (Sept. 27, 2011) (4 parts and related Amendments (AMx)).

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 15 of 156

mobile phones. ISO18092 supplemented and enhanced the 14443-4 command set with new command sets. The NFC Forum and EMVCo worked together to merge NFC technology with payment technology. *See EMV Byte 7 - Contactless - An Overview*, https://www.youtube.com/watch?v=2Zosb4hcbXw&list=PLq6InkZqS2g0ojgmtWiV8mXdEEuDXRKHo&index=7.

Other relevant standards include ISO/IEC7812 (Card issuers numbering) and ISO/IEC 7816 (smartcard hardware, commands, command management). A discussion of relevant ISO and EMV standards can be found at *29C3: A Rambling Walk Through an EMV Transaction (EN) - YouTube*, https://www.youtube.com/watch?v=VdNm9JJmCzg (December 30, 2012).

C. The Early History of NFC Contactless Payments for Smartphones

NFC was developed in the mid-2000s. https://web.archive.org/web/20110628203003/http://www.nfc-forum.org/news/pr/view?item_key=d8968a33b4812e2509e5b74247d1366dc8ef91d8; ISO/IEC14443. Samsung began integrating NFC technologies into its phones for contactless payments as early as 2007. *INSIDE Contactless to Equip KTFMobile Payment Project Mobile Phones; Korean Manufacturer Confirms INSIDE's NFC Maturity by Embedding MicroRead into LG Electronics and Samsung Electronics Mobile Phones for its Mobile Payment Project*, Business Wire, July 16, 2007, ("On a first basis, 200 MicroRead chips have been delivered to LG Electronics and Samsung Electronics to equip both manufacturers' NFC phones."); *New NFC-Enabled Phones to Hit Europe*, ReadWriteWeb, February 18, 2011 (Samsung Wave 578, Samsung's Galaxy S II). Samsung designed and manufactured its own NFC chips for use in its mobile devices. *Samsung cooks up its own NFC module, destined for the Nexus S?*, Engadget, December 1, 2010 ("Samsung Electronics Co., Ltd., a world leader in advanced semiconductor

solutions, announced today a new near field communications (NFC) chip with embedded flash memory.").

The Samsung Star included NFC capabilities for mobile contactless payments in early 2010 for mobile payments use. *Mobile Contactless Payments Trialed Live at Mobile World Congress 2010; GSMA, Samsung, Telefónica and Visa, with Giesecke & Devrient, Ingenico, ITN International and La Caixa, collaborate across industries to give Congress attendees an opportunity to experience NFC*, Business Wire, February 15, 2010 ("The participating companies have provided more than 400 NFC handsets to guests for use at the Congress. The Samsung Star NFC handsets contain Telefónica SIM cards from O2 pre-loaded with (EURO) 60 airtime credit as well as a La Caixa Visa Mobile Payment Application. Participants can use their NFC phones to pay for food and drink up to a value of (EURO) 75 at over 30 merchant locations around the Congress. Samsung Electronics Co. Ltd. provided the NFC-enabled Samsung Star handsets and offered technical support to ensure the stability of the very first NFC payment trial.").[4]

Another early smartphone to incorporate NFC was the joint Samsung/Google Nexus S in 2010. https://www.gsmarena.com/samsung_google_nexus_s-3620.php; https://web.archive.org/web/20131005041615/http://blogs.computerworld.com/17359/eric_schmidt_android_gingerbread; https://www.androidcentral.com/gingerbread-feature-near-field-communication. That phone was launched as a further stepping stone to mobile payment capable devices. *Google unveils first Android NFC phone — but Nexus S is limited to tag reading only*

[4] *See also* "La Caixa" 2010 Annual Report, p. 68 ("Jointly with Movistar and Visa, the first experiment in Spain was conducted as regards payments made via mobile phones with NFC technology."). https://fundacionlacaixa.org/documents/10280/944807/informe_anual_2010_en.pdf.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 17 of 156

for now • NFCW; https://www.nfcw.com/2010/12/07/35385/google-unveils-first-android-nfc-phone-but-nexus-s-is-limited-to-tag-reading-only-for-now/.[5] *Samsung and Google to Deliver Nexus S, the First Mobile Phone in the World Powered by Android 2.3; Nexus S offers the latest version of the Android platform, Gingerbread, 4" Super AMOLED touch screen with curved design, Near Field Communication (NFC), front and rear-facing cameras and 1GHz application processor*. (December 6, 2010, Business Wire). In 2011 Samsung launched mobile devices capable of mobile contactless payments in France in 2011. https://www.01net.com/actualites/nice-premiere-ville-a-passer-au-paiement-sans-contact-516923.html; https://www.nfcw.com/2011/02/14/35968/orange-to-offer-samsung-wave-578-nfc-across-europe-%e2%80%94-but-not-the-uk/; https://www.nfcw.com/2010/12/16/35498/orange-to-roll-out-nfc-services-across-europe-in-2011/.

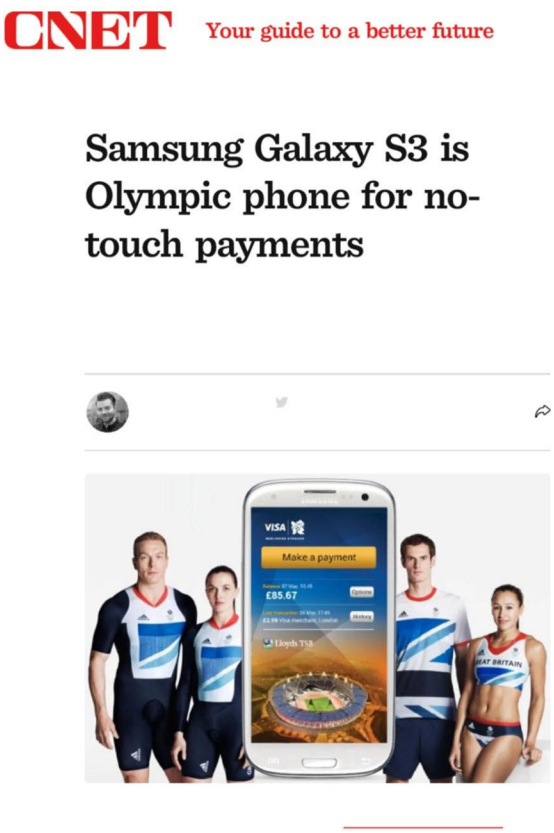
The Samsung Nexus S 4G sold through Sprint allowed mobile payments via Google Wallet in 2011 in the United States.[6] *Google Wallet Mobile Payments Coming to New York, San Francisco; Google Wallet will launch this summer to enable consumers to pay for goods by tapping their Samsung Nexus 2 4G Android phones at NFC-fitted sales terminals at Subway, Macy's and other retailers*, eWeek.com, May 26, 2011 ("Users tap their phones to a point-of-sale system made to pay for goods. The idea is that users needn't carry a wallet stuffed with credit cards, loyalty cards and gift cards. This is enabled by NFC technology, a short-range wireless technology that allows communications between sensors brought within close

[5] Samsung also incorporated NFC into smartwatches. *Samsung to Unveil NFC Smartwatch - Has Wrist-Payments' Time Come?*, Payments Source, September 2, 2013, Copyright 2013 SourceMedia LLC d/b/a Arizent ("The upcoming Samsung Galaxy Gear smartwatch will have a Near Field Communication chip in it, according to reports. But only time will tell if Samsung plans to use the chip for payments.").

[6] Google Wallet is discussed further below.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 18 of 156

proximity."). Further, in 2012, Samsung and Visa announced a partnership for providing an NFC mobile payment solution at the 2012 Olympics in London on the Galaxy S III:



Samsung Galaxy S3 is Olympic phone for no-touch payments - CNET, https://www.cnet.com/tech/mobile/samsung-galaxy-s3-is-olympic-phone-for-no-touch-payments/; *Samsung and Visa team up for NFC mobile payments at London 2012 Olympics*, Boy Genius Report, March 31, 2011. ("Here's how it will work: When you're ready to make a purchase, you'll just have to open the Visa application on your phone and then hold it in front of a special contactless reader. There are over 60,000 contactless readers already in London, and Visa says its continuing to work with banks and retailers to increase its NFC foundation. The NFC-enabled phone, with its Visa SIM card, will first be available to Samsung and Visa sponsored athletes, and it will also be available to consumers through mobile operators.");

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 19 of 156

Samsung and Visa Showcase Mobile Payments at the London 2012 Olympic and Paralympic Games; NFC technology takes a leap forward in the form of the Samsung GALAXY S III with Visa mobile contactless payments, Business Wire, May 9, 2012.

In early 2012, Visa certified Samsung devices for use with its PayWave NFC contactless payment service. *Visa Certifies BlackBerry, Samsung And LG Phones For PayWave NFC Payments, Payments Source*, January 10, 2012 ("The card brand has added six new mobile devices—the Samsung Galaxy SII, LG Optimus NET NFC, BlackBerry Bold 9900, BlackBerry Bold 9790, BlackBerry Curve 9360 and BlackBerry Curve—to its list of payWave- compliant products available for commercial deployment by financial institutions, the card brand announced Jan. 10. . . . 'In addition to issuing plastic magnetic stripe or chip-enabled payment cards, financial institutions can now consider offering their accountholders a way to transform their smartphones into fully functional mobile payment devices.'").

By mid-2012, many other smartphones by various manufacturers (LG, Apple, Blackberry, etc.) included NFC technology for present or planned use for mobile payments. *NFC Focus: Which Smartphones Have NFC?*, International Business Times News, August 9, 2012.

On February 25, 2013, Samsung and Visa announced that Visa's NFC payment system (PayWave) would be built into all Samsung smartphones. *Samsung and Visa Take NFC Mobile Payments Global*, Mashable.com, February 25, 2013 ("Your next Galaxy S smartphone might also be your Visa card. That's because Visa and Samsung announced Monday that Visa's NFC payment system will be built into all future Samsung smartphones.").

Similarly, MasterCard certified the Samsung Wave Y, Samsung Galaxy mini 2, Samsung Galaxy S Advance, and Samsung Galaxy Nexus (GT-i9250) for NFC contactless payments with MasterCard's PayPass in May, 2012. *MasterCard Approves NFC Phones from HTC, Intel, LG*

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 20 of 156

Electronics, Nokia, RIM, Samsung Electronics and Sony, Professional Services Close-Up, May 10, 2012. Samsung further collaborated with MasterCard to launch NFC mobile payments using Samsung GALAXY S42 (i9505 and i9507) smartphones in Australia in 2013 using MasterCard's PayPass service. *Commbank, Mastercard and Samsung collaborate to launch NFC payment service*, MarketLine NewsWire (Formerly Datamonitor), December 13, 2013 ("The CommBank offering has been made possible by a convergence of hardware, software and mobile banking technologies, which leverage Mobile MasterCard PayPass technology and Samsung's globalNFC payment infrastructure."). Similar efforts were made by Samsung in Japan (*Samsung partners with FeliCa for Japanese NFC solutions, unveils 2012 Olympics' mobile payment app with Visa*, Engadget, February 24, 2012 Friday 7:49 PM EST), in Spain (*Telefonica, Samsung to Pilot SIM-Based NFC Payment Solution in Spain*, IHS Global Insight, February 15, 2010), and in the Czech Republic (*'Telefonica O2 Czech Republic prepares NFC payments'*, DmEurope, March 25, 2011).

The above efforts by Samsung, Google, and other mobile phone providers variously used SIM as the secure element as well as an embedded secure element. *Samsung's New Secu-NFC Chip Enables Secure Mobile Payment by Enhancing NFC with Security Features*, Plus NEWS, November 30, 2011 ("Samsung Electronics Co., Ltd., a world leader in advanced semiconductor solutions, announced today its new system-in-package (SIP) near field communications (NFC) chip, the SENHRN1. The new Secu-NFC chip combines a NFC controller and a secure element storing personal information and security keys with advanced encryption technologies, a prerequisite for reliable and efficient mobile payment on NFC-enabled mobile devices."); *New Samsung Galaxy S4 phone includes NFC, innovative barcode technology; New Samsung smartphone adds a number of features that may spur mobile payment adoption*, Mobile

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 21 of 156

Payments Today, March 15, 2013 ("As expected, the S4 includes NFC capabilities and will be the first Samsung device to come pre-loaded with the Visa payWave applet in the embedded secure element. (The SE is where the phone securely stores payment account information.) The S4 will also support SIM-based secure elements as well.").

D. Visa PayWave

Visa PayWave launched on or around 2008.

Visa PayWave allowed users to wave their credit cards at a contactless terminal to make credit card payments, similar to MasterCard PayPass. https://web.archive.org/web/20130115100859/http://usa.visa.com/merchants/payment_technologies/paywave.html. Visa PayWave utilized NFC technology and known credit card cryptogram technology of the time:

Visa Paywave used secure element cryptographic processors. *See, e.g.*, *Visa Recommended Practices for EMV Chip Implementation in the U.S.*, https://technologypartner.visa.com/Download.aspx?id=153 (July 11, 2012). An NFC-capable smartphone using Google Wallet was also capable of contactless transactions at Visa PayWave

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 22 of 156

terminals. *Visa and Google Sign Licensing Deal to Boost Mobile Payment Adoption*, https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.8936.html (Sept. 19, 2011).

Visa filed patent applications regarding the use of cryptograms and substitute credit card numbers for contactless transactions. *See, e.g.*, U.S. Patent Application Publication No. US2008/0319905, titled *Secure Mobile Payment System* and U.S. Patent Application Publication No. 2015/0178724, titled *Limited-Use Keys and Cryptograms.*

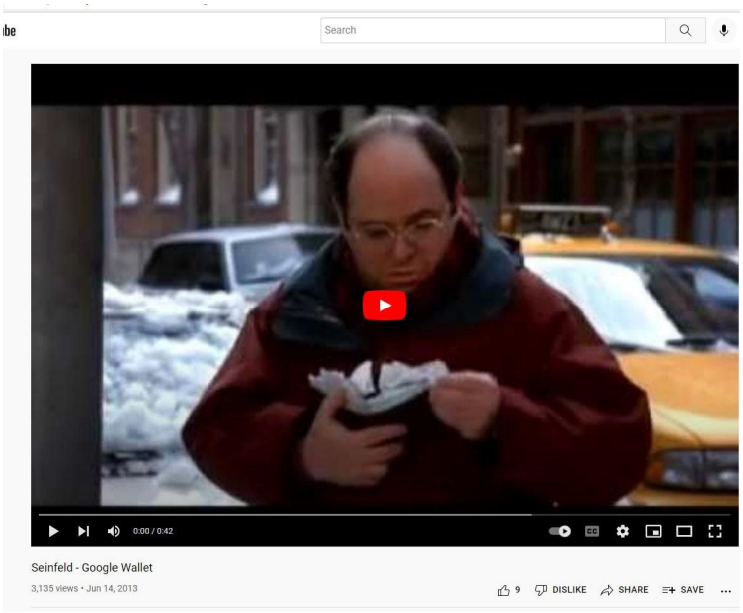
E. American Express Pay

It was known at the time that American Express operated as a closed-loop payment card system that operated its credit and charge card network, as well as acted as the card issuer and merchant acquirer for its cards. Thus, American Express maintained direct relationships with its cardholders and accepting merchants by providing issuing services to cardholders, acquiring and processing services to merchants, and network services to both sides of the platform in order to facilitate the use and acceptance of its payment cards.

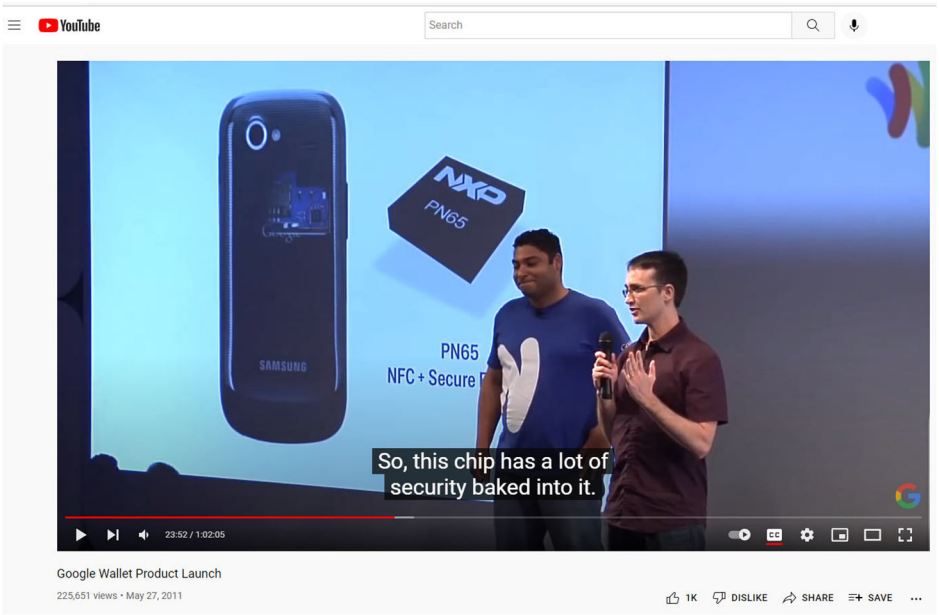
F. Google Wallet

As noted above, Google Wallet launched in 2011 and was co-founded by Jonathan Wall. *Google Wallet Product Launch* - YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0 (May 27, 2011); *Google Wallet Overview – YouTube*, https://www.youtube.com/watch?v=VuFVsaFCzsw (August 1, 2012). It was commercialized and well known in the United States:

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 23 of 156



Seinfeld - Google Wallet - YouTube, https://www.youtube.com/watch?v=baaCvgTRYsU (June 14, 2013); *Google Wallet mobile payments system launched to public*, The Guardian, https://www.theguardian.com/technology/2011/sep/19/google-wallet-available-public (Sept. 19, 2011). Google Wallet used the secure element of the device to store card credentials to facilitate contactless mobile payments:



Google Wallet Product Launch - YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0 at 19:53, 23:52 (May 27, 2011). Security and the prevention of credit card transaction fraud was a key motivator in the design of Google Wallet, as it was with all contactless transaction systems. https://listings.pcisecuritystandards.org/pdfs/pci_dss_emv.pdf (*PCI DSS Applicability in an EMV Environment, A Guidance Document,* Version 1, Release date: 5 October 2010). Google Wallet used NFC as the communication protocol between the mobile device running Google Wallet and the card reader terminal.[78]

Google Wallet utilized the PAN of the card and some elements of "mag-stripe mode" for payment transaction:

> For compatibility reasons, EMV payment applications contain data equivalent to that found on the magnetic stripe of physical cards. ***This includes account number (PAN), expiry date, service code and card holder name.*** EMV- compatible POS terminals are required to support transactions based on this data only ('Mag-stripe mode'), so some of it could be available on Google Wallet as well. Executing the needed READ RECORD commands shows that it is indeed found on the SE, and both MasterCard applications are linked to the same mag- stripe data. The data is as usual in TLV format, and relevant tags and format are defined in EMV Book C-2. When parsed it looks like this for the Google prepaid card (slightly masked):
>
> Track 2 Equivalent Data:
> ***Primary Account Number (PAN) - 5430320XXXXXXXX0***
> Major Industry Identifier = 5 (Banking and financial)
> Issuer Identifier Number: 543032 (Mastercard, UNITED STATES OF AMERICA)
> Account Number: XXXXXXXX
> Check Digit: 0 (Valid)
> Expiration Date: Sun Apr 30 00:00:00 GMT+09:00 2017
> Service Code - 101:
> 1 : Interchange Rule - International interchange OK
> 0 : Authorisation Processing - Normal
> 1 : Range of Services - No restrictions

---

[7] *Google built NFC into Android by 2011. Google I/O 2011: How to NFC* - YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q.

[8] *See VeriFone Partners with Google and Leading Retailers to Power NFC-based Mobile Payments Prominent Retail Brands Coast to Coast Embrace Mobile Payments Trial to Provide Greater Consumer Value* SAN JOSE, Calif. - May 26, 2011.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 25 of 156

Discretionary Data: 0060000000000

Exploring Google Wallet using the secure element interface (nelenkov.blogspot.com), https://nelenkov.blogspot.com/2012/08/exploring-google-wallet-using-secure.html (Aug. 27, 2012) (emphasis added). In other respects, including the use of cryptograms and the Application Transaction Counter (ATC), it followed existing EMV standards:

> As you can see, it does not include the card holder name, but all the other information is available, ***as per the EMV standard***. We even get the 'transaction in progress' animation on screen while our reader is communicating with Google Wallet. We can also get the PIN try counter (set to 0, in this case meaning disabled), and a transaction log in the format shown below. We can't verify if the transaction log is used though, since Google Wallet, like a lot of the newer Google services, happens to be limited to the US.
>
> Transaction Log:
> Log Format:
> ***Cryptogram Information Data (1 byte)*** Amount, Authorised (Numeric) (6 bytes) Transaction Currency Code (2 bytes) Transaction Date (3 bytes)
> ***Application Transaction Counter (ATC) (2 bytes)***

Exploring Google Wallet using the secure element interface (nelenkov.blogspot.com), https://nelenkov.blogspot.com/2012/08/exploring-google-wallet-using-secure.html (August 27, 2012) (emphasis added). *And see*,

> Google announced Google Wallet in May 2011, with general availability planned during October 2011, in New York and San Francisco. Using the Google wallet, consumers can use a Sprint NFC-enabled phone and a MasterCard PayPass or Google prepaid card to pay for purchases at merchants who accept MasterCard PayPass. Google is also working with POS system companies and top retail brands to allow consumers to be able to redeem promotions, and earn loyalty points. . . . .
>
> NFC mobile contactless payment transactions between a mobile phone and a POS terminal use the standard ISO/IEC 14443 communication protocol currently used by contactless EMV credit and debit cards. NFC-enabled mobile phones will be able carry one or more payment applications and accounts from different issuers; the NFC specifications don't define or specify the payment application. NFC payment applications will follow the payment

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 26 of 156

> brand specifications for the region of the world where they are being issued. An EMV payment application and account would be loaded in the NFC-enabled phone and used with compatible EMV POS terminals.

The Mobile Payments and NFC Landscape: A U.S. Perspective, Smart Card Alliance Payments Council White Paper Publication Date: September 2011, Publication Number: PC-11002, p. 12-13, 27-28, https://www.securetechalliance.org/resources/pdf/Mobile_Payments_White_Paper_091611.pdf.

Google Wallet's contactless mag-stripe mode operation included the creation of cryptographic checksums, application transaction counters and dynamically generated CVC3 numbers:

> The credit card applet is based on the *EMV Contactless Specifications for Payment Systems* and is a MasterCard PayPass card. It supports Mag-Stripe mode with dynamic CVC3 (card verification code) and requires online transactions. Full EMV mode is not supported. Also there is no cardholder verification. Even though, PIN-based cardholder verification would significantly complicate relay attacks or would even render them impossible if the attacker is unable to "guess" the PIN.
>
> A typical Mag-Stripe mode transaction with the Google Prepaid card consists of the following command sequence (cf. [1] for a detailed analysis of a Mag-Stripe transaction):
>
> 9) POS → Card: 80 2A 8E80 04 **nnnnnnnn** 00: Compute cryptographic checksum for a given unpredictable number **nnnnnnnn**.
> 10) Card → POS: 77 0F 9F61 02 **zzzz** 9F60 02 **yyyy** 9F36 02 **xxxx**: Respond with the application transaction counter (**xxxx**) and dynamically generated CVC3 for track 1 (**yyyy**) and track 2 (**zzzz**).
>
> Most of the data exchanged in a Mag-Stripe transaction is static for all transactions (e.g. the Mag-Stripe data). *Compute cryptographic checksum* (9 and 10) is the only APDU command/response pair that contains dynamically generated data that differs for each transaction: the unpredictable number generated by the POS, and the transaction counter and CVC3 codes generated by the card. Each *compute cryptographic checksum* command that is sent to the card must be preceded by a fresh *get processing options* (5 and 6) command. Thus, the minimum sequence for generating a dynamic CVC3 is

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 27 of 156

Applying Relay Attacks to Google Wallet, Roland et al., p. 3;

The Google Prepaid Card uses the *EMV Contactless Specifications for Payment Systems* and is a MasterCard PayPass card. It only supports the Mag-Stripe mode with dynamic CVC3 (card verification code) and online transactions[4].

Table 9: Compute Cryptographic Checksum: C-APDU

CLA	80	Proprietary class
INS	2A	Compute Cryptographic Checksum
P1	8E	
P2	80	
Lc	04	
DATA	00 00 00 80	Unpredictable number (UN)
Le	00	

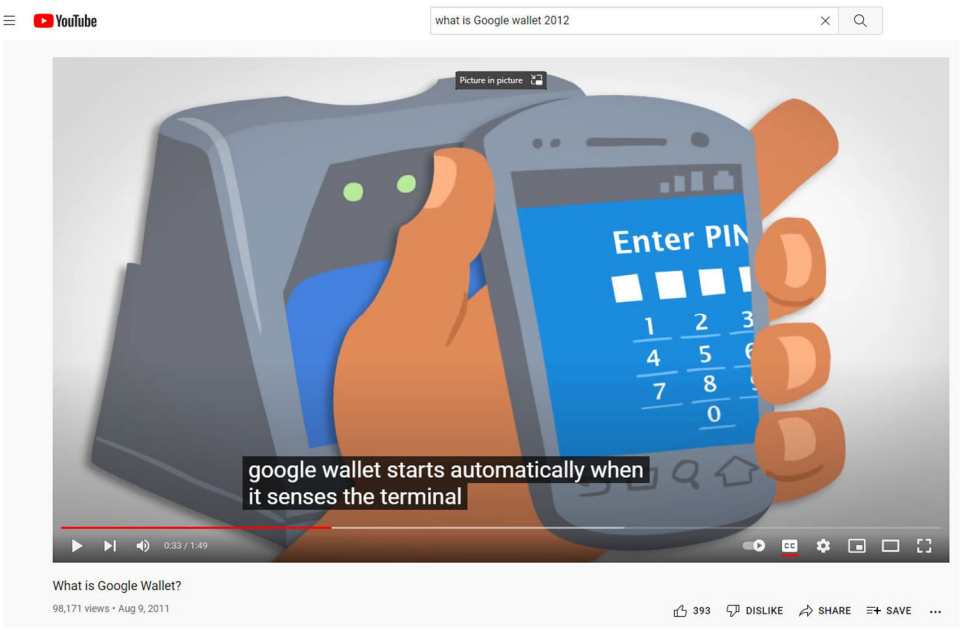
Applying recent secure element relay attack scenarios to the real world: Google Wallet Relay Attack, Roland, p. 12, 27.

Google Wallet also used PIN entry by a user for secure access confirmation:

> The controller applet securely stores Google Wallet state and event log data, but most importantly, it enables or disables contactless payment functionality when you unlock the Wallet app by entering your PIN. The latest version seems to have the ability to store and verify a PIN securely (inside the SE), however it does not appear it is actually used by the app yet, since the Wallet Cracker can still recover the PIN on a rooted phone. This implies that the PIN hash is still stored in the app's local database.

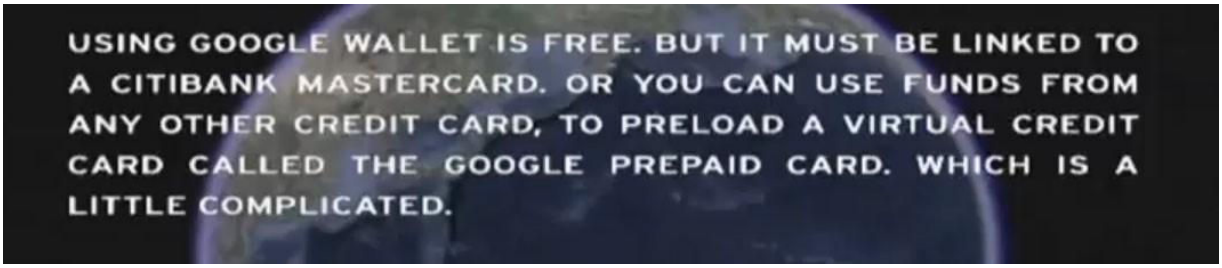
Exploring Google Wallet using the secure element interface (nelenkov.blogspot.com), https://nelenkov.blogspot.com/2012/08/exploring-google-wallet-using-secure.html (August 27, 2012). Google Wallet activated and deactivated NFC functionality on the mobile device based on proximity of the device to the NFC POS terminal:

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 28 of 156



What is Google Wallet, Aug 9, 2011, https://www.youtube.com/watch?v=iuvyN4iZiP8 at 0:32.

While Google Wallet transmitted a PAN from the mobile device to the NFC merchant pay terminal, that PAN could act as a substitute for another card. Google Wallet was launched with MasterCard and CitiBank and initially required use of a Citibank-issued credit card or Citibank-related Google debit card. The Google Debit card could be funded using any credit card, thus operating as a virtual credit card.



Technology: Google Wallet | The New York Times - YouTube, https://www.youtube.com/watch?v=l8JOT6ban7o (Sept. 23, 2011). Later, in 2012, other

preexisting credit cards of the user could be utilized by Google Wallet service operated through use of a virtual MasterCard card.[9] As explained on Google Wallet's help page from 2012:

> **Add any credit or signature debit card**
> You can now add your Visa, MasterCard, American Express, and Discover credit and debit cards to Google Wallet by navigating to the Payments card section in the app and entering your card details. Your credit or debit cards become either linked cards or cards which are directly enabled for use with Google Wallet mobile app.
>
> Note: Update to the most recent version of Wallet (R79v5 or higher) to take advantage of adding any credit or debit card.
>
> **Linked credit and debit cards**
> ***When you add credit or debit cards to the Google Wallet mobile app, you will be issued a virtual MasterCard® card*** by The Bancorp Bank, Google Wallet's partnering bank. This virtual MasterCard® is referred to as the "Google Wallet Virtual Card" in the Terms of Service. ***When you activate your credit or debit cards in Google Wallet, they are linked to the virtual MasterCard® card. When you make an in-store purchase, Google Wallet facilitates payment to the merchant for your in- store purchase using the virtual MasterCard®, then charges the amount of the original purchase to your selected debit or credit card.***
>
> ***For these transactions, the merchant will not receive your credit or debit card credentials. Rather, Google Wallet will presents the virtual MasterCard® card to the merchant.*** Transactions with linked cards will appear on your bank statement as Google *merchant name.
>
> If prompted by the cashier, say that you're "paying with credit" via MasterCard®. You can find the last four digits of your virtual MasterCard® account in the card details page of one of your linked cards . . . . .
>
> **Credit or debit card is directly enabled**
> Some cards, such as the Google Prepaid Card and most Citibank MasterCard® cards, are directly enabled by the issuing bank for use with Google Wallet and are not linked to the virtual MasterCard®

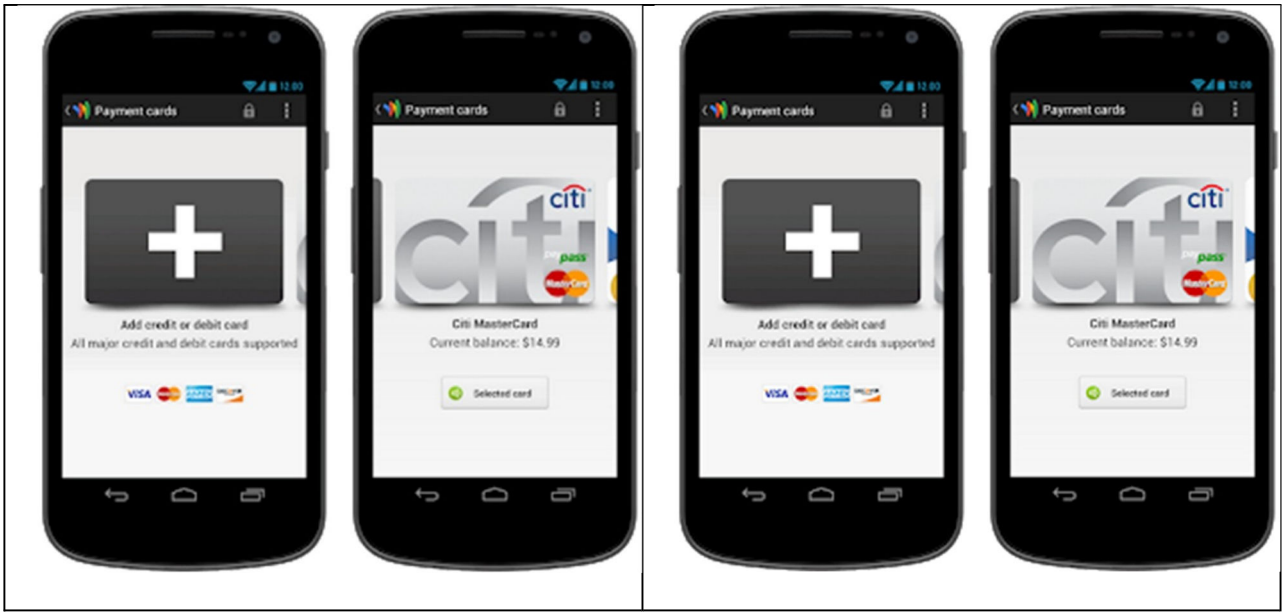
[9] Google consequently retired the use of the prepaid debit card. Google Prepaid Cards - Wallet Help (archive.org), https://web.archive.org/web/20121003192821/http://support.google.com/wallet/bin/answer.py?hl=en&answer=2477363&topic=2467414&ctx=topic (October 3, 2012).

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 30 of 156

> account. When you use the Google Wallet mobile app for an in-store purchase, your card details are presented directly to the merchant. The merchant will receive your registered card information, and will process the transaction as if you had presented the physical credit or debit card for payment.

https://web.archive.org/web/20120920004423/http://support.google.com/wallet/bin/answer.py?hl=en&answer=2701024 (September 20, 2012) (emphasis added); *Google Wallet Make Your Phone Your Wallet by Google - YouTube*, https://www.youtube.com/watch?v=qRVQTQlJV0g (February 18, 2013). *And see*:

> To support all credit and debit cards, we changed our technical approach to storing payment cards. The Google Wallet app now stores your payment cards on highly secure Google servers, instead of in the secure storage area on your phone. A wallet ID (virtual card number) is stored in the secure storage area of the phone, and this is used to facilitate transactions at the point of sale. Google instantly charges your selected credit or debit card.



http://googlecommerce.blogspot.com/2012/08/use-any-credit-or-debit-card-with.html (August 1, 2012). *And see*:

> **New and Improved Google Wallet – How it Works**
> At the heart of the new version of Google's cloud-based wallet is a virtual prepaid MasterCard that sits in the secure element in the

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 31 of 156

> phone. A consumer simply loads any MasterCard, Visa, American Express or Discover credit, debit or prepaid card as a funding card into the wallet. When a consumer pays in a store at any MasterCard PayPass location, they are using the virtual MasterCard in the phone – which is linked to their credit or debit cards that are stored in the cloud. This is a win for consumers because they can use their favorite credit or debit card when making a purchase using the virtual prepaid MasterCard. It's a win for issuers because they have another way for their cardholders to initiate transactions.

Mobile PayPass Meets Cloud in Google Wallet | Global Hub (mastercard.com),

https://newsroom.mastercard.com/2012/08/01/mobile-paypass-meets-cloud-in-google-wallet/

(August 1, 2012). *And see*

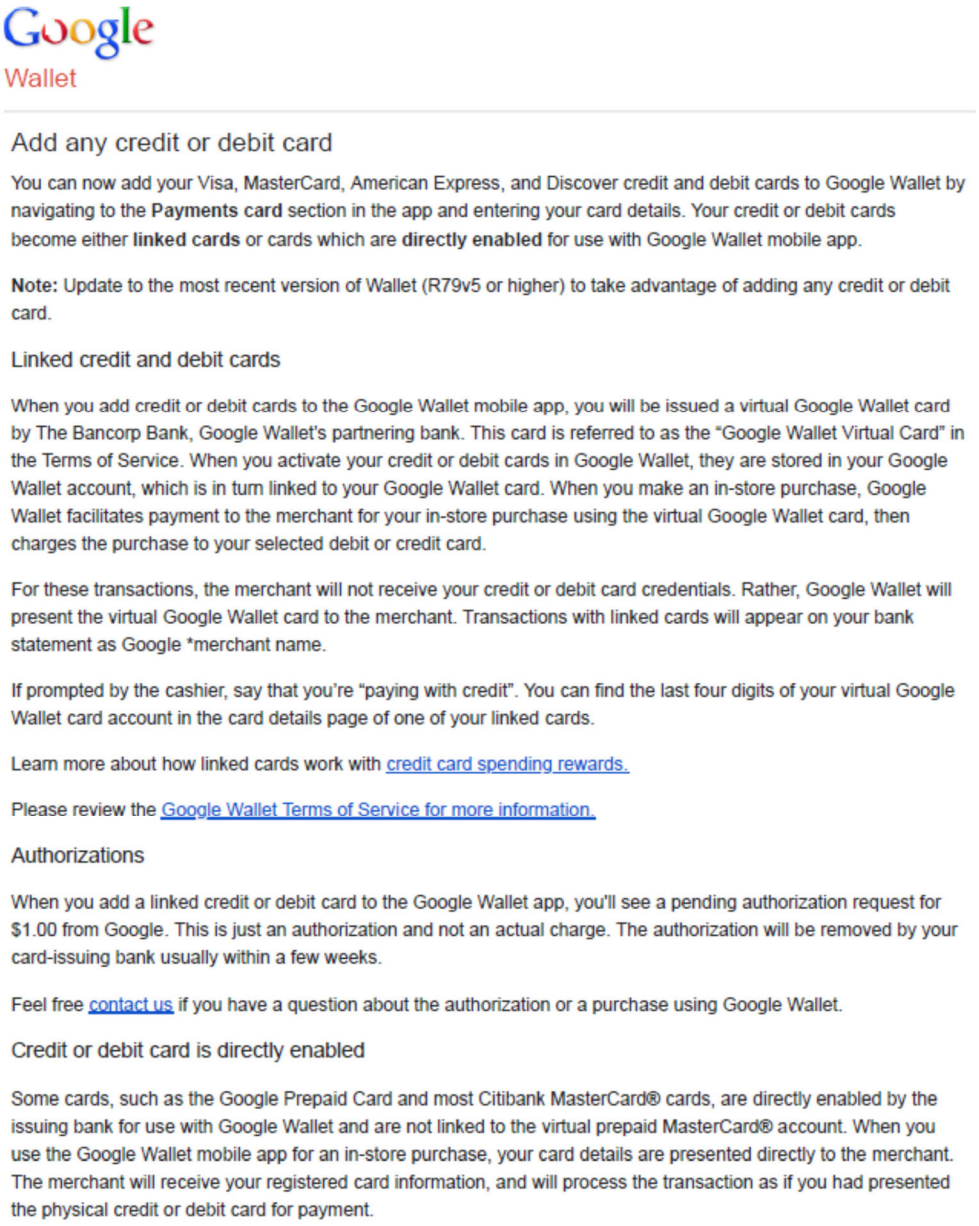
> Virtual prepaid MasterCard card
> Your Google Wallet app transaction is made using a virtual Google Wallet card by The Bancorp Bank, Google Wallet's partnering bank. This account information is passed to the merchant at the time of a transaction. Google Wallet then charges your selected debit or credit card for the full amount of the original purchase. You may see the last four digits of your virtual prepaid MasterCard on the receipt of your purchase.

How it Works - Wallet Help (archive.org),

https://web.archive.org/web/20130312061059/https://support.google.com/wallet/bin/answer.py?hl=en&answer=2463711 (March 12, 2013); and *see Google Payments Live - Google Wallet updates* - YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA at 7:28;

And see,

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 32 of 156



Google
Wallet

Add any credit or debit card

You can now add your Visa, MasterCard, American Express, and Discover credit and debit cards to Google Wallet by navigating to the **Payments card** section in the app and entering your card details. Your credit or debit cards become either **linked cards** or cards which are **directly enabled** for use with Google Wallet mobile app.

Note: Update to the most recent version of Wallet (R79v5 or higher) to take advantage of adding any credit or debit card.

Linked credit and debit cards

When you add credit or debit cards to the Google Wallet mobile app, you will be issued a virtual Google Wallet card by The Bancorp Bank, Google Wallet's partnering bank. This card is referred to as the "Google Wallet Virtual Card" in the Terms of Service. When you activate your credit or debit cards in Google Wallet, they are stored in your Google Wallet account, which is in turn linked to your Google Wallet card. When you make an in-store purchase, Google Wallet facilitates payment to the merchant for your in-store purchase using the virtual Google Wallet card, then charges the purchase to your selected debit or credit card.

For these transactions, the merchant will not receive your credit or debit card credentials. Rather, Google Wallet will present the virtual Google Wallet card to the merchant. Transactions with linked cards will appear on your bank statement as Google *merchant name.

If prompted by the cashier, say that you're "paying with credit". You can find the last four digits of your virtual Google Wallet card account in the card details page of one of your linked cards.

Learn more about how linked cards work with credit card spending rewards.

Please review the Google Wallet Terms of Service for more information.

Authorizations

When you add a linked credit or debit card to the Google Wallet app, you'll see a pending authorization request for $1.00 from Google. This is just an authorization and not an actual charge. The authorization will be removed by your card-issuing bank usually within a few weeks.

Feel free contact us if you have a question about the authorization or a purchase using Google Wallet.

Credit or debit card is directly enabled

Some cards, such as the Google Prepaid Card and most Citibank MasterCard® cards, are directly enabled by the issuing bank for use with Google Wallet and are not linked to the virtual prepaid MasterCard® account. When you use the Google Wallet mobile app for an in-store purchase, your card details are presented directly to the merchant. The merchant will receive your registered card information, and will process the transaction as if you had presented the physical credit or debit card for payment.

Add any credit or debit card - Wallet Help (archive.org),

https://web.archive.org/web/20121013234253/http://support.google.com/wallet/bin/answer.py?hl=en&answer=2701024&topic=2467414&ctx=topic (October 13, 2012);

And see,

> Cards added to Google Wallet are of two types [31]. Cards such as the Google Prepaid Card and most Citibank MasterCard® cards are directly enabled by the issuing bank for use with Google Wallet. In this case, the use of the application results in the direct transfer of

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 33 of 156

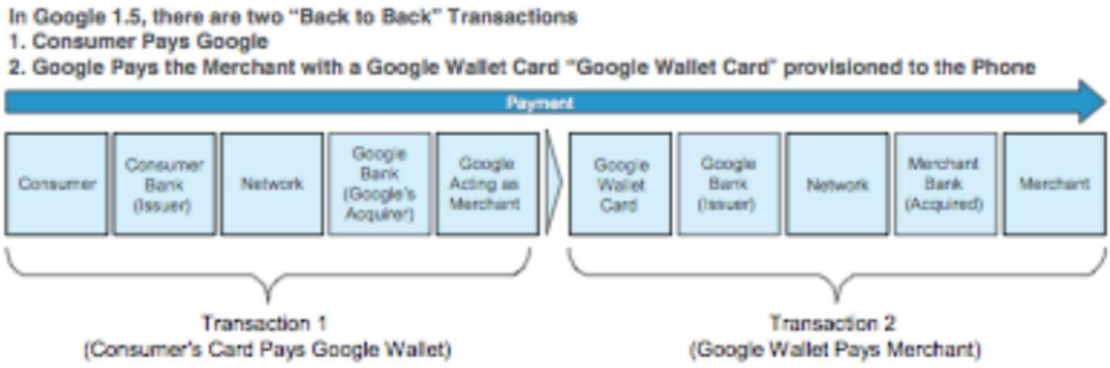
registered card information to the merchant and the transaction is processed as if the physical card was presented for payment [32].

The addition of other types of cards results in the issue of a "Google Wallet Virtual Card" by The Bancorp Bank. Upon activation, the card is stored in the user's Google Wallet account, which is in turn linked to the user's Google Wallet card. An in- store purchase to a merchant is facilitated via the virtual Google Wallet card and then charged to the selected credit or debit card. ***In the case of such a transaction, the application presents the virtual Google Wallet card to the merchant, rather than the actual card credentials [32].***
. . . .

Google assigns each Wallet user a unique Mastercard credit card number, which is used to make the transaction regardless of which stored card you select. However, prepaid cards and Citi Mastercards are still stored in the Secure Element part of the device.

Instead of storing linked debit or credit card credentials on the secure element, the application now stores the same on Google servers and only stores a wallet ID on the phone. ***Hence the real credit card numbers are usually masked ensuring a more secure transaction.***

A Comprehensive Study of Google Wallet as an NFC Application, International Journal of Computer Applications (0975 – 8887), Volume 58– No.16, November 2012, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=b03d4e50af376db0e230a248c09d3915e0785a7c (emphasis added). *And see*,



EMV and Mobile Payments, Questions abound, answers divide, Payments Summit Workshop, 2/4/2013, 07.pdf (securetechalliance.org), https://www.securetechalliance.org/resources/media/scap13_preconference/07.pdf.

The Google Wallet virtual card number is further explained in an August 2012 blog post analyzing Google Wallet:

> We have initialized the $10 prepaid card available when first installing Wallet, so *something* must be there. We know that the controller applet manages payment state, so after starting up and unlocking Wallet we finally get more interesting results (shown parsed and with some bits masked below). It turns out that locking the Wallet up effectively hides payment applications by deleting them from the PPSE. This, in addition to the fact that card emulation is available only when the phone's screen is on, provides better card security than physical contactless cards, some of which can easily be read by simply using a NFC-equipped mobile phone, as has been demonstrated.

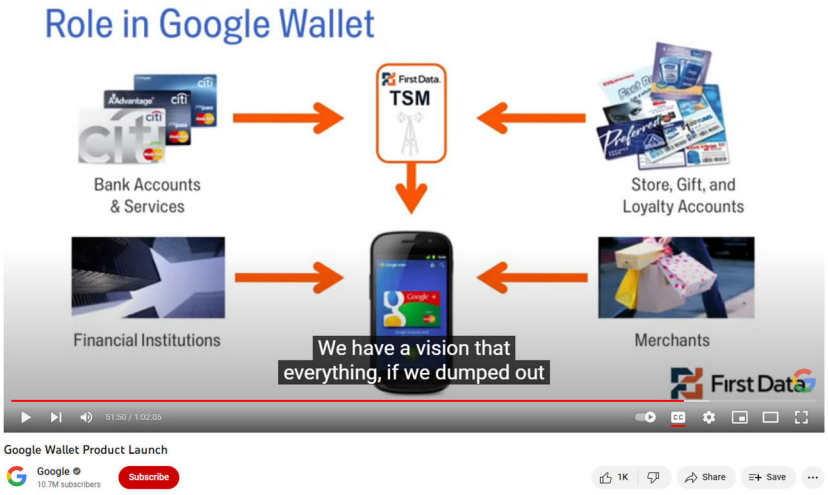
```
Applications (2 found):
  Application
   AID: a0 00 00 00 04 10 10 AA XX XX XX XX XX XX XX XX
     RID: a0 00 00 00 04 (Mastercard International [US])
     PIX: 10 10 AA XX XX XX XX XX XX XX XX
   Application Priority Indicator
     Application may be selected without confirmation of cardholder
     Selection Priority: 1 (1 is highest)
  Application
   AID: a0 00 00 00 04 10 10
     RID: a0 00 00 00 04 (Mastercard International [US])
     PIX: 10 10
   Application Priority Indicator
     Application may be selected without confirmation of cardholder
     Selection Priority: 2 (1 is highest)
```

One of the applications is the well known MasterCard credit or debit application, and there is another MasterCard app with a longer AID and higher priority (1, the highest). The recently announced update to Google Wallet allows you to link practically any card to your Wallet account, but transactions are processed by a single 'virtual' MasterCard and then billed back to your actual credit card(s). It is our guess that the first application in the list above represents this virtual card.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 35 of 156

Exploring Google Wallet using the secure element interface (nelenkov.blogspot.com), https://nelenkov.blogspot.com/2012/08/exploring-google-wallet-using-secure.html (August 27, 2012).

First Data spoke at the launch of Google Wallet:



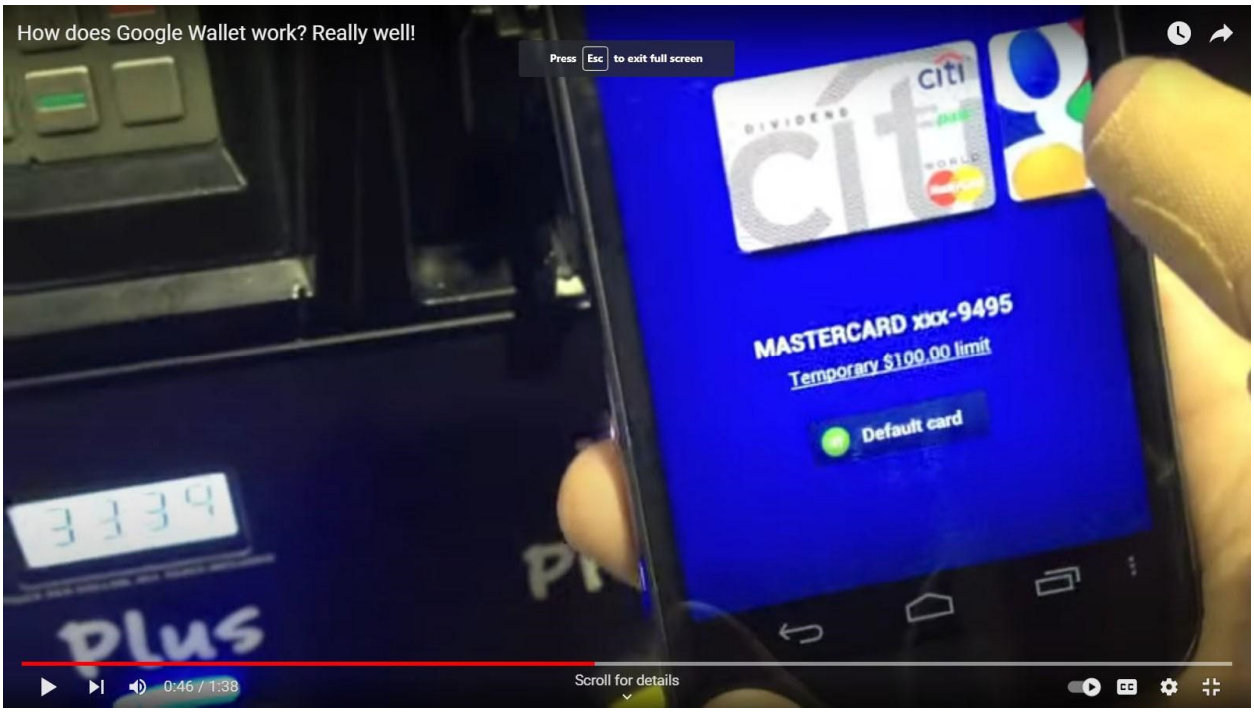
Google Wallet Product Launch - YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0 at 19:53 (May 27, 2011), at 51:50. First Data had filed a patent application in 2009 on creation and usage of dynamic cryptograms and a dynamic substitute encrypted credit card number for use in smartphone contactless transactions. United States Patent Application Publication No. 2010/0185545, titled *Dynamic Primary Account Number (PAN) and Unique Key Per Card*.

Google Wallet ran on the Nexus S (manufactured by Samsung)[10] and (as noted) required entry of a user defined PIN to enable contactless payments. *Technology: Google Wallet | The New York Times - YouTube*, https://www.youtube.com/watch?v=l8JOT6ban7o (Technology: Google Wallet | The New York Times, Sep 23, 2011) (Pin entry at 0:56 and 1:10, "virtual credit card" at 1:35, Nexus S at 1:44); *Google Wallet launches officially on Nexus S 4G - Android*

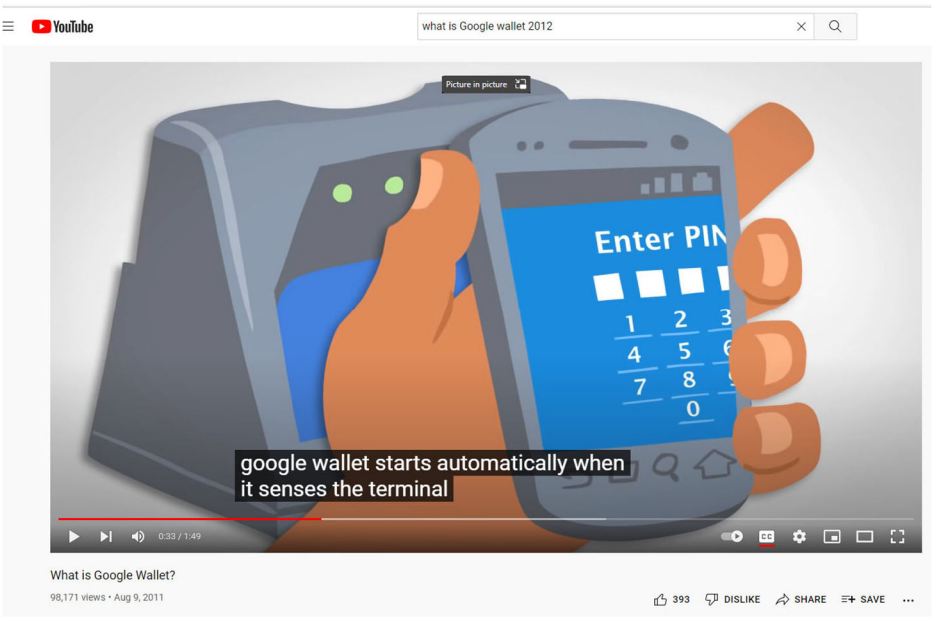
[10] Google Nexus S by Samsung at CES 2011 - YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM (January 11, 2011).

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 36 of 156

Community, https://androidcommunity.com/google-wallet-launches-officially-on-nexus-s-4g-20110919/ (September 19, 2011). Google Wallet displayed the last four numbers of the credit card to be utilized to the user:

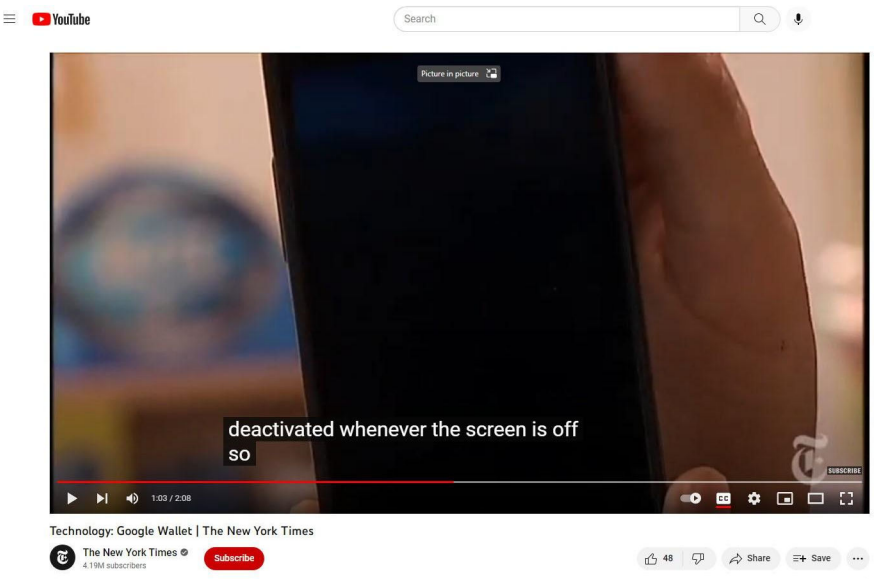


How does Google Wallet work? Really well! - YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA (December 7, 2011) at 0:46; *Google Wallet Demonstration - YouTube*, https://www.youtube.com/watch?v=6tBAB5ls5vM (May 26, 2011). Google Wallet contactless transactions were possible only when the NFC functionality of the phone was active, i.e. when the phone was close to the point-of-sale terminal:



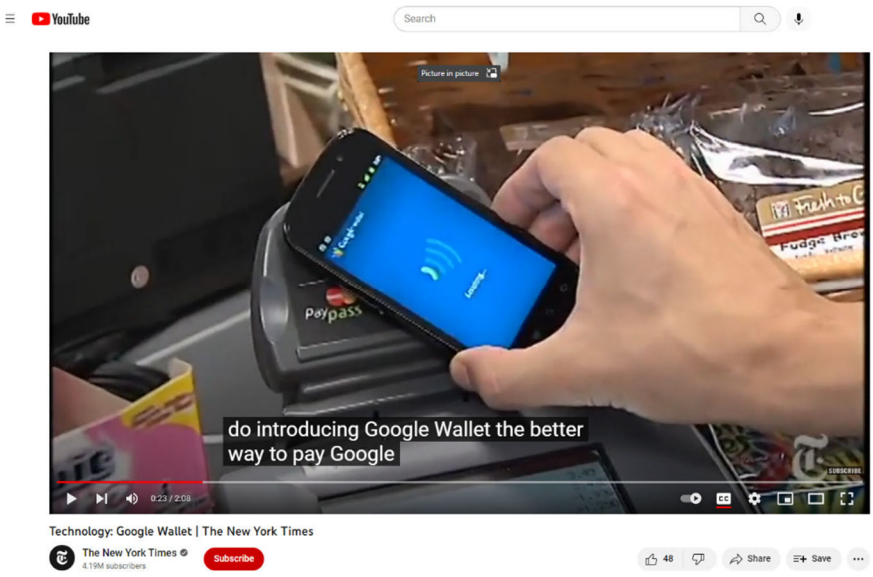
What is Google Wallet, Aug 9, 2011, https://www.youtube.com/watch?v=iuvyN4iZiP8 at 0:32.

Google Wallet could be deactivated when the screen was off:



Technology: Google Wallet | The New York Times - YouTube,

https://www.youtube.com/watch?v=l8JOT6ban7o (Sept. 23, 2011), at 1:30. As the transaction happened, Google Wallet displayed no card information, such as a credit card number:



Technology: Google Wallet | The New York Times - YouTube,

https://www.youtube.com/watch?v=l8JOT6ban7o (Sept. 23, 2011), at 0:23.[11]

Additional Google Wallet compatible device included:

> Samsung Galaxy Nexus on Sprint
> Samsung Galaxy Victory 4G LTE on Sprint
> Samsung Galaxy Nexus GSM/HSPA+ (available for purchase on Google Play) Samsung Galaxy SIII on Sprint, MetroPCS, and US Cellular
> LG Viper™ 4G LTE on Sprint
> LG Optimus Elite™ on Sprint and Virgin Mobile HTC EVO 4G LTE on Sprint
> Asus Nexus 7 Tablet (WiFi only) (available for purchase on Google Play) Samsung Galaxy Victory 4G LTE on Sprint

[11] Other videos describing the use of Google Wallet include: How To Use Google Wallet On Android - YouTube, https://www.youtube.com/watch?v=6DeiEVBlBcs; Google Wallet Hands-On | Engadget - YouTube, https://www.youtube.com/watch?v=5s9wYEkRAgs; Google Wallet Demonstration - YouTube, https://www.youtube.com/watch?v=6tBAB5ls5vM; Paying With Google Wallet - YouTube, https://www.youtube.com/watch?v=jTeiISIzBPQ; Google Wallet Walkthrough - YouTube, https://www.youtube.com/watch?v=xmbRSXYdFFs; How To Use Google Wallet On Verizon Galaxy Nexus | Pocketnow - YouTube, https://www.youtube.com/watch?v=AZ8t757ZfUs; Citi: What is Google Wallet? - YouTube, https://www.youtube.com/watch?v=duHgioveLvM; Using Google Wallet in McDonalds! - YouTube, https://www.youtube.com/watch?v=1p6co4YlvbA.

Eligible Devices - Wallet Help (archive.org), https://web.archive.org/web/20121108194442/http://support.google.com/wallet/bin/answer.py?hl=en&answer=1347934 (November 8, 2012). A teardown of the Nexus S from 2011 can be found at" Samsung Galaxy Nexus Teardown - iFixit, https://www.ifixit.com/Teardown/Samsung+Galaxy+Nexus+Teardown/7182 (Dec. 1, 2010); The Nexus S included an accelerometer. *Samsung Google Nexus S review: Royal droid* - GSMArena.com (archive.org), https://web.archive.org/web/20110718162933/https://www.gsmarena.com/google_nexus_s-review-565.php (July 18, 2011).

The Nexus S and other Google Wallet compatible devices ran on the Android OS, which allowed a user to view user and device specific information on the phone. E.g., *How to find out IMEI number on Google Nexus S phone – Tech Notes Desk*, https://blog.technotesdesk.com/how-to-find-out-imei-number-on-google-nexus-s-phone (January 10, 2013).

Publicly available Android OS, and corresponding code in Samsung and other Android devices at the time, included functionality for providing trust zones, motion sensor information, PIN code entry, screen and activity locks, biometric sensors, NFC, and WiFi, including for Google Wallet. For example, Android code at the time, such as Android 4.2 (JellyBean) October 29, 2012, shows use of the following (where similar functionality can be found in other Android versions before March 2013):

- Mobicor for trust zones for payment applications on Samsung devices. *See, e.g.*, http://androidxref.com/4.2_r1/xref/hardware/samsung_slsi/exynos5/mobicore/
- Google Wallet. *See, e.g.*, http://androidxref.com/4.2_r1/xref/device/samsung/manta/nfc/nfcee_access_debug.x

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 40 of 156

ml;

http://androidxref.com/4.2_r1/xref/frameworks/base/docs/html/guide/google/play/billing/billing_admin.jd; and

http://androidxref.com/4.2_r1/xref/frameworks/base/docs/html/guide/google/play/billing/billing_overview.jd;

http://androidxref.com/4.2_r1/xref/docs/source.android.com/src/tech/security/index.md ("A more robust approach to protecting data from root users is through the use of hardware solutions. OEMs may choose to implement hardware solutions that limit access to specific types of content such as DRM for video playback, or the NFC-related trusted storage for Google wallet.")

- touch screen. *See, e.g.*,

  http://androidxref.com/4.2_r1/xref/device/samsung/manta/Atmel_maXTouch_Touchscreen.idc;

  http://androidxref.com/4.2_r1/xref/docs/source.android.com/src/tech/input/touch-devices.md

- motion rate detector. *See, e.g.*,

  http://androidxref.com/4.2_r1/xref/frameworks/native/services/sensorservice/tests/sensorservicetest.cpp;

  http://androidxref.com/4.2_r1/xref/frameworks/native/data/etc/android.hardware.sensor.accelerometer.xml;

  http://androidxref.com/4.2_r1/xref/hardware/invensense/libsensors/MPLSensor.cpp;

  http://androidxref.com/4.2_r1/xref/frameworks/native/data/etc/android.hardware.sensor.gyroscope.xml

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 41 of 156

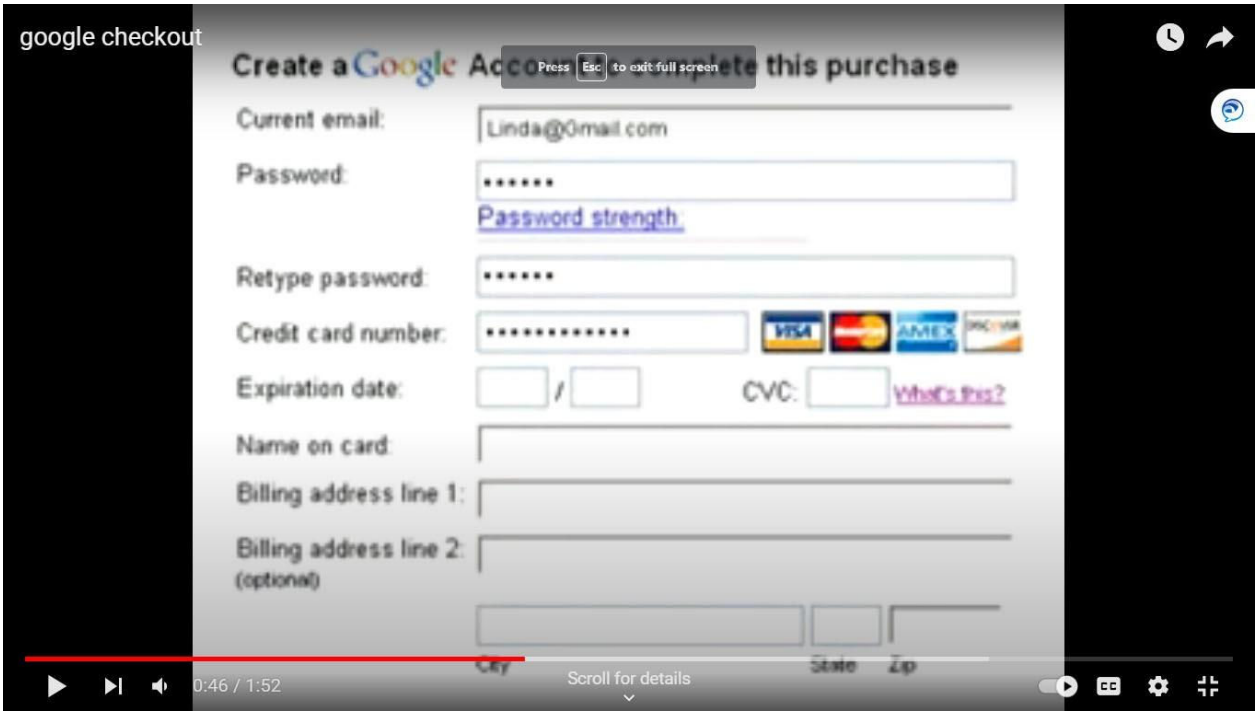
- WiFi. *See, e.g.*, http://androidxref.com/4.2_r1/xref/external/wpa_supplicant_8/hostapd/android.config
- lock screen and authorization. *See, e.g.*, http://androidxref.com/4.2_r1/xref/frameworks/base/tests/Assistant/res/layout/assist_intent_activity.xml; http://androidxref.com/4.2_r1/xref/frameworks/base/policy/src/com/android/internal/policy/impl/keyguard_obsolete/LockPatternKeyguardView.java
- USB. *See, e.g.*, http://androidxref.com/4.2_r1/xref/frameworks/base/core/java/android/hardware/usb/package.html
- NFC. *See, e.g.*, http://androidxref.com/4.2_r1/xref/frameworks/base/core/java/android/nfc/tech/
- biometric sensors. *See, e.g.*, http://androidxref.com/4.2_r1/xref/frameworks/base/policy/src/com/android/internal/policy/impl/keyguard/BiometricSensorUnlock.java
- NFC with an expiration time. *See, e.g.*, http://androidxref.com/4.2_r1/xref/external/libnfc-nci/src/nfc/nfc/nfc_task.c, lines ("void nfc_start_timer (TIMER_LIST_ENT *p_tle, UINT16 type, UINT32 timeout"))
- NFC AND device proximity. *See, e.g.*, http://androidxref.com/4.2_r1/xref/frameworks/base/docs/html/guide/topics/connectivity/nfc/nfc.jd

- double button press. *See, e.g.*, http://androidxref.com/4.2_r1/xref/frameworks/base/core/java/android/view/GestureDetector.java ("Notified when a double-tap occurs.")
- biometric sensor with proximity sensor. *See, e.g.*, http://androidxref.com/4.2_r1/xref/frameworks/base/policy/src/com/android/internal/policy/impl/keyguard/BiometricSensorUnlock.java; http://androidxref.com/4.2_r1/xref/frameworks/native/data/etc/android.hardware.sensor.proximity.xml
- disabling a device based on incorrect PIN entry. *See, e.g.*, http://androidxref.com/4.2_r1/xref/frameworks/base/policy/src/com/android/internal/policy/impl/keyguard/KeyguardViewMediator.java ("PERM_DISABLED")
- disabling features based on time expiry. *See, e.g.*, http://androidxref.com/4.2_r1/xref/frameworks/base/policy/src/com/android/internal/policy/impl/keyguard/KeyguardViewMediator.java ("KEYGUARD_LOCK_AFTER_DELAY_DEFAULT")
- swipe and gesture detection. *See, e.g.*, http://androidxref.com/4.2_r1/xref/frameworks/base/docs/html/design/patterns/swipe-views.jd

G. Google Checkout

Google Checkout was an online payment processing service provided by Google that launched in 2006. *google checkout* - YouTube, https://www.youtube.com/watch?v=-UeYkxePW2c (June 29, 2006) Google Checkout merged into Google Wallet in 2011. *Google Commerce: Building one wallet: Google Checkout is transitioning to Google Wallet*

(googleblog.com), https://commerce.googleblog.com/2011/11/building-one-wallet-google-checkout-is.html (November 16, 2011); *Google Checkout checks out, replaced by Google Wallet Android Community*, https://androidcommunity.com/google-checkout-checks-out-replaced-by-google-wallet-20111117/ (November 17, 2011). Google Checkout as an independent service was discontinued in 2013. Google Checkout facilitated online (web or mobile) payments. Users provided their credit or debit card (as well as shipping) information to Google. Google stored the information in the user's Google account.



google checkout - YouTube, https://www.youtube.com/watch?v=-UeYkxePW2c (June 29, 2006). When the user subsequently selected a Google Checkout button to effectuate a purchase at a web site or in a mobile app, Google Checkout servers would transact the purchase with the merchant using the user's previously provided information. The service was similar to PayPal's purchase checkout system at the time. See *Google I/O 2011: Google Checkout: A Foundation For Payments* - YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E (May 13 2011);

Google Checkout HTML API Short Attribute Reference - Google Checkout - Google Code (archive.org), https://web.archive.org/web/20120327131033/http://code.google.com/apis/checkout/developer/Google_Checkout_Basic_HTML_How_Checkout_Works.html (March 27, 2012); When used with Google Wallet, the service did not use or require NFC:

> Unless you happen to be using the right phone on the right carrier, you might not know that Google Wallet is even a reality: the close association with NFC-based mobile payments on one network has largely kept it out of the public eye. Many more are about to see Wallet in action now that Google has quietly introduced it to the web. No, you won't tap your phone against your computer screen; the web version is mostly targeted at microtransactions and gives readers more than a few ways to buy without getting burned, such as long and blurred-out previews, a narrow price range between 25 to 99 cents and an Instant Refund option that gives no-questions-asked credit within half an hour.

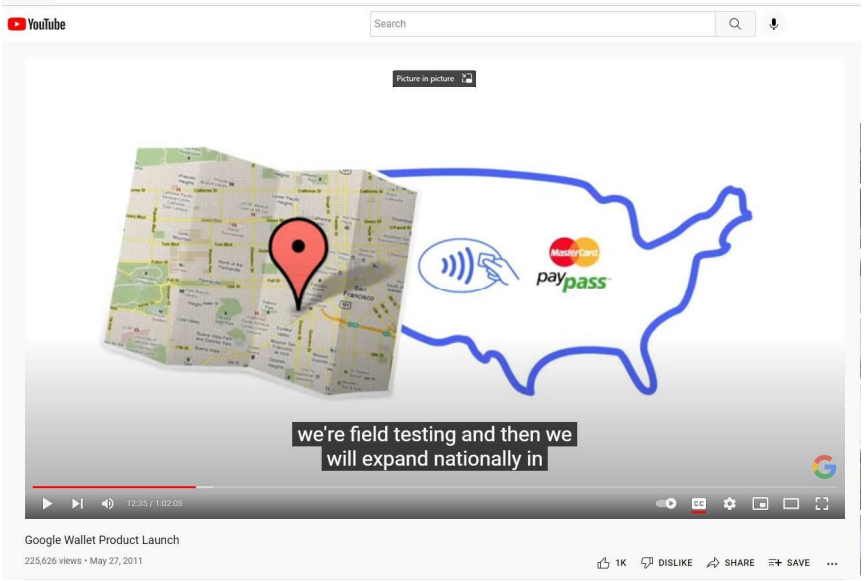
Google Wallet reaches the web, reminds most of us that it exists | Engadget, https://www.engadget.com/2012-10-04-google-wallet-reaches-the-web-reminds-most-of-us-that-it-exists.html (October 4, 2012).[12]

H. MasterCard PayPass

Google Wallet contactless payments operated on and was accepted at MasterCard PayPass terminals.

[12] PayPal also offered an API for allowing online purchases. *PayPal NVP API Developer Reference Enterprise Edition - eBay* (paypalobjects.com), https://www.paypalobjects.com/webstatic/en_US/developer/docs/pdf/PP_NVPAPI_DeveloperGuide_eBay.pdf; *Find out how PayPal* works - YouTube, https://www.youtube.com/watch?v=dn42Y-2uFQM (March 14, 2012); *How Does PayPal Work? YouTube*, https://www.youtube.com/watch?v=MdrPOCCFQ2k (July 24, 2012).

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 45 of 156



Google Wallet Product Launch - YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0 at 12:22 (May 27, 2011). *What is Google Wallet? - YouTube*, https://www.youtube.com/watch?v=iuvyN4iZiP8 at 1:49 (What is Google Wallet? Aug 9, 2011); Tap and Pay - Wallet Help (archive.org), https://web.archive.org/web/20121003192651/http://support.google.com/wallet/bin/answer.py?hl=en&answer=2466137&topic=2467414&ctx=topic (October 3, 2012). MasterCard launched PayPass in 2008 to facilitate contactless credit card transactions.

PayPass utilized virtual card numbers and MasterCard advertised PayPass for NFC mobile phone contactless transactions:

> **MasterCard Virtual Card Numbers (VCNs)** are one-time use prepaid account numbers that are used complete a transaction using a mobile phone or on the internet. MasterCard's inControl™ platform generates these VCNs giving consumers a safe and secure way to pay using their mobile phones

Microsoft Word - MasterCard - Mobile Commerce Fact Sheet - 05-26-2011.doc, https://newsroom.mastercard.com/wp-content/uploads/2011/09/MasterCard-Mobile-Commerce-Fact-Sheet-05-26-2011.pdf (May 26, 2011). Technology reviewers at the time described Google Wallet as substituting the smartphone for known credit cards:

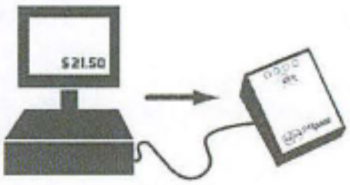
> Card Emulation Mode - The mode in which Google Wallet and other forms of contactless pay will be based, card emulation mode is exactly what it sounds like -- the phone becomes your credit card. Emulating a traditional smart card makes it convenient for companies like MasterCard and Visa that already have infrastructures set up for contactless pay, since nothing has to be changed.

Engadget Primed: What is NFC, and why do we care?, Engadget, June 10, 2011.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 47 of 156

How it Works

A computer chip in the payment card or device securely communicates with the merchant terminal. Within a fraction of a second, a light or beep indicates an approved transaction, and the cardholder is on their way.



Transaction details are sent to the *PayPass*-enabled terminal from the electronic cash register (ECR).

Card/device is tapped. Terminal activates and recognises the *PayPass* card/device and exchanges payment account details. *PayPass* card/device generates a dynamic cryptogram that creates a secure transaction in a fraction of a second.

Transaction data is transmitted to issuer along with payment account details via acquirer. Issuer validates the dynamic cryptogram, authenticates the data, and authorises transaction.

FORM FACTORS

For cards, *PayPass* is available as both *PayPass* M/Chip and *PayPass* Magstripe. *PayPass* is also available on devices like key fobs, wristbands, mobile tags, and mobile phones. In fact, enabling for *PayPass* now can help put you ahead of the NFC adoption curve.

Interoperabilty is also a major *PayPass* requirement. *PayPass*-enabled cards or devices can be tapped and processed using *PayPass*-enabled terminals.

Paypass Toolkit for Financial Institutions, 2012, p. 3.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 48 of 156

MasterCard filed patent applications for mobile smartphone contactless transactions using cryptograms and substitute card numbers. *See, e.g.*, U.S. Patent Application Publication US 2013/0232083 titled *System and Methods for Mapping a Mobile Cloud Account to a Payment Account* and U.S. Patent Application Publication US 2013/0262317 titled *Systems and Methods for Processing Mobile Payments by Provisoning Credentials to Mobile Devices without Secure Elements*.

MasterCard eventually purchased the payments company Orbiscom in 2009. *See* https://investor.mastercard.com/investor-news/investor-news-details/2009/MasterCard-Acquires-Orbiscom-to-Accelerate-Development-of-Innovative-Payment-Solutions/default.aspx.[13]

I. ISIS (Verizon, AT&T, T-Mobile)

In 2012, other wireless carriers noted Google Wallet's required access of the Secure Element. *Verizon won't offer Google Wallet for the Galaxy Nexus because it uses a 'secure element' - The Verge*, https://www.theverge.com/2012/12/10/3751538/verizon-google-wallet-galaxy-nexus-secure-element/comment/132058761 (December 10, 2012). Verizon, AT&T and T-Mobile at the time developed their own NFC contactless payment solution for smartphones to be offered through the carriers' joint venture called ISIS, which solution required access to the Secure Element.[14] On information and belief, the ISIS wallet system operating on a mobile phone operated similar to Google Wallet regarding the use of NFC for contactless transmission, EMV

[13] https://web.archive.org/web/20080523123532/http:/orbiscom.com/clients.php?link=home and https://web.archive.org/web/20100315024304/http:/www.orbiscom.com/.

[14] Samsung and other device manufacturers had announced support for the ISIS solution in 2011. *Handset makers line up behind Isis NFC payment platform – Old GigaOm*, https://old.gigaom.com/2011/09/27/handset-makers-line-up-behind-isis-nfc-payment-platform/.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 49 of 156

cryptograms, passing of the PAN, funding of reloadable prepaid card, and a the ability to operate on a preexisting credit card network, such as VISA and American Express.[15]

Gemalto, an EMV NFC contactless card provider was also involved in the project. https://web.archive.org/web/20130310085256/http://www.gemalto.com/brochures/download/tel_mobile_payment_services.pdf; https://web.archive.org/web/20120124225944/http://www.gemalto.com/brochures/download/allynis_tsm.pdf; https://web.archive.org/web/20111226050743/http://www.gemalto.com/brochures/download/emv_deployment.pdf; https://web.archive.org/web/20120131073441/http://www.gemalto.com/brochures/download/allynis_mobile_nfc.pdf; https://web.archive.org/web/20111125040548/http://www.gemalto.com/brochures/download/nfc_mobile_operators.pdf; *Services in the U.S.; Gemalto to Provide Isis Mobile Commerce Platform with Trusted Service Manager (TSM) Solution*, Business Wire, December 12, 2011. The ISIS service launched in late 2012 in Austin and Salt Lake City. *Isis™ Launches in Austin and Salt Lake City; As Many as 20 Isis Ready™ Handsets to Be Available by Year End*, October 22, 2012, https://www.businesswire.com/news/home/20121022005698/en/Isis%E2%84%A2-Launches-in-Austin-and-Salt-Lake-City-As-Many-as-20-Isis-Ready%E2%84%A2-Handsets-to-Be-Available-by-Year-End. Samsung , HTC, LG, Motorola, RIM and Sony Ericsson pledged to

[15] Given the similarity of Google Wallet and the ISIS systems with regard to the asserted claims, Google submits that the charts for Google Wallet apply, and should be understood as applicable, to the ISIS system. To this end, Google has in some instances, included information about the ISIS system in its charts for Google Wallet. As noted, the ISIS system was ultimately purchased by Google and merged into a successor product to Google Wallet, further suggesting the similarity of the products. Google will supplement these contentions pending discovery on the system art.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 50 of 156

support the carriers' ISIS efforts in 2011. *Isis Revealed: Carrier-Led Mobile Payments Venture Shows Off Its New App, Announces Banking Partners | TechCrunch*, https://techcrunch.com/2012/02/27/isis-revealed-carrier-led-mobile-payments-venture-shows-off-its-new-app-announces-banking-partners/. ISIS could be utilized in the United States on the following Samsung devices in 2012:

> To be specific, only one device – the Droid Incredible 4G LTE — supports Isis on Verizon for now, while you can use Isis on three T-Mobile smartphones – the ***Samsung Galaxy S3, Samsung Galaxy S2, and Samsung Galaxy Relay 4G***. As for AT&T, the carrier has announced that the ***Samsung Galaxy S3, Samsung Exhilarate, Samsung Rugby Pro, LG Escape***, and HTC One X will all support Isis on launch day.

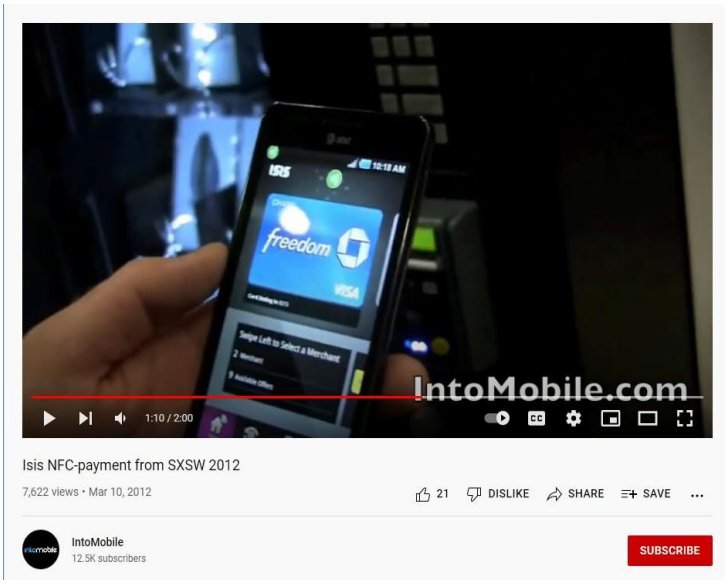
Isis to officially launch on Oct 22, more supported devices announced (androidauthority.com), https://www.androidauthority.com/isis-mobile-payment-launch-devices-123710/ (October 18, 2012) (emphasis added). The Galaxy S3 included Face scan recognition functionality in 2012 to prevent use of the device by anyone other than the owner of the device:

> Face unlock: When enabled, you unlock the phone by looking at the screen. This option offers low security, because someone who looks similar to you could unlock your phone. Touch the option for more information, and to set up Face unlock.

Verizon User Manual Samsung Galaxy SIII (2012), p. 139.

The user interface for ISIS in 2012 is described in the following videos, including the use of user PIN entry for security:

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 51 of 156



Isis NFC-payment from SXSW 2012 - YouTube,

https://www.youtube.com/watch?v=Z2MOAtUhR7k (Isis NFC-payment from SXSW 2012) March 10, 2012; *Hands-on with ISIS Mobile Wallet – YouTube* https://www.youtube.com/watch?v=eOMqvGVKjmM (Mar 10, 2012). A user's ISIS account was funded with a VISA reloadable prepaid account, acting as a virtual credit card:

> While PayPal incorporated a plastic payment card for the point of sale this year, and Google Wallet was considering the same thing through Discover Financial Services, Isis already had its Isis Cash card. Isis Cash, a Visa reloadable prepaid account, appears in the mobile wallet for the consumer, who receives the plastic card when enrolling in Isis.
>
> Isis could be described as a container holding virtual plastic cards.

Mobile Wallet Consortium Strives Cautiously In 2012; The telco joint effort proceeded more slowly than expected, but its leaders maintain that the mobile wallet business is big enough for lots of players, ISO&Agent, January 1, 2013. ISIS later replaced the Visa Prepaid virtual card with Amex's Serve Digital Wallet to facilitate the same feature:

> In the revamped Isis app launched this week, anyone without the proper JPMorgan Chase or Amex credit card must sign up for

> Amex's Serve digital wallet to make Isis payments. Isis at one time offered an Isis Cash virtual prepaid card to serve the same purpose, but Amex has completely taken over that role.
>
> Today, "there is no Isis prepaid account. We are the prepaid account," says Stefan Happ, senior vice president and general manager of U.S. payment options for American Express.

Amex Plays a Major Role in Revamped Isis Mobile Wallet, PaymentSource paymentssource.com, November 15, 2013.

Google Wallet transitioned to HCE to avoid reliance on the Secure Element built into the smartphone devices. Later in 2015, Google bought ISIS (which had by that time been renamed SoftCard) and integrated it into Google Wallet.

J. Substituting Tokens for Credit Card Numbers

It was known in the art that the transmission of a user's credit card number (aka Personal Account Number or PAN) to a merchant as part of a credit card transaction was a security risk. To address this issue, *Financial Cryptography*, 5th International Conference, FC 2001, Grand Cayman, British West Indies, February Proceedings, Paul F. Syverson (Ed.), copyright 2002, noted that by 2001 credit card companies like American Express and VISA provided single use or limited use credit card known as "tokens." That work further described what it purported to be a novel solution of generating a limited use token on the user device itself:

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 53 of 156

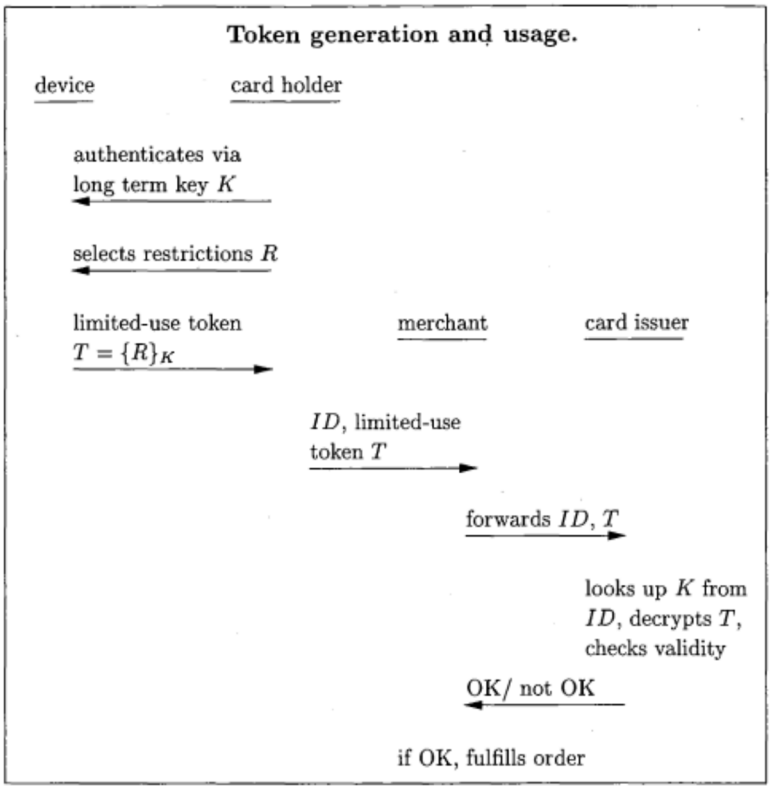


Fig. 1. The card holder authenticates to the device and selects the set R of restrictions. The device uses a key derived from the credit card number to encrypt R and produce a token T. The card holder then transmits T to the merchant, along with some identifying information ID. The merchant forwards these to the card issuer, who uses ID to look up the account, retrieve the card holder's long term key K, and decrypts the token. If the restrictions are met, the transaction is processed; otherwise, it is denied

Off-Line Generation of Limited-Use Credit Card Number, at p. 196-209.[16]

In 2009, VISA published a "best practices" document that encouraged use of tokens in place of a credit card PAN for all transactions. *bulletin-tokenization-best-practices.pdf (visa.com)*, https://usa.visa.com/dam/VCOM/global/support-legal/documents/bulletin-tokenization-best-practices.pdf (July 14, 2010). In 2011, the PCI Security Standards Council published a technical standard for replacing the credit card number with a token. PCI DSS

[16] *See also* p. 210-231, *A Security Framework for Card-Based Systems*; p. 232-242, how credit card transactions worked in 2001 and discusses another varied method for secure credit card transactions; p.232-242, *SecureClick: A Web Payment Systems with Disposable Credit Card Number*, discussing disposable credit card numbers.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 54 of 156

Information Supplement Tokenization (pcisecuritystandards.org), v. 2.0, August 2011 ("Tokenization is a process by which the primary account number (PAN) is replaced with a surrogate value called a ―token. One of the primary goals of a tokenization solution should be to replace sensitive PAN values with non-sensitive token values. For a token to be considered non-sensitive, and thus not require any security or protection, the token must have no value to an attacker.").

In 2012, Bell ID offered for sale the Bell ID® Mobile Token Manager that provided tokens for use with NFC-based mobile payment platforms: "advanced mobile (NFC) lifecycle management capabilities that assist organizations in executing Trusted Service Manager (TSM) services or in provisioning their applications onto mobile handsets. The solution is based on a proven and scalable software platform already used by financial institutions worldwide to manage millions of contact/contactless cards and payment applications." Further, the solution was advertised as being "ideally placed to assist organizations in expanding their token portfolio from contact and contactless cards to mobile (NFC) devices." https://web.archive.org/web/20120831071422/http://www.bellid.com/solutions/ota-lifecycle-management; *Bell ID Simplifies EMV Smart Card and NFC Application Management with Versatile New Platform*, eBanking & Payment News, May 5, 2011 ("Bell ID announced the launch of Bell ID® EMV Token Manager, a new web based solution which coordinates and simplifies the management of any type or combination of EMV token deployment, including contact, contactless and dual interface cards as well as the option to support contactless applications in NFC enabled mobile phones."). The token technology was used by Blackberry (RIM) in early 2013. *RIM implements Bell ID's Token Manager software for mobile payments*,

WMI Company News, January 23, 2013. Google Wallet used the technology in 2016.[17] BellID's technology was acquired by Visa in 2019.

https://www.businesswire.com/news/home/20191022005204/en/Visa-Completes-Acquisition-Rambus-Payments-Portfolio/.

K. Contactless ATM

It was known at least as early as 2011 that a contactless withdraws could be made from an ATM using a mobile device:

> Spain-based bank Caja de Ahorros y Pensiones de Barcelona, or "La Caixa," which operates the largest cash machine network in Spain, in early April installed the first contactless ATMs, leveraging technology from Fujitsu Global (see story). La Caixa deployed the machines in Barcelona, Sitges and Palma. The technology integrated into the machines enables consumers to either withdraw funds using their contactless EMV chip-and-PIN bankcard or a Near Field Communication-enabled phone. Consumers place their contactless card or mobile phone near the reader on the ATM and enter their PIN to complete the withdrawal for no additional fee.

Mobile's Gains Prompt More Banks To Move Beyond Cards For ATM Access, ATM and Debit News, May 12, 2011.

[17] *A closer look at Google Pay and tokenization - Rambus*, https://www.rambus.com/blogs/a-closer-look-at-android-pay-and-tokenization-2/; *Rambus' Bell ID to support Android Pay - Rambus*, https://www.rambus.com/blogs/rambus-bell-id-to-support-mobile-pay/.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 56 of 156

caixer contactless lacaixa - YouTube, https://www.youtube.com/watch?v=It2CpMcxQC4 (April 4, 2011). Standard had even been prepared for EMV contactless withdraws for ATMs:

> The ATM Industry Association has announced the publication of new best practices for accepting contactless payments in ATM systems.
>
> "With banks like la Caixa in Spain pioneering the deployment of contactless ATMs, including plans for a few hundred more contactless ATMs in the near-future, ATMIA felt the time had come to be proactive and look at the security aspects of this evolving global technology," said ATMIA CEO, Mike Lee, in the announcement. "Even though there is little reliable evidence of fraud deriving from contactless payment methods as yet, some risks do remain which can be mitigated."
>
> Examples of topics covered in the manual include:
>
> the contactless communications landscape - including NFC, RFID and passive contactless systems that use plastic payment cards - and describes how the contactless payments space works.

ATMIA publishes contactless ATM best practices; The ATM Industry Association has announced the publication of new best practices for accepting, ATM Marketplace, September 27, 2012.

Bank of America filed an application in 2011 leading to issuance of US Patent No. 9,098,846

titled *Contactless automated teller machine* that described an ATM machine "that has been equipped with a contactless interface for interacting with an external apparatus such as a debit/credit card, mobile device, and/or contactless transmission equipped stickers" and a mobile wallet chip that "is incorporated in an element within the mobile device 500 that provides NFC capabilities to the mobile device 500." *See also, BofA pursuing contactless ATM patent*, Mobilepaymentstoday.com News, September 20, 2012; *Is a contactless ATM inevitable?; Bank of America seems to think so; the FI has filed a patent application for a 'Contactless Automated Teller Machine'* ATM Marketplace, September 20, 2012.

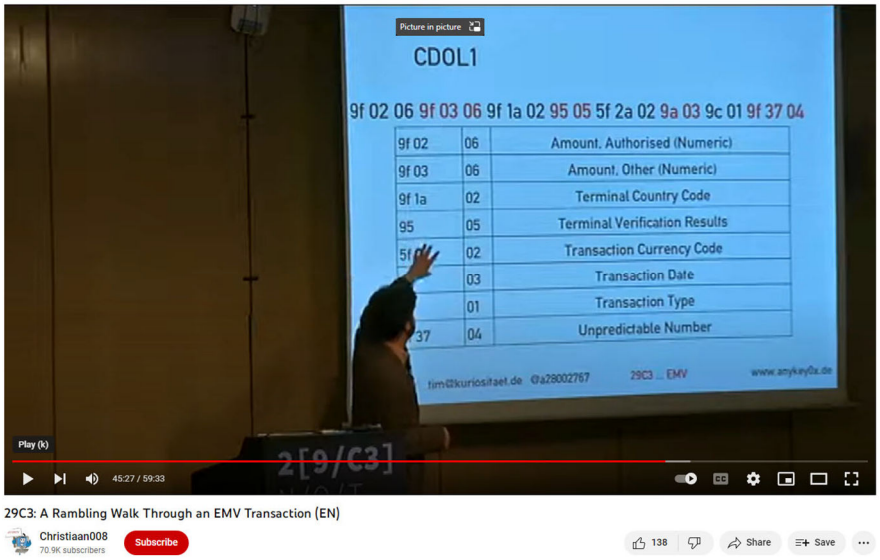
Google considered adding ATM functionalities to its Google Wallet app in 2012:

Google Payments Live - Google Wallet updates - YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA (August 23, 2012). Citibank, which originally launched its card with Google Wallet (see above), filed a patent on contactless ATM. United States Patent Application Publication No. 2013/0124410, titled System and *Method for Conducting a Transaction at a Financial Transaction Terminal Using a Mobile Device*.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 58 of 156

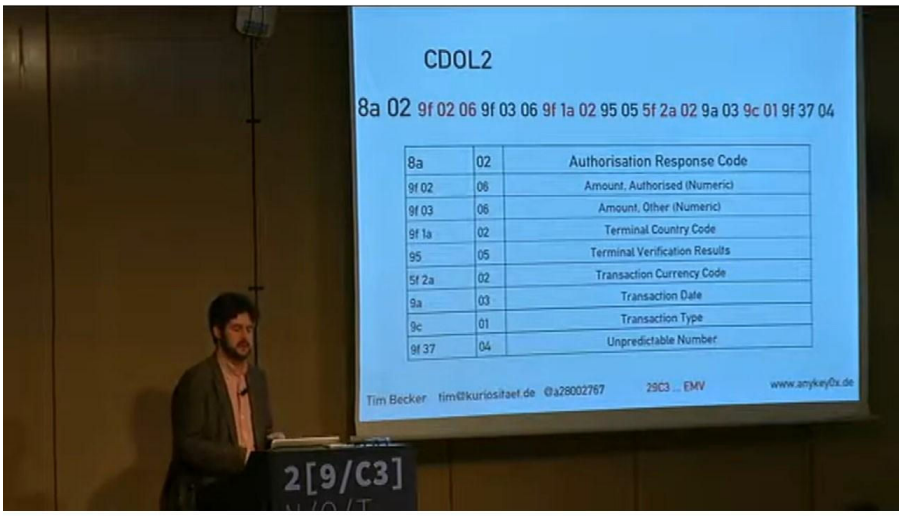
In January 2013, the PCI Security Standards/Council published the Information Supplement[18] that described guidelines for NFC interaction with ATM machines stating that "As cards and the acceptance infrastructure migrate to chip and NFC technologies, ATMs will continue to play a key role in providing increasingly complex services to chip cards and NFC enabled device holders ATM Security Guidelines." Section 3.1.

Further, the minimum set of data elements for EMV cryptograms includes an "Amount, Other (Numeric)." That data element is for use in "cash back" transactions:



[18] Standard: PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI), Version: 1.0, Date: January 2013; Author: PCI Security Standards Council, https://listings.pcisecuritystandards.org/pdfs/PCI_ATM_Security_Guidelines_Info_Supplement.pdf.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 59 of 156



"Amount other would be for cashback" *29C3: A Rambling Walk Through an EMV Transaction (EN) - YouTube*, https://www.youtube.com/watch?v=VdNm9JJmCzg (December 30, 2012), at 45:26. Cash back is an ATM-like feature that allows a merchant to give cash to a debit card user at a merchant point of sale.

L. Magento and PayPal

On or around September 30, 2013, Magento , an open eCommerce platform, announced a new credit card payment solutions for PayPal, namely, a PayPal Credit Card Tokenization extension adds that substituted a token for a credit card number to facilitate PCI DSS compliance:

> You see, what we're talking about isn't actually stored credit card data at all. The PCI DSS compliance that comes with storing sensitive payment data is unfeasible for many online merchants, and secure token alternatives exist in both PayPal and Authorize.Net API integration. These solutions allow the full experience of saved cards for the customer, while the credit card data itself is stored at the payment provider instead of the merchant site.

PayPal Credit Card Tokenization in Magento - SitePoint, https://www.sitepoint.com/paypal-credit-card-tokenization-magento/; *Save Credit Cards With Our Free Magento Extension - Classy Llama*, https://www.classyllama.com/blog/credit-cards-magento-paypal-extension (August 15, 2013); http://www.magentocommerce.com/magento-connect/catalog/product/view/id/18715/s/paypal-credit-card-tokenization-extension-4490/ (October 5, 2013):

M. EMV Tokenisation Framework

On October 1, 2013, the EMV (Visa, MasterCard, American Express) announced a "proposed framework for a new global standard to enhance the security of digital payments and simplify the purchasing experience when shopping on a mobile phone, tablet, personal computer or other smart device," which concerned the use of tokens for mobile transactions. *MasterCard, Visa and American Express Propose New Global Standard to Make Online and Mobile Shopping Simpler and Safer | Global Hub*, https://newsroom.mastercard.com/press-releases/mastercard-visa-and-american-express-propose-new-global-standard-to-make-online-and-mobile-shopping-simpler-and-safer/. The EMV subsequently published *EMV® Payment Tokenisation Specification - Technical Framework v1.0 on or around March 11, 2014. EMVCo To Develop*

Tokenisation Standards, https://www.emvco.com/wp-content/uploads/2017/05/EMVCo_Releases_Technical_Framework_March-2014.pdf.

N. Apple Pay

Apple Pay launched in October 2014 after at least two years of development with partners American Express, MasterCard, and Visa[19]. *Banks Did It Apple's Way in Payments by Mobile* - The New York Times (nytimes.com), https://archive.nytimes.com/dealbook.nytimes.com/2014/09/11/banks-did-it-apples-way-in-payments-by-mobile/ (September 11, 2014). Apple Pay utilized EMV tokenization:

> The token is used in place of an actual credit card number and is what Apple, in its marketing materials, refers to as a unique Device Account Number.
>
> **What the heck is a token?**
> The token itself, as implemented in Apple Pay, is a randomly generated and unique 16-digit number that ostensibly resembles a valid credit card number but is, in fact, fundamentally useless. Think of the token as nothing more than a placeholder or reference ticket for your actual credit card information. The only thing a token has in common with its corresponding credit card number are the last 4 digits on the card.

Apple Pay: An in-depth look at what's behind the secure payment system | Engadget, https://www.engadget.com/2014-10-02-apple-pay-an-in-depth-look-at-whats-behind-the-secure-payment.html (October 10, 2014).[20]

[19] Nimish Shah was the architect and technical domain lead for Visa Token Services from 2011-2017 and focused on Apply Pay Services.

[20] On information and belief and for the reasons described herein, Apple Pay operated like Google Wallet when it was launched in 2014 and as it was developed starting in 2012, with regard to the asserted claims. Samsung will supplement these contentions pending discovery on Apple Pay relating to its development in 2012 through its 2014 launch.

O. Google Wallet Relaunch

Google relaunched Google Wallet in part as Android Pay in 2015. *Android Pay, Google's Apple Pay Rival, Arrives Today* | TechCrunch, https://techcrunch.com/2015/09/10/android-pay-googles-apple-pay-rival-goes-live/. Like the original Google Wallet, Android Pay utilized substitute numbers for the user's PAN:

> Google's system will tokenize card numbers, in the same way that Apple Pay and Samsung Pay do, meaning it generates a one-time payment token for transmission to the receiving terminal for each transaction, rather than just offering the user's static credit card information. This decreases the risk if the transmission is intercepted, since a one-time token with finite expiry is of no use once it's already been consumed.

Android Pay Is Real, And Will Give Developers The Reins As An API | TechCrunch, https://techcrunch.com/2015/03/02/android-pay-is-real-and-will-give-developers-the-reins-as-an-api/?_ga=2.44994596.1274329962.1665514198-1383763186.1651868056 (March 2, 2015).

Most of the systems described above utilized NFC contactless payment technology, including EMV defined cryptograms (defined originally in 2011), tokens, priming and user authentication technologies:

> Contactless mobile payment solutions, such as Apple Pay, must satisfy minimum compliance with the EMV specification 3.0 and the corresponding contactless reader specification of the scheme [20]. Therefore, mobile contactless payments use standard a transaction authorisation method (e.g., ARRQ, ARPC). . . . .
>
> In EMV chip-based credit card payment solutions, we can safely store cryptographic key material within the SE of the smart card. This facilitates the application of strong card authentication and payment authorisation mechanisms. This capability, and the need for secure storage for the cryptographic key material, constitute major requirements for mobile payment solutions. However, mobile phone platform providers do not always provide secure elements (SE) or trusted execution environments (TEE) to guarantee the same security as an EMV chip card. As a mitigation method, EMV [21] incorporates the concept of deriving dynamic cryptographic key material, which facilitates the use of different keys for each payment transaction. In the case that an attacker can eavesdrop on payment

transactions, this prevents the captured data from being used for further reply attacks, i.e., crosscontaminations.

The derivation of the dynamic key material (session key) used in an authorisation cryptogram follows a certain pattern in an EMV transaction, which is described below.

Definition Description

UN Random number generated by the PoS terminal
MAC Message authentication code algorithm used to provide integrity
DDOL Dynamic data authentication data object list
amount Amount payable
Currency Currency code
Exp Date Expiry date
ATC Application transaction counter, incremented after each payment
other data Not specified as standard
DATA Certain relevant customer data used as input for key derivation
tUDK Unique derived token key for this customer
tokenPAN Unique tokenised PAN for this customer
tPAN Unique tokenised PAN for this customer
LUK Derived limited use key for this transaction–session key

Table 2:2 Definitions for Cryptogram and Key Derivation . . . .

User Authentication: Apple Pay's ID&V process (e) for the cardholder enforces biometric fingerprint verification, called Touch Id. The payment process begins at the PoS contactless reader (5). The cardholder presents their NFC interface (c) to the contact reader sign, and identifies themselves as the legitimate cardholder and device owner by authenticating with their fingerprint (Touch Id), which also authorises the payment. Importantly, the wallet always asks for fingerprint authentication.

User Authentication: Android Pay's ID&V process (e) for the cardholder supports biometric fingerprints, IRIS scans, standard PIN codes, or pattern based authentication to authorise payment transactions, where no authentication method is enforced.

After five unsuccessful attempts [34] to match a fingerprint, the device allows for passcode authentication.

Apple Pay: How different is it from other Pay solutions, what role does tokenisation play, and to what degree can Card not Present payment benefit from Apple Pay in future Marcel Fehr

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 64 of 156

Technical Report RHUL–ISG–2018–3, 3 April 2018, https://www.royalholloway.ac.uk/media/5612/rhul-isg-2018-3-techreport-marcelfehr.pdf.

P. Samsung MST

When Samsung launched Samsung Pay in 2015, it included MST. *Samsung Announces Launch Dates for Groundbreaking Mobile Payment Service: Samsung Pay – Samsung Global Newsroom*, https://news.samsung.com/global/samsung-announces-launch-dates-for-groundbreaking-mobile-payment-service-samsung-pay (August 14, 2015). MST, which stands for Magnetic Secure Transmission, is a "method of sending data using magnetic waves. MST replicates a card swipe by wirelessly transmitting magnetic waves from the supported Samsung device to a standard card reader. MST turns every card reader into a contactless payment receiver." *S-Pay: What is MST? | Samsung Levant*, https://www.samsung.com/levant/support/mobile-devices/s-pay-what-is-mst/. The MST technology was purchased by Samsung via its acquisition of LoopPay in February 2015. *SAMSUNG to Acquire LoopPay, Transformative Digital Wallet Platform - Samsung US Newsroom*, https://news.samsung.com/us/431-2/ (February 18, 2015). LoopPay began its development of MST technology at least as early as 2012. That technology included a keyfob with no card number markings thereon that could be used for contactless transactions. *KickStarter*, https://www.kickstarter.com/projects/loop/pay-with-loop. *See Loop Architecture, Card Loading and Security (2013)* regarding other LoopPay technology. In February 2021, Samsung started to phase out MST from its devices. *Samsung Begins to Phase Out Support of MST for Samsung Pay - PaymentsJournal*, https://www.paymentsjournal.com/samsung-begins-to-phase-out-support-of-mst-for-samsung-pay/.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 65 of 156

Q. Google's Patents

Google owns multiple patents and patent applications relating to NFC and other aspects of contactless transactions and online payment transactions having a priority date earlier than March 2013. A selected list of those is presented here:

Application No.	Patent/Publication No.	Title
11/413,330	U.S. 7,907,896	Mobile Commerce Method and Device
13/244,806	U.S. 8,196,131	Payment Application Lifecycle Management in a Contactless Smart Card
13/475,112	U.S. 8,401,904	Real-Time Payment Authorization
13/472,441	U.S. 8,422,949	Public Kiosk Providing Near Field Communication Services
13/846,924	U.S. 8,626,592	Real-Time Payment Authorization
13/970,548	U.S. 8,814,055	Secure Application Directory
13/408,794	U.S. 8,898,088	In-Card Access Control and Monotonic Counters for Offline Payment Processing System
13/315,818	U.S. 9,008,616	Point of Sale Processing Initiated by a Single Tap
14/324,416	U.S. 9,198,214	Detecting a Communication Tap Via Signal Monitoring
13/412,957	U.S. 9,355,391	Digital Wallet
13/731,090	U.S. 10,127,533	Managing Devices Associated with a Digital Wallet Account
11/618,135	U.S. 10,311,427	Method and System for Monitoring Secure Application Execution Events During Contactless RFID/NFC Communication
13/246,076	U.S. 2012/0143703	Multiple Contactless Device Interactions and Communication Protocols Per Tap
13/970,573	U.S. 2014/0052637	Portable Device Wireless Reader and Payment Transaction Terminal Secure Memory Functionality
13/436,819	U.S. 2016/0132859	Initiating Peer-to-Peer Transactions with a Magnetic Strip Card

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 66 of 156

Application No.	Patent/Publication No.	Title
13/410,209	U.S. 2016/0132918	One-Tap Sign Up for Merchant Loyalty Programs
2011343474	AU 2011343474B	Local Trusted Services Manager for a Contactless Smart Card
2012308186	AU 2012308186B2	One-Click Offline Buying
2013201076	AU 2013201076B2	Fraud Protection for Online and NFC Purchases
PCT/US2011/063091	CA 2819830A1	Multiple Device Interactions and Communication Protocols per Tap
2820963	CA 2847942C	Writing Application Data to a Secure Element
PCT/US2013/042455	CA 2874652C	Systems, Methods, and Computer Program Products for Providing a Contactless Protocol
2012CN-80048309	CN 103843020B	One-Click Offline Purchase
PCT/US2013/035521	EP 2671198B1	Secure Reset of Personal and Service Provider Information on Mobile Devices

R. Every Element of the Asserted Claims was Known in the Art Before March 2013

- Combining the functionality of an NFC contactless card with a mobile device for mobile transactions:

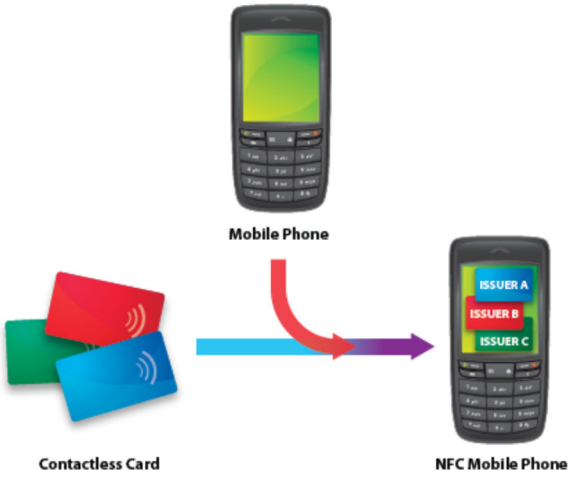


Figure 2.1 Concept of the NFC Mobile Phone

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 67 of 156

Essentials for Successful NFC Mobile Ecosystems, October 2008

(https://www.slideshare.net/Tmac77/nfc-forum-mobile-nfc-ecosystem-white-paper.)

- The use of **tokens** to replace a credit card number:
    - PCI DSS Information Supplement Tokenization (pcisecuritystandards.org), https://listings.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf, August, 2011.
    - Visa Best Practices for Tokenization Version 1.0, *bulletin-tokenization-best-practices.pdf (visa.com)*, https://usa.visa.com/dam/VCOM/global/support-legal/documents/bulletin-tokenization-best-practices.pdf
    - *Near-Field Communication-Based Secure Mobile Payment Service*, ICEC'09, August 12–15, 2009, Taipei, Taiwan
      "While our payment message conforms to the traditional payment processing protocol, our proposal replaces the sensitive information, such as bank account number (PAN) and password (PIN), with an authorization token. The processing of the transaction request at the mobile banking channel involves the validation of the authorization token (the validation procedure will be detailed in Section 5). The credit/debit transaction relies on a validated authorization token to ensure the correct customer account and actual payment amount specified by the mobile user."
    - https://web.archive.org/web/20121103225221/http://www.hotel-online.com/News/PR2005_4th/Oct05_Shift4.html
    - *What is Tokenization? - YouTube*, https://www.youtube.com/watch?v=ypm5FFfEN34 (January 17, 2011),
      "Tokenization is a best practice technology that replaces sensitive financial account information in an ACH transaction or credit & debit card information in a card-based transaction with a random character string, or token. The technology is used to prevent the theft of credit card or bank account data while in transmission or storage. Instead of storing financial account information in your system, you submit that information to PaymentVision via a PayAPI web service. The PaymentVision token manager generates a token which is returned in the web service response, while the financial account information is securely stored in our token vault. You store the token in your system instead of financial account data for use with future authorizations."
    - *CardVault by 3Delta Systems - Securing Credit Card Payments for B2B and B2G through Tokenization - YouTube*, https://www.youtube.com/watch?v=h3zuiLiF51k (February 1, 2010).

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 68 of 156

- virtual terminal- #1 storing credit card data with tokenization - YouTube, https://www.youtube.com/watch?v=eSXIlGbACew (*virtual terminal- #1 storing credit card data with tokenization*, Feb 28, 2011) "Virtual Terminal tokenization demo shows how to store encrypted credit card data for variable amount billing. Most virtual terminals offer a recurring billing option for the same dollar amount. Our PCI Compliant solution solves the card storage problem for B2B, attorney, and many others with a secure token to rebill customers, without storing card data internally, for different amounts on each invoice."

- *Credit Card Processing with EPX BuyerWall Tokenization - YouTube*, https://www.youtube.com/watch?v=_7E5hj9li4g (Credit Card Processing with EPX BuyerWall Tokenization, Dec 21, 2010).

- *How Credit Card Number Tokenization can Reduce PCI Compliance Stress - File 1 of 3 - YouTube*, https://www.youtube.com/watch?v=FHD5XzAlKDI (How Credit Card Number Tokenization can Reduce PCI Compliance Stress - File 1 of 3, Jul 28, 2009), "EPX Webinar with Matt Ornce – 'HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS...AND DATA PROTECTION COSTS' A joint presentation by The PCI Knowledge Base and Electronic Payment Exchange (EPX) Matt Ornce, COO and Chief Security Officer of EPX (www.epx.com), discusses the key criteria to be considered when evaluating cardholder data replacement solutions as an alternative to full encryption."

- *"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS" - File 2 of 3 - YouTube*, https://www.youtube.com/watch?v=t-fWpcLdb3o ("HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS" Jul 28, 2009), "Webinar with Dave Taylor – 'HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS...AND DATA PROTECTION COSTS' A joint presentation by The PCI Knowledge Base and Electronic Payment Exchange (EPX), Dr. Dave Taylor, Founder of The PCI Knowledge Base (www.pciknowledgebase.com), is a leading authority on PCI compliance and a long-time Gartner Group senior analyst. Dr. Taylor will present the latest research on what leading organizations are thinking about tokenization as a solution and review the timely debate over end-to-end encryption vs. credit card data "tokenization."

- *HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS - File 3 of 3 - YouTube*, https://www.youtube.com/watch?v=_CdoKEuEB9s (HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS - File 3 of 3, July 28, 2009, "Webinar with Dave Taylor - "HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS...AND DATA PROTECTION COSTS", A joint presentation by The PCI Knowledge Base and Electronic Payment Exchange

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 69 of 156

(EPX), Dr. Dave Taylor, Founder of The PCI Knowledge Base (www.pciknowledgebase.com), is a leading authority on PCI compliance and a long-time Gartner Group senior analyst. Dr. Taylor will present the latest research on what leading organizations are thinking about tokenization as a solution and review the timely debate over end-to-end encryption vs. credit card data "tokenization."

- Encryption_vs_Tokenization.pdf (townsendsecurity.com), https://townsendsecurity.com/sites/default/files/Encryption_vs_Tokenization.pdf (2010). "The token value does not contain sensitive information, it replaces it, maintaining the original value. There is one and only one token value for any given original value. For example, a credit card number 4111-1111-1111-1111 might be assigned the token value of 1823-5877-9043-1002. Once this token is assigned it will always be used when the original value would have been used."

- *Tokenization Guidance: How to reduce PCI compliance costs*, https://web.archive.org/web/20121015212221/https://gateway.elavon.com/documents/Tokenization_Guidelines_White_Paper.pdf (December 10, 2011, archived October 15, 2012)

- Tokenization: What's Next After PCI (moneymint.com), https://moneymint.com/wp-content/uploads/2021/03/Tokenization-Whats-next-after-PCI.pdf (2012).

- WO 2005/119607 A2 (single transaction tokens)

- The use of a **cryptograms** and related algorithms for credit card transaction security to provide one-time or limited use data for transaction authorization and authentication:

  - EMV Integrated Circuit Card Specifications for Payment Systems. Book 2, Security and Key Management, Version 4.3, November 2011, https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_2_Security_and_Key_Management_20120607061923900.pdf.

    - And see earlier versions of the same: EMV Integrated Circuit Card Specifications for Payment Systems Book 2 Security and Key Management Version 4.1 May 2004, http://mech.vub.ac.be/teaching/info/mechatronica/finished_projects_2007/Groep%201/Smartcard_files/EMV%20v4.1%20Book%202.pdf

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 70 of 156

- EMV®* Contactless Specifications for Payment Systems, Book B, Entry Point Specification, Version 2.1, March 2011 and earlier 2004 version

- EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements, Version 4.3, November 2011 and earlier 2004 version

- EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3, November 2011 and earlier 2004 version

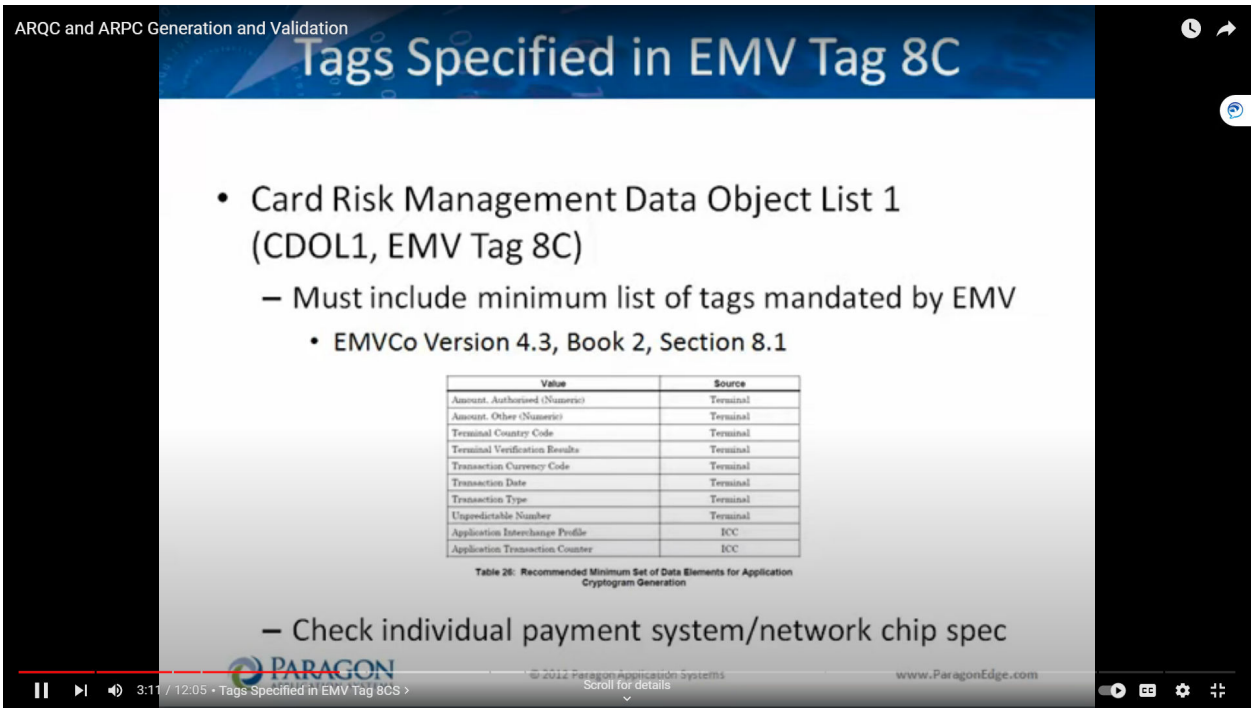
- EMV Integrated Circuit Card Specifications for Payment Systems, Book 3, Application Specification, Version 4.3, November 2011) and earlier 2004 version.

- *The future is now*, Industrial Engineer, June 2006, Copyright 2006 ProQuest Information and Learning, Copyright 2006 Institute of Industrial Engineers, Section: Pg. 36; Vol. 38; No. 6; ISSN: 1542-894X (emphasis added).

    - "American Express was the first credit card company in the United States to launch contactless credit cards when it unveiled the latest version of Blue in June 2005. The Blue card features an embedded computer chip powered by radio frequency technology. Developed by Texas Instruments, the technology has also found its way into MasterCard's contactless payment solution called MasterCard PayPass. The credit card companies are wagering that the increased consumer convenience provided by the hassle-free payment option will increase sales, says Trevor Pavey, manager of contactless payments for Texas Instruments. And Texas Instruments, which has been in the radio frequency identification market for 16 years, is exclusively placing its technology in the smart cards rolled out by the companies. . . . Pavey says that the credit card companies have added additional security applications in their contactless solutions. "Each transaction is unique, ***and a cryptogram is generated by the transponder by the secure microcontroller in the payment token***," he says. "That cryptogram is sent to the backend authorization network so each transaction is unique and secure."

- *ARQC and ARPC Generation and Validation*, https://www.youtube.com/watch?v=I1XTn175FFk (July 25, 2012, Paragon Application Systems):

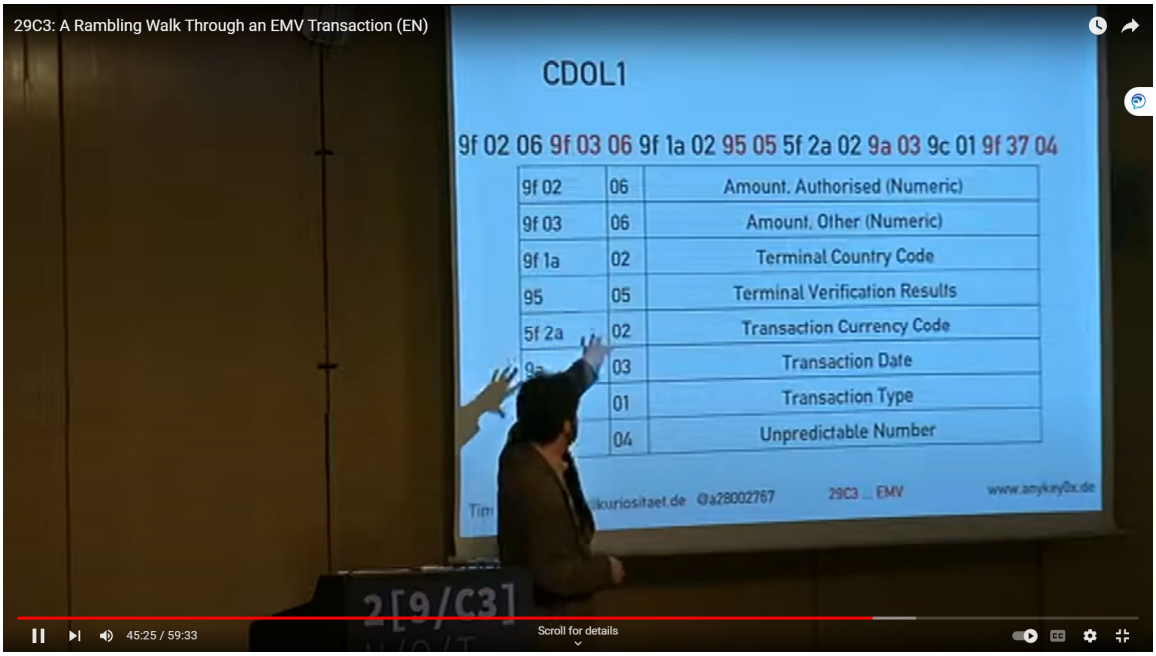
CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 71 of 156

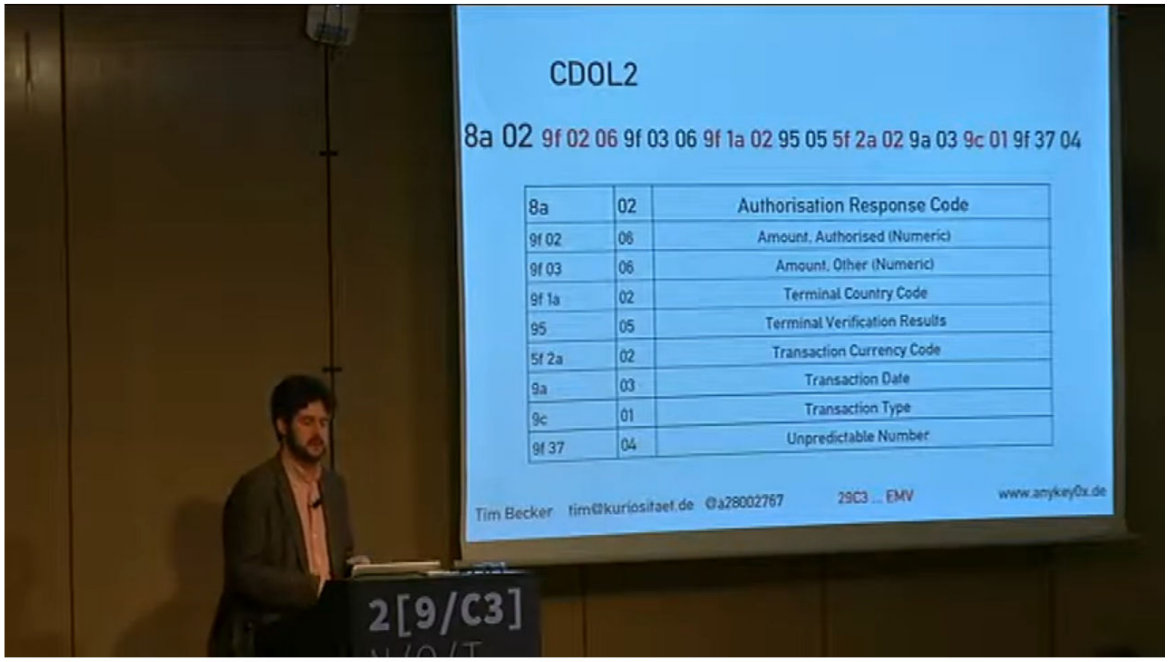


Note particularly that at 2:50, the narrator explains that EMV specifications from the "various payment systems" such as American Express, Visa, and MasterCard can require additional tags than those identified in Section 8.1 above. The beginning of the video explains that a significant benefit of the EMV specification is the reduction of card counterfeit fraud.

And, relatedly,
https://web.archive.org/web/20120818221214/http://www.paragonedge.com/solutions/emv-solutions.html

- *29C3: A Rambling Walk Through an EMV Transaction (EN) - YouTube*, https://www.youtube.com/watch?v=VdNm9JJmCzg (December 30, 2012):





- The use of **<u>NFC and other wireless communications methods</u>** for transmitting card payment information for mobile payments:

    - *Samsung and Visa join forces to enable NFC mobile payment at 2012 Olympics | Engadget*, https://www.engadget.com/2011-04-01-samsung-and-visa-join-forces-to-enable-nfc-mobile-payment-at-201.html

- *Samsung and Visa to Showcase Mobile Payments @ the London Olympics – Samsung Global Newsroom*, https://news.samsung.com/global/samsung-and-visa-to-showcase-mobile-payments-the-london-olympics

- *Samsung Galaxy S III for Verizon Wireless review | Engadget*, https://www.engadget.com/2012-07-09-samsung-galaxy-s-iii-review-verizon-wireless.html

- Samsung picks NXP for S3 • NFCW, https://www.nfcw.com/2012/05/14/315663/samsung-picks-nxp-for-s3/

- Visa PayWave

- MasterCard PayPass

- American Express ExpressPay

- Discover Zip

- **Combining** tokens and cryptograms for contactless payment:

  - American Express ExpressPay

  - *Near-Field Communication-Based Secure Mobile Payment Service*, ICEC'09, August 12–15, 2009, Taipei, Taiwan

    - While our payment message conforms to the traditional payment processing protocol, our proposal replaces the sensitive information, such as bank account number (PAN) and password (PIN), with an authorization token.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 74 of 156

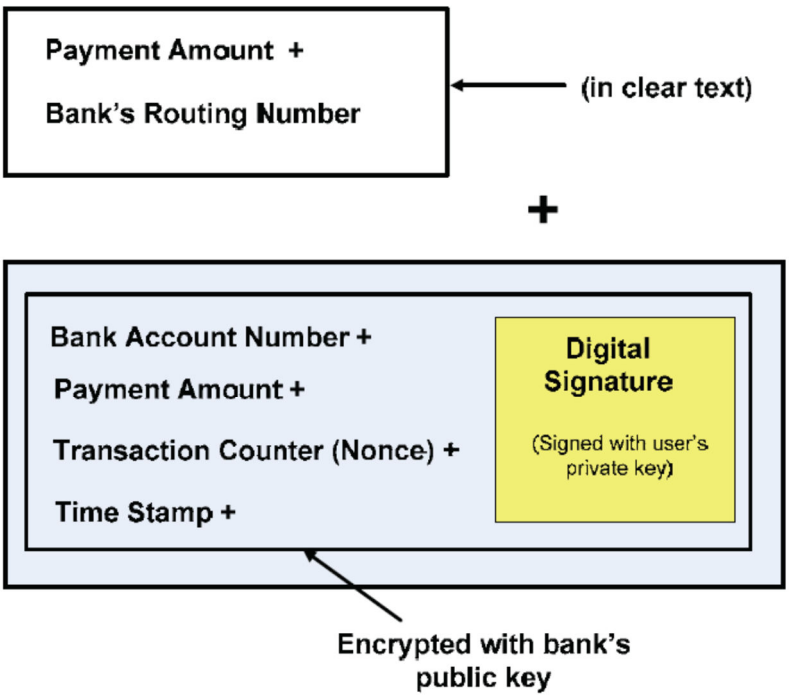


Figure 3. Payment authorization token issued from mobile phones.

- *Contactless Payment: Secure Enough*?, Card Technology, September, 2005, Copyright 2005 SourceMedia, Inc., Section: SPECIAL ISSUE: CONTACTLESS TECHNOLOGY; Vol. 10; No. 8; Pg. 36 (emphasis added).

  - "Contactless payment cards and ***tokens*** might speed consumers through checkout lines, but what about security? . . . Could thieves steal contactless payment data from cardholders? But stolen card numbers won't automatically translate into massive fraud. For example, American Express doesn't transmit actual card numbers during contactless transactions, says David Bonalle, the company's vice president and general manager of advanced payments. ***The number transmitted instead links to the customer's account***. . . . However, a contactless transaction does ***include transmission of a cryptogram, encrypted data that is based in part on the number of transactions that the contactless card has initiated previously***. The cryptogram changes with each purchase-it would be different for the second purchase than the first. Because virtually all U.S. card transactions are authorized at the time of purchase, the issuer can spot an out-of-sequence cryptogram, such as receiving more than one cryptogram saying this is the card's first transaction. That would be a red flag, says Bruno Carpreau, a MasterCard vice president at the company's Global Chip Center of Excellence."

- *The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options*, Economic Review - Federal Reserve Bank of Kansas City, Second Quarter 2010, Copyright 2010 ProQuest Information and Learning, Copyright 2010 Federal Reserve Bank of Kansas City, Section: Pg. 101; Vol. 95; No. 2; ISSN: 0161-2387, p. 8/18 (emphasis added):

    - Data breaches and their consequences have led elements of the U.S. payment industry to explore ways to improve card payment security. Card issuers have been deploying contactless payment cards, which have a small radio to transmit card information to a payment terminal. Because it is difficult to counterfeit these cards, they are considered more secure than magnetic stripe cards. Issuers are considering an upgrade to EMV-compliant contactless cards, ***which will use a cryptogram (an encrypted identifying number for each transaction)*** to allow the card issuer to check the authenticity of the payment card and the uniqueness of the transaction. Two initiatives are being developed in the merchant community in cooperation with payment service providers. One initiative targets a weakness in the PCI DSS, which requires encryption of sensitive card data when it is transmitted over public networks, but not when transmitted over private networks. Merchants are investigating "end-to-end encryption," which would encrypt payment data over the entire communications channel from the point-of-sale terminal to the card issuer (Hernandez). ***Another initiative disguises a card account number by replacing it with a token number.*** This "tokenization" would occur after a card payment has been authorized so that a merchant can store the transaction information without having to store the card account number (Taylor). Merchants can retrieve the card account number for later processing, if needed. Both of these options could make merchant and processor computer networks less of a target because they would not store or transmit sensitive payment card information in forms that would be useful to hackers."

- Google Wallet Virtual Credit Card

- The use of touchscreens and **user interface elements** and sensors for mobile devices to facilitate **user interactions**, including **tapping**, **human presence** sensing, and user action **confirmation**:

    - Google I/O 2012 - Introducing Google Wallet Cloud APIs - YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY (Google I/O 2012 - Introducing Google Wallet Cloud APIs, June 29, 2012), "There have been exciting developments in the world of Payments at Google as we move forward with our digital wallet, and we have new APIs to share with you.

Come and join us as we kick off the Commerce track at Google I/O 2012 with Peter Hazlehurst, Global Head of Product Management, Payments."

- Google Wallet- How to Setup and Use this Exciting NFC Technology - YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs (Google Wallet- How to Setup and Use this Exciting NFC Technology, July 26, 2012).

- NFC - Google Wallet and More - EE Times - Mobile World Congress - YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw (NFC - Google Wallet and More - EE Times - Mobile World Congress, Mar 6, 2012)

- *Samsung Galaxy SIII, Verizon, User Manual*, 2012, e.g., p. 38, 50, 65, 86, 110, 157 (user interface and button action confirmation)

- Credit card or other bill, cash register display, web purchase confirmation page (displaying the result of a transaction)

- https://discussions.apple.com/thread/3690633 (Limiting the number of password attempts and locking a device after an predetermined number of failed attempts, or allowing a retry after a predetermined amount of time)

- https://www.youtube.com/watch?v=npD48agt0xY (T-Mobile proximity sensor)

- https://www.youtube.com/watch?v=Q0V_ld7iNw4 ("Android sensors: accelerometer, gyroscope, light, and more.")

- Android 4.0 APIs | Android Developers (mit.edu), https://stuff.mit.edu/afs/sipb/project/android/docs/about/versions/android-4.0.html (General Android 4.0 user interface components)

- Fitbit, https://web.archive.org/web/20120620210558/http://www.fitbit.com/product/specs

- Motorola MotoACTV Smartwatch, http://www.manualplanet.com/pdf/watches/motorola/motorola-motoactv-gps-fitness-tracker-quick-start-guide.pdf, (tapping and sensors)

TOUCH TIPS

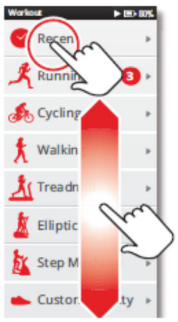
It's all in the touch:

Touch: Touch to choose an option, see more workout details, or zoom on maps.

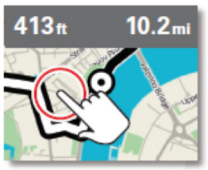
Tap: While in a workout, tap with your whole hand to get spoken feedback about your workout progress or to switch to the next lap.

Drag: Scroll or move.

Tip: There's more about maps and tapping in the full user guide online. Check it out.



Touch to select an item, see more details, or zoom.



Drag to scroll panels (or long lists).

SENSORS

Before you get your blood pumping, connect your heart rate monitor, foot pod, or bike sensor. Turn on your ANT+ or BLE sensor (sold separately) in range of your device. Touch **Settings** > **Wireless** > **Sensors** > **Add New Sensors** to connect.

Note: Your device needs to acquire a GPS signal before you start an outdoor workout. GPS acquisition may take a couple of minutes. Stand in an open area with a clear view of the sky. GPS performance tips: for running/walking, use the wristband or armband; for cycling, use the bike mount. If using the clip, put it at chest level or higher, like upper arm.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 78 of 156

Additional patents and publications describing the state of the art include: U.S. Patent No. 7,590,846; U.S. Patent No. 9,033,218; U.S. Patent No. 9,105,021; U.S. Patent No. 9,171,302; U.S. Patent No. 10,515,359; U.S. Patent No. 11,836,706; U.S. Patent Application Publication No. 2002/0198848; U.S. Patent Application Publication No. 2007/0294182; U.S. Patent Application Publication No. 2009/0048971; U.S. Patent Application Publication No. 2009/0159696; U.S. Patent Application Publication No. 2009/0210308; U.S. Patent Application Publication No. 2010/0125509; U.S. Patent Application Publication No. 2010/0131415; U.S. Patent Application Publication No. 2010/0299267; U.S. Patent Application Publication No. 2011/0251962; U.S. Patent Application Publication No. 2013/0036050; U.S. Patent Application Publication No. 2013/0124292; U.S. Patent Application Publication No. 2013/0134216; U.S. Patent Application Publication No. 2013/0191290; U.S. Patent Application Publication No. 2013/0246202; U.S. Patent Application Publication No. 2013/0262317; U.S. Patent Application Publication No. 2015/0134540; U.S. Provisional Patent Application No. 61/635,277; U.S. Provisional Patent Application No. 61/647,112; U.S. Provisional Patent Application No. 61/713,302; Japanese Patent Application No. 2011053931A; Korean Patent Application No. 20120095275A; Molloy, et al, "Dynamic Virtual Credit Card Numbers."

II. IDENTIFICATION OF PRIOR ART

In addition to the prior art identified in the prosecution history of the Asserted Patent, Defendant also relies upon the prior art identified pursuant in the attached Exhibits in support of these Invalidity Contentions. Defendant's identification of patents and publications as prior art herein and in the attached claim charts includes the publications themselves, as well as the use of the products, devices, apparatuses and/or systems described therein. Although Defendant's investigation continues, information available to date indicates that such products, devices, and systems were known or used before the alleged filing date of the Asserted Claims. These prior

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 79 of 156

art products, devices, apparatuses, and systems, and their associated references anticipate and/or render obvious each of the Asserted Claims.

Defendant further intends to rely on inventor admissions concerning the scope of the prior art relevant to the Asserted Patent found in, *inter alia*, the prosecution history of the Asserted Patent and any related patents, patent applications, and/or post-grant proceedings including reexaminations and *inter partes* reviews; any deposition testimony of a named inventor on the Asserted Patent; and the papers filed and any evidence submitted by Plaintiff in conjunction with this litigation.

Discovery is in its earliest stages, and Defendant's prior art investigation, including via discovery and third-party discovery, is therefore not yet complete. Defendant reserves the right to rely upon additional evidence of invalidity obtained in the future, to the extent that further investigation and discovery yield information forming the basis for such claims.

A. Applicant-Admitted Prior Art[21]

The Asserted Patents admit that the following techniques and technology was known in the art:

- There are several different types of credit cards available in the marketplace at present. A first type of credit card is a conventional, standard piece of plastic with a magnetic strip, which is readily available and in wide commercial use. The advantage of this first type of credit card is that a large portion of the infrastructure for credit card transactions is

[21] This section is for illustrative purposes only, as it is not required by the Scheduling Order or Standing Order. As such, Defendant reserves all rights to contend that additional or different prior art was admitted by the applicant.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 80 of 156

built around this type of card, and consequently such a card works in a wide array of vendors' credit card machines, automated teller machines (ATMs), and other devices that support the present credit card and banking infrastructure. ('520, 1:32-40)

- Another type of credit card device employs the use of a smart integrated circuit chip. These types of credit cards have a built in microprocessor with cryptographic capabilities. These microprocessors operate in a similar manner to a cell phone having a chip comprising a cryptographic processor. Such a smart card device requires contact with a reader in order to be read and to perform a transaction. The reader provides the manner in which a facility interacts with the built-in processor on the card, e.g., for purposes of performing verification on the authenticity of the card or for making a direct deposit on the card. These credit card devices also comprise a magnetic strip such that they are compatible with standard plastic credit card readers in wide use. ('520, 1:42-55)
- A different type of credit card device in circulation employs radio frequency identification ("RFID"). These cards essentially have a low-power RF antenna built into the card, and when the cardholder passes the antenna in front of a reader comprising an RF field, enough power is generated to enable the processor to interact wirelessly with the receiving device. ('520, 1:56-61).
- In other instances, well-known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the present disclosure. ('520, 3:54-57). Including, but not limited to:
    - Credit cards operating by NFC. ('520, 6:36-39).
    - Planar coils ('520, 4:33)
    - Touch sensor array ('520, 5:47-48)

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 81 of 156

- Processor unit (’520, 6:7)
- Memory (’520, 5:32)
- Real-Time Clock (’520, 5:47)
- Backup Power Source (’520, 5:54)
- Optical sensor array (’520, 7:22-23)
- Accelerometer (’520, 7:23)
- Conventional credit card readers (’520, 7:30)
- Password protection (’520, 9:27)
- USB connections (’520, 11:57-66)
- “conventional credit cards utilizing wireless communication means” (’520, 14:9-10)
- a computer system or integrated circuit, or similar electronic device, including an embedded system (’520, 4:19-21)
- a display (’520, 5:51-54)
- a touch screen panel (’520, 5:50)
- a touch-sensor array (’520, 6:29-30)
- a keypad (’520, 5:51)
- conventional magnetic card readers (such as point-of-sale locations, banks, and ATMS) (’520, 12:44-46)
- credit cards utilizing wireless communication (’520, 14:9)
- biometric input (’520, claim 11)
- biometric user identification (’520, claim 19)
- a biometric sensor (’520, claim 20)

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 82 of 156

- a “proximity contact sensor” (’520, claim 11)
- ATMs capable of performing transactions wirelessly with a user’s electronic device (’520, claim 18)
- Accelerometers (’520, 5:41)
- Cryptocurrency addresses (’520, claim 13)
- Cryptocurrency keys (’520, claim 13)
- Cryptocurrency public keys (’520, claim 22)
- Cryptocurrency private keys (’520, claim 22)
- Cryptocurrency network (’579, claim 17)
- Cryptocurrency server (’520, claim 22)
- Cryptocurrency server (’520, claim 22)
- Cryptocurrency types (’520, claim 22)
- Biometrically sensed user information (’520, claim 22)
- Credit Card Authority/Payment Issuing Authority (’520, 10:12, 10:26, claim 7, claim 17)
- Conventional Functions (e.g., Reject[ing], ’820, claim 4; Cryptographically Dynamically Generat[ing], ’520, 1:46-47, ’820 claim 10; Combination, ’820 claim 10; Adjusting, ’820 claim 20; Denying, ’820 claim 20; Approving, 20 claim 20)
- Personal computing device (’820 claim 11)
- Cell phone (’520 1:46)
- Payment card numbers, including account number, expiration date, and security code (’820 claim 18)

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 83 of 156

- Motion rate detection array (’520 2:51)
- Device-specific and user-specific information (’520 claim 1)
- Static numbers (’520 10:34)
- Counter (’520 claim 5)
- Hash (’520 13:51)

Device identifiers/keys (’520 claim 12)

B. Prior Art Patents

Defendant contends that the following prior art patents anticipate or render obvious one or more Asserted Claims of the Asserted Patents under Pre-AIA 35 U.S.C. § 102(a) and (b), AIA 35 U.S.C. § 102(a) or Pre-AIA and AIA 35 U.S.C. § 103.

Country	Patent/Publication No.	Issue or Publication Date	Inventor (et al.)
US	9,600,808	March 21, 2017	Gomez
US	2013/0124410	May 16, 2013	Kay
US	2008/0319905	December 25, 2008	Carlson
US	2010/0185545	July 22, 2010	Royyuru
US	2013/0262305	October 3, 2013	Jones
PCT	WO 2012/154915	November 15, 2012	Mullen
US	2006/0089171	April 27, 2006	Yoo
US	9,098,846	September 6, 2012	Gill
US	2009/0048971	February 19, 2009	Hathaway
US	2013/0232083	September 5, 2013	Smith
US	7,690,580	April 4, 2010	Shoemaker
US	2008/0126260	May 29, 2008	Cox

Country	Patent/Publication No.	Issue or Publication Date	Inventor (et al.)
US	8,499,334	March 15, 2012	Doughty
PCT	WO 2005/119607	December 15, 2005	Spitzer
US	2008/0222047	September 11, 2008	Boalt
GB	2,485,442	May 16, 2012	Dixon
US	11,100,431	November 15, 2012	Mullen
US	8,255,323	August 28, 2012	Casey
US	2008/0172317	July 17, 2008	Deibert
US	2009/0159701	June 25, 2009	Mullen
US	2012/0317035	December 13, 2012	Royyuru
US	8,423,462	April 16, 2013	Amacker
US	2012/0310760	December 6, 2012	Phillips
US	2008/0302876	December 11, 2008	Mullen
US	2015/0147065	May 28, 2015	Civelli
US	2014/0143785	May 22, 2014	Mistry
US	10,460,314	January 15, 2015	Hird
US	9,846,866	August 28, 2008	Royyuru
US	8,052,052	November 8, 2011	Power
US	2007/0278291	December 6, 2007	Rans
US	2012/0150750	June 14, 2012	Law
US	2013/0036050	February 7, 2013	Giordano
US	2015/0134540	May 14, 2015	Law
US	7,280,096	October 9, 2007	Marvit
US	7,907,838	March 15, 2011	Nasiri

Country	Patent/Publication No.	Issue or Publication Date	Inventor (et al.)
US	9,619,741	April 11, 2017	Rigatti
US	2012/0123937	May 17, 2012	Spodak

C. Prior Art Publications to the Asserted Patents

Defendant contends that the following publications anticipate or render obvious one or more Asserted Claims of the Asserted Patents under Pre-AIA 35 U.S.C. § 102(a) and (b), AIA 35 U.S.C. § 102(a), or Pre-AIA or AIA 35 U.S.C. § 103.

Publication Title	Date	Publisher	Author (et al.)
A web transaction security scheme based on disposable credit card numbers	2007 (Vol. 1, No. 2)	Int. J. Electronic Security and Digital Forensics	Assora
Implementing disposable credit card numbers by mobile phones	February 23, 2011	Electron. Commer. Res.	Buccafurri
A new credit card payment system based on 3D-Secure using one-time-use transaction numbers	2010 (Vol. 1)	Information Assurance and Security Letters	Javani
A security-enhanced one-time payment scheme for credit card	March 28, 2004	IEEE	Li
A pragmatic approach to temporary payment cards numbers	2009 (Vol. 2, No. 3)	Int. J. Electronic Security and Digital Forensics	Boyd
EMV Integrated Circuit Card Specifications for Payment Systems. Book 2, Security and Key Management, Version 4.3, November 2011	November, 2011	EMVCo.	EMV
EMV Integrated Circuit Card Specifications for Payment Systems Book 2 Security and	May, 2004	EMVCo.	EMV

Publication Title	Date	Publisher	Author (et al.)
Key Management Version 4.1 May 2004			
Standard: PCI Data Security Standard (PCI DSS), Version: 2.0, Information Supplement: PCI DSS Tokenization Guidelines	2011	PCI Security Standards Council	Scoping SIG, Tokenization Taskforce PCI Security Standards Council
Visa Best Practices for Tokenization Version 1.0	July 14, 2010	Visa	Visa
ISO/IEC7812 (Card issuers numbering)		ISO	ISO
ISO/IEC14443 (contactless operation)		ISO	ISO
ISO/IEC 7816 (smartcard hardware, commands, command management)		ISO	ISO
Publications and videos identified hereinabove describing the operation of Google Wallet	Various (see above)	Various (see above)	Various (see above)
Publications and videos identified hereinabove describing the operation of Google Checkout	Various (see above)	Various (see above)	Various (see above)
Publications and videos identified hereinabove describing the operation of ISIS (later SmartCard)	Various (see above)	Various (see above)	Various (see above)
Publications and videos identified hereinabove describing the operation of Visa PayWave	Various (see above)	Various (see above)	Various (see above)
Publications and videos identified hereinabove	Various (see above)	Various (see above)	Various (see above)

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 87 of 156

Publication Title	Date	Publisher	Author (et al.)
describing the operation of MasterCard PayPass			
Publications and videos identified hereinabove describing the operation of American Express	Various (see above)	Various (see above)	Various (see above)
Publications and videos identified hereinabove describing the operation of Discover	Various (see above)	Various (see above)	Various (see above)
Publications and videos identified hereinabove describing the operation of PayPal (eBay)	Various (see above)	Various (see above)	Various (see above)
Publications and videos identified hereinabove describing the operation of Magento (Adobe)	Various (see above)	Various (see above)	Various (see above)
Publications and videos identified hereinabove describing the operation of Apple Pay	Various (see above)	Various (see above)	Various (see above)
A New Secure Wireless Financial Transaction Architecture	2005	EUROCON 2005	Killoran
On-Line E-Wallet System with Decentralized Credential Keepers	2003	Mobile Networks and Applications	Mjølsnes
Interactive Shopping with Mobile Wallet	2012	World Congress on Sustainable Technologies	Qasim
What Would You Do with a Hundred MIPS on Your Wrist?	January 22, 2001	RC 22057	Narayanaswami

Publication Title	Date	Publisher	Author (et al.)
How to grab a screenshot from iPhone, Android, and nearly any other smartphone	April 20, 2012	Computer World	Purdy

D. Prior Art Public Use/Disclosure/Sales/Offers for Sale to the Asserted Patents

On information and belief, Defendant contends that the following items, which were used and/or offered for sale before the relevant filing dates, anticipate or render obvious one or more Asserted Claims of the Asserted Patents under pre-AIA 35 U.S.C. § 102(b) and/or post-AIA 35 U.S.C. § 102(a) or 35 U.S.C. § 103.

Item Name or Description	Date Available	Manufacturer
Google Wallet[22]	Mid-2011	Google
Google Checkout	2006	Google
ISIS (later SoftCard)	2012	Verizon, AT&T, T-Mobile
Visa PayWave, for contactless card and contactless mobile device transactions	At least 2008 for contactless cards; 2012 for contactless mobile device transactions (e.g., London Olympics)	Visa

[22] By identifying Google Wallet and Google Checkout in these invalidity contentions, Google makes no admissions and does not concede that any facts, allegations, or legal conclusions in Plaintiff's infringement contentions, complaint, or any other pleadings or papers are true. Instead, Plaintiff's infringement contentions merely reflect Plaintiff's admission that—based on Plaintiff's erroneous factual and legal conclusions, and unfounded claim interpretations, with which Defendant does not agree—Google Wallet and/or Google Checkout anticipates and/or renders obvious the Asserted Claims of the Asserted Patents,. *See Commscope Techs. v. Dali Wireless Inc*., 10 F.4th 1289, 1294 (Fed. Cir. 2021) ("As the Supreme Court has stated, '[t]hat which infringes, if later, would anticipate, if earlier.'") (quoting *Peters v. Active Mfg. Co*., 129 U.S. 530, 537 (1889)). Google will supplement its production with additional documents, source code and other information regarding the functionality of Google Wallet as it operated on and before March, 2013.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 89 of 156

Item Name or Description	Date Available	Manufacturer
MasterCard PayPass for contactless card and contactless mobile device transactions	At least 2008 for contactless cards; May, 2012 for mobile device transactions (e.g., certification for Samsung and other manufacturer devices)	MasterCard
American Express single-use and contactless credit cards, including Express Pay	At least as early as 2005	American Express
Discover Zip for contactless credit cards	At least as early as 2012	Discover
Online payment API and Magento tokenization solution for PayPal (then eBay)	At least as early as 2011 (Payment API) and 2013 (Magento tokenization)	PayPal
Magento (now Adobe)	See above re PayPal	Magento
Apple Pay	At least as early as 2014	Apple
Bell ID® Mobile Token Manager, including as used by RIM	2011-2013	BellID (acquired by VISA)
Caja de Ahorros y Pensiones de Barcelona, or "La Caixa," contactless ATM	At least as early as 2011	La Caixa
LoopPay	In development since 2012 and launched by its acquisition by Samsung in 2015	Samsung
Samsung Pay and/or Samsung Wallet as implemented on Samsung-branded mobile devices and/or Samsung-branded smart watches	Samsung Pay was Launched in August-September 2015	Samsung

E. Pre-AIA 35 U.S.C. § 102(f)

On information and belief, Defendant contends that patentee derived the invention from persons associated with the following systems and entities under pre-AIA 35 U.S.C. § 102(f).

Name of Person from Whom the Invention Was Derived	Circumstances Under which the Invention or any Part of It was Derived
One or more individuals at Apple	See above discussion of Apple Pay and public disclosures relating to same.
One or more individuals at EMVCo	See above discussion of specification and standards publicly issued by EMVCo
One or more individuals at VISA	See above discussion of Visa and Visa PayWave and public disclosures relating to same
One or more individuals at Mastercard	See above discussion of MasterCard and MasterCard PayPass and public disclosures relating to same
One or more individuals at American Express	See above discussion of American Express single-use and contactless credit cards, including Express Pay, and public disclosures relating to same
One or more individuals at Discover	See above discussion of Discover Zip for contactless credit cards and public disclosures relating to same
One or more individuals at PayPal (eBay)	See above discussion of the PayPal online payment API and Magento tokenization solution for PayPal (then eBay) and public disclosures relating to same
One or more individuals at Magento	See above discussion of the Magento tokenization solution for PayPal (then eBay) and public disclosures relating to same
One or more individuals at eBay	See above discussion of the Magento tokenization solution for PayPal (then eBay) and public disclosures relating to same
One or more individuals at Google	See above discussion of Google Wallet and public disclosure relating to same
ISIS (SoftCard)	See above discussion of ISIS and public disclosure relating to same
One or more individuals at Samsung (LoopPay)	See the above discussion of LoopPay and public disclosures relating to same

F. Pre-AIA 35 U.S.C. § 102(g)

On information and belief, Defendant contends that the following persons or entities made the purported invention before the patent applicant under Pre-AIA 35 U.S.C. § 102(g).

Identity of Person or Entities Involved in Making the Invention	Circumstances Surrounding the Making of the Invention
Apple and one or more individuals at Apple	See above discussion of Apple Pay
EMVCo and one or more individuals at EMVCo	See above discussion of EMV standards and specifications
VISA and one or more individuals at VISA	See above discussion of Visa and Visa PayWave
MasterCard and one or more individuals at Mastercard	See above discussion of MasterCard and MasterCard PayPass and public disclosures relating to same
Discovery and one or more individuals at Discover	See above discussion of Discover Zip for contactless credit cards
American Express and one or more individuals at America Express	See above discussion of American Express single-use and contactless credit cards, including Express Pay
PayPal and one or more individuals at PayPal	See above discussion of the PayPal online payment API and Magento tokenization solution for PayPal (then eBay)
Magento and one or more individuals at Magento	See above discussion of the Magento tokenization solution for PayPal (then eBay)
eBay and one or more individuals at eBay	See above discussion of the Magento tokenization solution for PayPal (then eBay)
Google and one or more individuals at Google	See above discussion of Google Wallet and ISIS (later SoftCard)
Samsung and one or more individuals at Samsung (LoopPay)	See above discussion of LoopPay

Discovery is in its earliest stages, and Defendant's prior art investigation, including via discovery and third-party discovery, is therefore not yet complete. Defendant reserves the right to rely upon additional evidence of invalidity obtained in the future as to any prior art public use/sales/offers for sale, including by Plaintiff, that may anticipate or render obvious one or more

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 92 of 156

Asserted Claims of the Asserted Patents. Defendant also reserves the right to rely upon additional evidence demonstrating the first date on which the above-identified devices were publicly used, sold, or offered for sale. Google's investigation is ongoing. Google will supplement its production with documents, source code and other information regarding the operation of Google Wallet on and before March 2013.

G. Printed Matter with No Patentable Weight[23]

Multiple Asserted Claims include features that are directed to printed matter (e.g., fixed payment information, displaying information, or lack of printed/displayed information) that has no functional or structural relationship to the claimed device or method, and therefore should be afforded no patentable weight. *See*, *e.g.*, '520 patent, claim 14 ("rendering on the display of the electronic device the payment method types stored in the electronic device, wherein said rendering comprises rendering with images, alphanumeric characters and iconography including at least one of a set comprising: a bank logo; an issuer logo; card network icons; payment network icons; a portion of the account number; and a cardholder name"); '579 claim 1 ("displaying, on the touch-screen display, images of: a card issuer payment method selection, including a last 4-digit partial number of a card issuer supplied account number of a payment card; a card logo; and other iconography of the payment card"); 634 claim 1 ("displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account"). As such, no prior art is required to invalidate those claim elements because they will not receive patentable weight in an anticipation or obviousness analysis, or a section 101 eligibility analysis. *See In re Gulack*, 703 F. 2d 1381, 1385 (Fed. Cir.

[23] This section is for illustrative purposes only, as it is not required by the Scheduling Order or the Standing Order. As such, Defendant reserves all rights to contend that additional or different claim elements are non-limiting.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 93 of 156

1983); *Praxair Distribution, Inc. v. Mallinckrodt Hosp. Prod. IP Ltd.*, 890 F.3d 1024, 1035 (Fed. Cir. 2018) ("The only secondary consideration Mallinckrodt alleges is based on the information claimed in the providing information limitation, which we have held lacks any functional relationship to the non-printed matter limitations in claims 1–8 and 10. That claimed information has no patentable weight in an obviousness analysis because printed matter without a functional relationship to a substrate is not eligible subject matter. Such printed matter cannot be brought within the ambit of patent eligibility by showing that it was surprising. No patentable weight means no patentable weight.") (citation omitted); *In re Marco Guldenaar Holding B.V.*, 911 F.3d 1157, 1161 (Fed. Cir. 2018) ("Appellant's argument on appeal has a different focus from what it argued below. It now contends that 'the specifically-claimed di[c]e' that have markings on one, two, or three die faces are not conventional and their recitation in the claims amounts to 'significantly more' than the abstract idea. The markings on Appellant's dice, however, constitute printed matter, as pointed out by the Board, and this court has generally found printed matter to fall outside the scope of § 101.") (citation omitted).

III. ANTICIPATION AND OBVIOUSNESS

In addition to and including the prior art disclosed in the Exhibits incorporated by reference herein and attached hereto, each of the Asserted Claims of the Asserted Patents is anticipated by and/or obvious in view of one or more of items of prior art identified above in Sections II.A. (list of prior art patents), II.B. (list of prior art publications), II.C. (list of prior art by offered for sale or publicly used or known), II.D (list of prior art from which the Asserted Claims of the Asserted Patents was derived), and/or IV.D (list of prior art by others who made the purported invention before the patent applicant) alone or in combination. Generally, it would have been obvious to one of ordinary skill in the art to combine or modify any of these

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 94 of 156

references to arrive at the alleged invention. Such a combination or modification would have yielded predictable results, and a POSITA would have had a reasonable expectation of success.

The Asserted Claims of the Asserted Patents are directed to known and/or obvious combinations of old and familiar elements, each performing the same function it has long been known to perform, which yield nothing more than predictable results. Put another way, the claimed subject matter is obvious because it is nothing more than (i) combinations of prior art elements according to known methods to yield predictable results, (ii) simple substitutions of one known element for another to yield predictable results, (iii) applications of known techniques to known devices ready for improvement to yield predictable results, and/or (iv) obvious to try.

Generally, it would have been obvious to one of ordinary skill in the art to combine any of these systems and references to arrive at the claimed invention. The combination of familiar elements according to known methods is obvious here because it would have yielded predictable results. Indeed, nothing in any of the Asserted Patents suggests that anything about the claimed systems and methods concerns an unexpected result or anything but a routine and conventional application of known hardware and software components, performing known or routine and conventional functions, to achieve an expected and predictable result.

One of skill in the art would have been motivated to either modify the prior art identified herein, and in the accompanying invalidity exhibits or to combine that prior art in view of, for example, their background knowledge, design incentives, effects of demands known to the design community, or other market forces, in particular the recent widespread adoption of isolating transformers and wireless charging in both stationary and portable devices. Further, the prior art discussed in these contentions relates to the same general field of payment systems, devices, and methods, and addresses many of the same as well as different design and

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 95 of 156

operational features of these systems. This would have further motivated one of skill in the art to combine the prior art. In view of the simplicity of the claimed subject matter and its use of well-known components performing conventional operations, the common sense a person skilled in the art also would have served as a motivation to combine any of the identified references and demonstrates that the Asserted Claims of the Asserted Patents would have been obvious.

Defendant's attached exhibits contain claim charts identifying examples of prior art that anticipates and/or renders obvious each Asserted Claims of the Asserted Patents. Specifically, to the extent the attached claim charts cite to a reference for each element or limitation of an asserted claim, Defendant contends that such reference anticipates that claim. Defendant incorporates by reference each prior art reference of record in the prosecution of the Asserted Patent and related applications, including the statements made therein by the applicant, as well as the prior art discussed in the specification. Defendant further incorporates by reference all *inter partes* review proceedings and post-grant review proceedings filed in the future that challenge the patentability of any claim of the Asserted Patents, including all prior art, argument, and evidence. In addition, to the extent that the attached claim charts cite to additional references, Defendant contends, in the alternative, that the Asserted Claims are rendered obvious for the reasons set forth in the attached charts and exhibits. To the extent the attached claim charts do not identify any explicit disclosures of the prior art for a claim or claim limitation, Defendant contends those claims or claim limitations would have been obvious in view of the reference as a whole and/or the knowledge, skill, and experience of a person having ordinary skill in the art. To the extent any obviousness combinations are included in the attached charts and exhibits, they are provided in the alternative to Defendant's anticipation contentions and are not to be construed to suggest that any reference included in the combinations is not by itself anticipatory.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 96 of 156

Invalidity Claim Charts for the ’520 Patent
Ex. A-01: ’520 Patent in view of Assora
Ex. A-02: ’520 Patent in view of Cox
Ex. A-03: ’520 Patent in view of Doughty
Ex. A-04: ’520 Patent in view of Gill
Ex. A-05: ’520 Patent in view of Gomez
Ex. A-06: ’520 Patent in view of Google Wallet
Ex. A-07: ’520 Patent in view of Hathaway
Ex. A-08: ’520 Patent in view of Javani
Ex. A-09: ’520 Patent in view of Jones
Ex. A-10: ’520 Patent in view of Kay
Ex. A-11: ’520 Patent in view of Killoran
Ex. A-12: ’520 Patent in view of Mjølsnes
Ex. A-13: ’520 Patent in view of Mullen-915
Ex. A-14: ’520 Patent in view of Qasim
Ex. A-15: ’520 Patent in view of Royyuru-866
Ex. A-16: ’520 Patent in view of Royyuru-545
Ex. A-17: ’520 Patent in view of Shoemaker
Ex. A-18: ’520 Patent in view of Spitzer
Ex. A-19: ’520 Patent in view of Yoo
Ex. A-20: ’520 Patent in view of Boalt
Ex. A-21: ’520 Patent in view of Carlson
Ex. A-22: ’520 Patent in view of Dixon
Ex. A-23: ’520 Patent in view of Mullen-431
Ex. A-24: ’520 Patent in view of Smith
Ex. A-25: ’520 Patent in view of Casey
Ex. A-26: ’520 Patent in view of Deibert
Ex. A-27: ’520 Patent in view of Mullen-701
Ex. A-28: ’520 Patent in view of Royyuru-035
Ex. A-37: ’520 Patent in view of Law-540
Ex. A-38: ’520 Patent in view of Spodak

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 97 of 156

Invalidity Claim Charts for the ’520 Patent
Ex. A-39: ’520 Patent in view of Giordano
Ex. A-43: ’520 Patent in view of Nasiri
Ex. A-44: ’520 Patent in view of Marvit
Ex. A-45: ’520 Patent in view of Rigatti

Invalidity Claim Charts for the ’579 Patent
Ex. B-01: ’579 Patent in view of Assora
Ex. B-02: ’579 Patent in view of Cox
Ex. B-03: ’579 Patent in view of Doughty
Ex. B-04: ’579 Patent in view of Gill
Ex. B-05: ’579 Patent in view of Gomez
Ex. B-06: ’579 Patent in view of Google Wallet
Ex. B-07: ’579 Patent in view of Hathaway
Ex. B-08: ’579 Patent in view of Javani
Ex. B-09: ’579 Patent in view of Jones
Ex. B-10: ’579 Patent in view of Kay
Ex. B-11: ’579 Patent in view of Killoran
Ex. B-12: ’579 Patent in view of Mjølsnes
Ex. B-13: ’579 Patent in view of Mullen-915
Ex. B-14: ’579 Patent in view of Qasim
Ex. B-15: ’579 Patent in view of Royyuru-866
Ex. B-16: ’579 Patent in view of Royyuru-545
Ex. B-17: ’579 Patent in view of Shoemaker
Ex. B-18: ’579 Patent in view of Spitzer
Ex. B-20: ’579 Patent in view of Boalt
Ex. B-21: ’579 Patent in view of Carlson
Ex. B-22: ’579 Patent in view of Dixon
Ex. B-23: ’579 Patent in view of Mullen-431
Ex. B-24: ’579 Patent in view of Smith
Ex. B-25: ’579 Patent in view of Casey

Invalidity Claim Charts for the ’579 Patent
Ex. B-26: ’579 Patent in view of Deibert
Ex. B-29: ’579 Patent in view of Narayanaswami
Ex. B-30: ’579 Patent in view of Amacker
Ex. B-31: ’579 Patent in view of Phillips
Ex. B-32: ’579 Patent in view of Purdy
Ex. B-33: ’579 Patent in view of Civelli
Ex. B-34: ’579 Patent in view of Mistry
Ex. B-37: ’579 Patent in view of Law-540
Ex. B-38: ’579 Patent in view of Spodak
Ex. B-39: ’579 Patent in view of Giordano
Ex. B-40: ’579 Patent in view of Powers

Invalidity Claim Charts for the ’538 Patent
Ex. C-01: ’538 Patent in view of Assora
Ex. C-02: ’538 Patent in view of Cox
Ex. C-03: ’538 Patent in view of Doughty
Ex. C-04: ’538 Patent in view of Gill
Ex. C-05: ’538 Patent in view of Gomez
Ex. C-06: ’538 Patent in view of Google Wallet
Ex. C-07: ’538 Patent in view of Hathaway
Ex. C-08: ’538 Patent in view of Javani
Ex. C-09: ’538 Patent in view of Jones
Ex. C-10: ’538 Patent in view of Kay
Ex. C-11: ’538 Patent in view of Killoran
Ex. C-12: ’538 Patent in view of Mjølsnes
Ex. C-13: ’538 Patent in view of Mullen-915
Ex. C-14: ’538 Patent in view of Qasim
Ex. C-15: ’538 Patent in view of Royyuru-866
Ex. C-16: ’538 Patent in view of Royyuru-545
Ex. C-17: ’538 Patent in view of Shoemaker

Invalidity Claim Charts for the ’538 Patent
Ex. C-18: ’538 Patent in view of Spitzer
Ex. C-20: ’538 Patent in view of Boalt
Ex. C-21: ’538 Patent in view of Carlson
Ex. C-22: ’538 Patent in view of Dixon
Ex. C-23: ’538 Patent in view of Mullen-431
Ex. C-24: ’538 Patent in view of Smith
Ex. C-25: ’538 Patent in view of Casey
Ex. C-26: ’538 Patent in view of Deibert
Ex. C-30: ’538 Patent in view of Amacker
Ex. C-31: ’538 Patent in view of Phillips
Ex. C-35: ’538 Patent in view of Mullen 876
Ex. C-36: ’538 Patent in view of Hird
Ex. C-37: ’538 Patent in view of Law-540
Ex. C-38: ’538 Patent in view of Spodak
Ex. C-41: ’538 Patent in view of Law 750
Ex. C-42: ’538 Patent in view of Rans

Invalidity Claim Charts for the ’634 Patent
Ex. D-01: ’634 Patent in view of Assora
Ex. D-02: ’634 Patent in view of Cox
Ex. D-03: ’634 Patent in view of Doughty
Ex. D-04: ’634 Patent in view of Gill
Ex. D-05: ’634 Patent in view of Gomez
Ex. D-06: ’634 Patent in view of Google Wallet
Ex. D-07: ’634 Patent in view of Hathaway
Ex. D-08: ’634 Patent in view of Javani
Ex. D-09: ’634 Patent in view of Jones
Ex. D-10: ’634 Patent in view of Kay
Ex. D-11: ’634 Patent in view of Killoran
Ex. D-12: ’634 Patent in view of Mjølsnes

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 100 of 156

Invalidity Claim Charts for the ’634 Patent
Ex. D-13: ’634 Patent in view of Mullen-915
Ex. D-14: ’634 Patent in view of Qasim
Ex. D-15: ’634 Patent in view of Royyuru-866
Ex. D-16: ’634 Patent in view of Royyuru-545
Ex. D-17: ’634 Patent in view of Shoemaker
Ex. D-18: ’634 Patent in view of Spitzer
Ex. D-20: ’634 Patent in view of Boalt
Ex. D-21: ’634 Patent in view of Carlson
Ex. D-22: ’634 Patent in view of Dixon
Ex. D-23: ’634 Patent in view of Mullen-431
Ex. D-24: ’634 Patent in view of Smith
Ex. D-25: ’634 Patent in view of Casey
Ex. D-26: ’634 Patent in view of Deibert
Ex. D-30: ’634 Patent in view of Amacker
Ex. D-31: ’634 Patent in view of Phillips
Ex. D-35: ’634 Patent in view of Mullen 876
Ex. D-36: ’634 Patent in view of Hird
Ex. D-37: ’634 Patent in view of Law-540
Ex. D-38: ’634 Patent in view of Spodak
Ex. D-39: ’634 Patent in view of Giordano
Ex. D-41: ’634 Patent in view of Law 750
Ex. D-42: ’634 Patent in view of Rans

To the extent not identified above in Section II, Defendant identifies all references listed in the above tables as prior art references anticipating and/or rendering obvious one or more claims of the Asserted Patents. Defendant also identifies and incorporate herein Exhibits A-D to

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 101 of 156

Plaintiff Cardware Inc.'s Infringement Contentions regarding Google Pay and/or Google Wallet as implemented on Google or third party mobile devices and/or smart watches.[24]

To the extent that Plaintiff contends that any one of the references in the above Invalidity Claim Charts does not disclose one or more elements of the Asserted Claims, it would have been obvious to combine the references in the Invalidity Charts with one another as discussed more fully in each of the Invalidity Charts (Exs. A-01 through D-42), and the Combinations Exhibit (Ex. I).

All of the Asserted Claims of the Asserted Patents are anticipated, expressly or inherently, and therefore fail to meet one or more of the requirements for patentability, as detailed in the Anticipatory Charts. Additionally, and in the alternative, the Asserted Claims of the Asserted Patents are obvious in view of the state of the prior art (including Admitted Prior Art) alone and/or in combination with the references described in the above-referenced claim charts. The alleged inventions claimed in the Asserted Claims of the Asserted Patents would have been obvious because the prior art, common knowledge, and the nature of the problems, viewed through the eyes of a person ordinarily skilled in the art, disclosed or suggested the claimed elements. A person of ordinary skill in the relevant fields would have possessed knowledge and skills rendering him or her capable of combining or modifying the prior art

[24] By identifying Google Wallet and Google Checkout in these invalidity contentions, Google makes no admissions and does not concede that any facts, allegations, or legal conclusions in Plaintiff's infringement contentions, complaint, or any other pleadings or papers are true. Instead, Plaintiff's infringement contentions merely reflect Plaintiff's admission that—based on Plaintiff's erroneous factual and legal conclusions, and unfounded claim interpretations, with which Defendant does not agree—Google Wallet and/or Google Checkout anticipates and/or renders obvious the Asserted Claims of the Asserted Patents. *See CommScope Techs. v. Dali Wireless Inc.*, 10 F.4th 1289, 1294 (Fed. Cir. 2021) ("As the Supreme Court has stated, '[t]hat which infringes, if later, would anticipate, if earlier.'") (quoting *Peters v. Active Mfg. Co.,* 129 U.S. 530, 537 (1889)). Google will supplement its production with documents, source code and other information describing the operation of Google Wallet on and before March 2013.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 102 of 156

references with knowledge in the field and common sense. Moreover, the Asserted Claims represent well-known combinations of familiar and pre-existing elements, yielding only predictable results. Additional reasons that a person of ordinary skill in the art would have been motivated to combine the identified prior art are provided in the Exhibits attached hereto.

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed, Defendant may rely on any other combination of any prior art references disclosed herein and upon prior art disclosed within the prosecution history of the references cited herein or incorporated by reference into the disclosed prior art. The obviousness combinations set forth in these contentions reflect Defendant's present understanding of the potential scope of the claims that Plaintiff appears to be advocating and should not be seen as Defendant's acquiescence to Plaintiff's interpretation of the Asserted Claims. Defendant will amend or supplement these contentions regarding anticipation or obviousness of the Asserted Claims as appropriate under the applicable rules, including in response to further information from Plaintiff or information discovered during discovery. Plaintiff has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time of the alleged invention. Therefore, for any claim limitation that Plaintiff alleges is not disclosed in a particular prior art reference, Defendant reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the asserted claim obvious.

In an effort to focus the issues, Defendant has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 103 of 156

in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. As noted above, Defendant will rely upon the prior art references identified herein in their entirety, including un-cited portions.

Additionally, any reference or combination of references that anticipates or renders obvious an asserted independent claim also renders obvious any asserted claim dependent on that independent claim because every element of each dependent claim was known by a person of ordinary skill at the time of the alleged invention, and it would have been obvious to combine those known elements with the independent claims at least as a matter of common sense and routine innovation.

Exemplary combinations of references demonstrating the obviousness of the Asserted Claims of the Asserted Patents under 35 U.S.C. § 103 are listed in the Combinations Exhibit. *See* Ex. I. In addition to the specific combinations of prior art references and the motivations to combine discussed in Exhibit I, a person of ordinary skill would have been motivated to address the alleged problems or achieve the purported objectives identified in the "BACKGROUND OF THE INVENTION" section of the Asserted Patents. Moreover, the Asserted Patents admit that numerous claim features[25] were well known at the time of the alleged invention including, for example, those identified above in Section II.A.

[25] Additionally, as stated below, Defendant believes some of these elements to be indefinite and do not concede they are adequately disclosed or delineated in the Asserted Patents, but simply that the Asserted Patents admit these elements are not novel based on Plaintiff's implicit constructions in the Infringement Contentions. Furthermore, this list is only illustrative because it is not required by the Scheduling Order or Standing Order, and Defendant does not concede that other claim elements not listed here were not expressly or implicitly admitted by the patentees to be present in the prior art.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 104 of 156

IV. INVALIDITY UNDER 35 U.S.C. § 112

In addition to and including the grounds of invalidity set forth above, Defendant contends that the Asserted Claims of the Asserted Patents are invalid under 35 U.S.C. § 112 for at least the following reasons.

A. Indefiniteness under 35 U.S.C. § 112

The Asserted Claims of the Asserted Patents are invalid because they fail to comply with the definiteness requirement of 35 U.S.C. § 112. *See* 35 U.S.C. § 112(6) ("The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or joint inventor regards as the invention."); AIA § 112(b) (same). "[A] patent is invalid for indefiniteness if its claims, read in light of the specification delineating the patent, and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014). Furthermore, a patent claim is invalid for indefiniteness when it recites "both a system and the method for using that system," because "it does not apprise a person of ordinary skill in the art of its scope. *IPXL Holdings, L.L.C. v. Amazon.com, Inc.*, 430 F.3d 1377, 1384 (Fed. Cir. 2005) (holding claim invalid as indefinite where unclear whether infringement occurs when one creates a system that allows user to change predicted transaction information or accept the displayed transaction, or whether infringement occurs when the user actually uses the input means to change transaction information or uses the input means to accept a displayed transaction). The Asserted Claims are indefinite at least because they fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 105 of 156

In addition, one or more of the claims identified above is invalid as an improper dependent claim under 35 U.S.C. § 112 ¶¶ 2, 4, and/or AIA § 112(b), (d).[26] "A dependent claim that contradicts, rather than narrows, the claim from which it depends is invalid." *Multilayer Stretch Cling Film Holdings, Inc. v. Berry Plastics Corp.*, 831 F.3d 1350, 1362 (Fed. Cir. 2016); *see* 35 U.S.C. § 112(d) (requiring that "a claim in dependent form shall contain a reference to a claim previously set forth and then *specify a further limitation of the subject matter claimed*" (emphasis added)); *Pfizer, Inc. v. Ranbaxy Labs. Ltd.*, 457 F.3d 1284, 1291–92 (Fed. Cir. 2006) (holding a claim invalid under pre-AIA 35 U.S.C. § 112 ¶ 4 for claiming subject matter that was "non-overlapping" with the claim from which it depended); *Curtiss–Wright Flow Control Corp. v. Velan, Inc.*, 438 F.3d 1374, 1380 (Fed. Cir. 2006) (noting that a dependent claim can be invalid for failing to comply with pre-AIA 35 U.S.C. § 112 ¶ 4); *see also Trs. of Columbia Univ. v. Symantec Corp.*, 811 F.3d 1359, 1366–67 (Fed. Cir. 2016) (holding that claims that were internally contradictory were invalid as indefinite); *Allen Eng'g Corp. v. Bartell Indus.*, 299 F.3d 1336, 1349 (Fed. Cir. 2002) (holding that claims that contradicted the specification were invalid as indefinite). For example, asserted claim 11 of the '520 patent is an improper dependent claim and is thus invalid under 35 U.S.C. § 112 ¶ 2, ¶ 4, and/or AIA § 112(b), (d), as it improperly attempts to broaden claim 10 and contradicts claim 10.

[26] The discussion of 35 U.S.C. § 112 ¶ 4 and AIA § 112(d) is exemplary, as the rules do not require Defendant to identify improper dependent claims invalid under § 112 ¶ 4/(d) in these invalidity contentions.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 106 of 156

In particular, at least the following terms or phrases (alone, either in their entirety or in part, in combination, and/or in context) render the Asserted Claims of the Asserted Patents indefinite[27]:

’520 Patent	
Claim	**Term(s) or Phrase(s)**
Asserted Claim 1	“a computer readable medium having instructions stored thereon that, responsive to execution by the electronic device, cause the electronic device to perform operations comprising” “wherein the memory comprises device-specific and user-specific information” “wherein the user provided payment information is communicated wirelessly; and, wirelessly receiving a static device account number payment information for storage on the electronic device” “static device account number payment information” “dynamically-generating a one-time limited-use numbers based on at least one of a set of information including: user-identifying information; user secrets; device information; device secrets; time; merchant; facility location; sequence count; payment information; account information; amount; and transaction information; and using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction” “the payment information” “a one-time limited use numbers” “said static device account number” “issued payments information” “user-specific information” “device-specific [information]”
Asserted Claim 4	“an introduction of a transaction-specific identifier” “a lock/unlock command determining operation of the electronic device according to an input sequence or a gesture across the plurality of touch sensors”

27 Defendant hereby incorporates by reference the Claim Construction Memorandum and Order in *CardWare Inc. v. Samsung Electronics Co.*, No. 2:22-cv-00141-JRG-RSP, Dkt. 138 (E.D. Tex. Aug. 23, 2023), finding certain asserted claim terms indefinite.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 107 of 156

’520 Patent	
Asserted Claim 5	“a sequence counter” “sequential parameter” “a transaction identifier” “a credit card authority secret”
Asserted Claim 6	“the limited-use number”
Asserted Claim 7	“wherein the display enables information to be displayed regarding the limited-use number, the time, a passcode, a sequence code, a currency amount, and other credit card transaction information of the user, a merchant, a bank or a credit card authority” “other credit card transaction information of the user” “the limited-use number” “a sequence code”
Asserted Claim 8	“the transaction unit” “a cryptographic hash”
Asserted Claim 10	“the electronic device comprises device-specific and user-specific information” “a static device account number payment information” “the payment information” “payment information” “a issuer provided payment information” “issuer provided payment information” “using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction” “user-specific information” “device-specific [information]” “a static device account number payment information” “said static device account number”
Asserted Claim 11	“the electronic device is configured to accept the user input by at least one of a means comprising: a touch sensor array; a touch screen; a keypad; buttons; device motion; an accelerometer; a biometric input; a proximity contact sensor; optical sensors; an NFC unit; a wireless interface; a wired connection; a USB connection; an RF antenna; an inductor assembly”

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 108 of 156

’520 Patent	
	“a proximity contact sensor” “a biometric input"
Asserted Claim 12	“the device-specific information comprises at least one of a set including: . . . device usage sequence counters; and device account numbers” “device identifiers” “device secrets”
Asserted Claim 13	“the user-specific information comprises at least one of a set comprising: . . . device account numbers” “user information” “signature information” “user secrets”
Asserted Claim 14	“rendering on the display of the electronic device the payment method types stored in the electronic device, wherein said rendering comprises rendering with images, alphanumeric characters and iconography including at least one of a set comprising: a bank logo; an issuer logo; card network icons; payment network icons; a portion of the account number; and a cardholder name”
Asserted Claim 17	“the issuer provided payment information” “device account number” “card security codes; card validation values; card identification numbers”
Asserted Claim 18	“recording a user selection from the user interface of the electronic device of a user selected account from which the electronic device is operable to wirelessly convey with an ATM” “wherein the identification, selection, information and authorizing operations are exchanged wirelessly between the electronic device and the ATM via NFC” “wherein the ATM is configured for performing the user selected account operation using the identification and authorizing information” “wherein the identification and authorizing information exchanged wirelessly between the electronic device and the ATM comprises: statically and dynamically generated limited-use number portions” “the identification, selection, information and authorizing operations”

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 109 of 156

’520 Patent	
	“authorizing operations” “identification” “the user selected account operation” “the identification and authorizing information” “wherein user input information from the user interface includes at least one of a set comprising: . . . operation and authorizing information” “operation” “device-identifiers” “merchant-identifiers”
Asserted Claim 19	“at least one of a set identification and data comprising” “the identification and authorizing information” “biometric user identification” “device-identifiers” “payment numbers” “usage sequence counts” “device account numbers” “secrets”
Asserted Claim 20	“user entered identification and authorizing information” “action and sequence of motions of the electronic device as performed by a user” “confirming the electronic device has remained in the possession of the user” “biometric sensor”
Asserted Claim 22	“the limited-use number dynamically generated in the device” “the facility performing the transaction” “a count of past transactions” “a sequence count” “a device-internal secret” “a device unique identifier” “a payment issuer authority secret” “a cryptocurrency server”

’520 Patent	
	“a user secret”
Asserted Claim 23	“a token account number” “the payment information comprises combining a plurality of static portions, and a plurality of dynamically generated limited-use portions, and wherein the static portion is a token account number with a limited-duration expiration date”

’579 Patent	
Claim	**Term(s) or Phrase(s)**
Asserted Claim 1	“a priming operation of the electronic device” “a limited-use payment information”
Asserted Claim 2	“a device transaction sequence counter” “a device account number” “device secret keys”
Asserted Claim 3	“a card validation value originated from the card issuer” “transaction sequence counter count” “wherein further, said dynamically generating the cryptogram number results in a one-time limited-use number via the device incrementing said device transaction sequence counter count on a transaction” “a device account number” “device secrets” “payment issuer secrets”
Asserted Claim 4	“a device account number” “wherein a limited-use number comprises a device account number” “performing payment transactions by the electronic device including the limited-use number” “combining the limited-use number and said device account number within a device generated payment information”
Asserted Claim 5	“a device transaction sequence counter” “a device account number” “device secrets” “issuer secrets”

’579 Patent	
Asserted Claim 6	“a transaction sequence count information” “a device account number” “an invalid device account number” “issuer secrets”
Asserted Claim 7	“a device biometric sensor interface” “wherein the receiving an input at an electronic device comprises receiving an input via a user interface from one of the set of user interfaces comprising: . . . a device user-interface selection”
Asserted Claim 8	“a device biometric sensing of a valid user identity” “a device biometric sensing the electronic device is continuously remaining in the proximity possession of a valid user” “swiping of a recognized user skin over a device sensor array”
Asserted Claim 9	“a device biometric user-sensor” “a device biometric sensing of a valid user identity” “a device biometric sensing the electronic device is continuously remaining in the proximity contact of a valid user” “the proximity contact” “the device account number” “the primary account number”
Asserted Claim 10	“the electronic device priming”
Asserted Claim 11	“completing the transaction on the electronic device” “the electronic device leaving the user’s possession” “the proximity contact” “a biometric sensing the electronic device leaving the possession of a user since a last user validation”
Asserted Claim 12	“a payment account number portion” “a device account number portion” “subsequent to the priming operation”
Asserted Claim 13	“a correct user passcode re-entry” “a device priming operation” “a payment priming operation” “the priming operation”

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 112 of 156

’579 Patent	
	“the proximity contact” “a button double press” “a biometric sense of the device continuously remaining in the proximity contact of a valid user, since a last validation” “denying the priming operation for payment when the electronic device is not sensed as being continuously within the proximity contact of a valid user” “until after successfully re-validating a user” “a successful priming action” “disabling a device priming operation responsive to completing a transaction” “re-validating a user requires a correct user passcode re-entry”
Asserted Claim 14	“the priming operation” “a payment priming operation” “a device priming operation”
Asserted Claim 15	“proximity contact” “a biometric user-sensor” “a device biometric sensor”
Asserted Claim 18	“imminent payment” “a swiping of a recognized user skin over a sensor array of the electronic device” “a skin-contact sense of a valid user” “a device biometric recognition of a valid user”
Asserted Claim 19	“enabling the electronic device for imminent performance of a payment operation responsive to the priming action of a valid user”
Asserted Claim 20	“a biometric recognition of a valid user” “a biometric sensing of a valid users [sic] skin” “a biometric detection that the electronic device continuously remains in contact with a valid user”
Asserted Claim 21	“a static device-specific device account number of limited-use ”
Asserted Claim 22	“a static device-specific device account information including a device account number”
Asserted Claim 23	“cryptographically combining of at least one information accessible on the electronic device”

’579 Patent	
	“a device account number” “a device secret”

’538 Patent	
Claim	**Term(s) or Phrase(s)**
Asserted Claim 1	“said limited-use payment information” “a biometric sensor” “static” “said selected payment method” “said selected original issuer-supplied payment information” “a device account number”
Asserted Claim 3	“said confirmation result of said complete device payment information authentication status from a payment processing authority”
Asserted Claim 4	“the generating the limited-use payment information utilizes a unique device generated information limited-in-use to said selected issuer-payment method” “the limited-use payment information” “a valid device generated limited-use information” “said device account information”
Asserted Claim 5	“the limited-use payment information” “said limited-use payment information” “said device-generated limited-use payment information” “the processing authority generated valid limited-use payment transaction information” “a device-unique information” “a payment processor recognizable information” “a device account number” “said generating of said limited-use payment information, is authorizable for a payment, for the singular counted transaction, for said selected payment method, by said device, in said transaction”
Asserted Claim 6	“said information” “the limited-use payment information”

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 114 of 156

’538 Patent	
	“a payment processing authority” “the authority” “said payment processing authority generated payment information” “a limited-use payment” “a device account number”
Asserted Claim 8	“the limited-use payment information” “all valid device generated limited-use information elements” “said combining device” “said device-specific information” “said generating is limiting in-scope-of-use said generated payment information” “said generated payment information” “authorizable payments” “a device-specific account number”
Asserted Claim 9	“said information” “the limited-use payment information”
Asserted Claim 10	“the limited-use payment information” “payment issuer secret”
Asserted Claim 11	“the limited-use payment information”
Asserted Claim 12	“the limited-use payment information” “a recipient NFC facility”
Asserted Claim 13	“the limited-use payment information”
Asserted Claim 14	“the limited-use payment information” “a transaction facility”
Asserted Claim 15	“the limited-use payment information”
Asserted Claim 16	“the limited-use payment information” “a payment facility type”
Asserted Claim 17	“the limited-use payment information” “an online transaction information”
Asserted Claim 18	“a device account number” “payment processing authority secrets”

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 115 of 156

’538 Patent	
Asserted Claim 19	“said selected account information” “the receiving of a user payment approval authorization”
Asserted Claim 20	“said dynamically generating said card validation value number results in a one-time limited-use payment information” “secrets known to a payment processing authority”
Asserted Claim 22	“generating a limited-use security code number for use in place of a card issuer card security code, by cryptographically combining information from at least one of a set of information comprising: a device transaction sequence counter; a device account number; a payment account information, device secrets; payment processing authority secrets”
Asserted Claim 21	“said limited-use number” “a valid dynamically generated limited-use number” “static device account number” “said device account number” “said static device account number”
Asserted Claim 23	“wherein a payment processing authority verifying and authorizing a transmitted limited-use number based on a time of use, and cryptographically combining a transaction sequence count information; a device account number; a user account information; a payment issuer information; a payment processing authority secrets; a transaction information” “a device account number”
Asserted Claim 25	“accept a priming action of the electronic device” “imminent performance” “a statically generated portions” “the communication interface is operable to transmit” “the device inputs” “the device” “the electronic device”
Asserted Claim 26	“the device human input sensors” “a human to device inputs” “touch input sensor recognition of a unique customer identifier”
Asserted Claim 27	“said device processor”

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 116 of 156

’538 Patent	
	“said cryptogram number is created by said device processor cryptographic combination of device transaction sequence counter count, a payment account information, a user information, and information stored in the device and specific to the device and which is not communicated in the transaction” “wherein the generating said complete combined device payment information comprises a device combining said static device-specific device account number, said device account expiration date, said user information, said payment account information, and said dynamically generated cryptogram, and transmitting said complete device payment information when said issuer payment account method is selected” “said information” “said secrets” “said payment account information” “a device-specific expiration date of limited duration of validity” “wherein the generating said complete combined device payment information comprises a device combining said static device-specific device account number, said device account expiration date, said user information, said payment account information, and said dynamically generated cryptogram, transmitting said complete device payment information when said issuer payment account method is selected” “static device-specific device account number” “a static device-specific account number known to a payment processing authority and limited in use to the device use in place of an issuer payment method” “transmitting said complete device payment information when said issuer payment account method is selected” “cryptographically compute”
Asserted Claim 28	“a combining of a static device-specific payment account information, a device generated information, and other user and account information stored on the device which is uniquely identifying the specific user, specific selected account, and the specific device” “wherein the one or more device processors are further operable to combine said limited-use static device account information and said one-time use cryptogram number(s) to produce the complete combined device payment information”

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 117 of 156

’538 Patent	
Asserted Claim 29	“dynamically generate a one-time limited-use cryptogram number, via a known cryptographic combination of at least one information unique to the electronic device, and also known to at least one of a payment processing authority and a payment issuer authority” “said payment account” “said payment authorities” “authority computed cryptogram” “receive an approval and a denial status of said transaction, from said payment authorities, and visually convey said transaction status in the user-interface on the display disposed of the device” “said transaction status” “a device account number” “a device secret” “a payment processing authority secret”
Asserted Claim 30	“The electronic device of claim 25, further comprising a processor and a non-transitory, computer-readable medium storing computer executable instructions that when executed by the one or more processors, cause the one or more device processors to . . .” “the one or more device processors” “unique to the electronic device” “wherein said user device is operable to receive an approval and a denial status of said transaction information validation, and visually convey said transaction status in the user-interface on the display disposed of the device” “device payment account number” “at least one information unique to the electronic device” “the electronic device” “at least one information known to: the device, the payment issuer authority, and a payment processing authority, and unique to the electronic device, and selected from a set of information including: a transaction sequence counter; a user payment account number; a device payment account number; a device secret; device keys; a payment issuer original account information;

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 118 of 156

’538 Patent	
	a payment issuer device account information; a payment processing authority secret; a transaction information; and a user private information” “said selected payment account” “and visually convey said transaction status in the user-interface on the display disposed of the device”

’634 Patent	
Claim	**Term(s) or Phrase(s)**
Asserted Claim 1	“limited-use payment information” “responsive to said priming operation, readying said device to perform a payment transaction by an identified user” “wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device”
Asserted Claim 2	“limited-use payment information” “a cryptogram number”
Asserted Claim 3	“a payment processing authority” “a static device account information”
Asserted Claim 4	“a static device account information” “limited-use payment information”
Asserted Claim 5	“dynamically generating Lather” “limited-use payment information” “payment processing authority secret information”
Asserted Claim 6	“limited-use payment information” “at least one secret information” “payment processing authority”
Asserted Claim 12	“known user biometric touch characteristics”
Asserted Claim 17	“a static device account information” “payment processing authority”

’634 Patent	
Asserted Claim 18	“a static device account information” “limited-use payment information” “a combined payment information”
Asserted Claim 19	“limited-use payment information” “payment processing authority secret information”
Asserted Claim 20	“limited-use payment information” “payment processing authority secret information”
Asserted Claim 21	“limited-use payment information” “payment processing authority secret information”
Asserted Claim 22	“limited-use payment information” “payment processing authority secret information”
Asserted Claim 23	“limited-use payment information” “payment processing authority supplied secret information”
Asserted Claim 24	“static device account information” “payment processing authority supplied secret information”
Asserted Claim 25	“static device account information” “a static device account number” “a static device-specific expiration date”
Asserted Claim 26	“the static device account number”
Asserted Claim 27	“the limited-use payment information” “payment processing authority secret information”
Asserted Claim 28	“limited-use payment information” “at least one secret information shared by both the electronic device and the payment processing authority” “payment processing authority”
Asserted Claim 29	“a sequential counter count from the electronic device” “static device-specific user account information” “limited-use payment information”
Asserted Claim 30	“limited-use payment information” “a cryptogram number”
Asserted Claim 31	“static device account information”

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 120 of 156

'634 Patent	
Asserted Claim 32	"static device account information" "static device account number"
Asserted Claim 33	"static device account information" "static device account expiration date"
Asserted Claim 35	"static device account information"
Asserted Claim 36	"limited-use payment information" "payment processing authority" "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;" "wherein said shared information is shared by both the electronic device and a payment processing authority"
Asserted Claim 37	"limited-use payment information" "payment processing authority secrets"
Asserted Claim 38	"limited-use payment information" "payment processing authority secrets"
Asserted Claim 39	"limited-use payment information" "payment authority information" "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; a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction" "a per-transaction sequential parameter originating from the electronic device" "secret information associated with a selected issued payment account"
Asserted Claim 40	"payment authority information"
Asserted Claim 41	"payment authority information" "secret information shared by both the electronic device and a payment processing authority"

’634 Patent	
Asserted Claim 42	“a static device account number” “processing authority information”
Asserted Claim 43	“a static device account expiration date.” “processing authority information”
Asserted Claim 44	“processing authority information”
Asserted Claim 45	“limited-use payment information” “payment authority information” “a cryptogram number”
Asserted Claim 46	“processing authority information”
Asserted Claim 47	“static device account number” “processing authority information”
Asserted Claim 48	“static device account expiration date” “processing authority information”
Asserted Claim 51	“a biometric sensor” “biometric sensing”
Asserted Claim 52	“biometric sensing”
Asserted Claim 53	“biometric recognition”
Asserted Claim 55	“processing authority information”
Asserted Claim 56	“a secret information” “limited-use payment information” “payment authority information” “responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction” “a per-transaction sequential parameter originating from the electronic device” “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”
Asserted Claim 57	“payment authority information”
Asserted Claim 58	“static device account number” “payment authority information”

’634 Patent	
Asserted Claim 59	“static device account expiration date” “payment authority information”
Asserted Claim 61	“payment authority information”
Asserted Claim 62	“limited-use payment information” “a cryptogram number”
Asserted Claim 63	“payment authority information”
Asserted Claim 64	“static device account number” “payment authority information”
Asserted Claim 65	“static device account expiration date” “payment authority information”
Asserted Claim 68	“a biometric sensor” “biometric sensing”
Asserted Claim 69	“biometric sensing”
Asserted Claim 70	“biometric recognition”
Asserted Claim 72	“payment information” “payment authority information”

To the extent other Asserted Claims contain one of these terms or phrases, either directly or through being dependent on a claim that does, those Asserted Claims are also invalid under 35 U.S.C. § 112.

B. Lack of Enablement under 35 U.S.C. § 112

The Asserted Claims of the Asserted Patents are invalid because they are not enabled as required by 35 U.S.C. § 112. *See* 35 U.S.C. § 112(6) (“The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same.”); AIA § 112(a) (same). *See AK Steel Corp. v. Sollac*, 344 F.3d 1234, 1244 (Fed. Cir. 2003) (“The enablement requirement is

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 123 of 156

satisfied when one skilled in the art, after reading the specification, could practice the claimed invention without undue experimentation.") (citing *In re Wands*, 858 F.2d 731, 736–37 (Fed. Cir. 1988)). Because the Asserted Patents do not disclose sufficient information to enable a person having ordinary skill in the field of the alleged invention(s) to make and use the full scope of the alleged invention(s), as set forth in the claims, at the time of filing without undue experimentation, the Asserted Claims are invalid for lack of enablement.

In particular, at least the following terms or phrases (alone, either in their entirety or in part, in combination, and/or in context) are not enabled:

'520 Patent	
Claim	**Term(s) or Phrase(s)**
Asserted claim 1	"touch screen display" "sequence count" "issued payments information" "user-specific information" "device-specific [information]"
Asserted Claim 4	"an introduction of a transaction-specific identifier"
Asserted Claim 5	"a sequence counter which generates a sequential parameter when the processor initiates a transaction" "a transaction identifier"
Asserted Claim 7	"a sequence code"
Asserted Claim 10	"touch screen display" "sequence count" "issued payment information"
Asserted Claim 11	"a biometric input" "a proximity contact sensor" "a wired connection"
Asserted Claim 12	"device usage sequence counters" "device identifiers"
Asserted Claim 13	"signature information"

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 124 of 156

'520 Patent	
Asserted Claim 16	"wherein the user selection is a default payment method to be used in transactions"
Asserted Claim 17	"card identification numbers" "card validation values"
Asserted Claim 19	"usage sequence counts" "biometric user identification" "device-identifiers" "merchant identifiers"
Asserted Claim 20	"a biometric sensor confirming the electronic device is in a grip of the user" "a biometric sensor confirming the electronic device has remained in the possession of the user"
Asserted Claim 22	"a count of past transactions" "a sequence count" "a biometrically sensed user information" "a device unique identifier"
Asserted Claim 23	"a token account number with a limited-duration expiration date"

'579 Patent	
Claim	**Term(s) or Phrase(s)**
Asserted Claim 1	"touch screen display"
Asserted Claim 2	"device transaction sequence counter"
Asserted Claim 3	"device transaction sequence counter" "device identifiers" "a card validation value"
Asserted Claim 5	"device transaction sequence counter" "device identifiers" "a card issuer security code" "a payment card security code"
Asserted Claim 6	"transaction sequence count information" "a payment processing authority verifies a limited-use number based on at least one information of the set of information comprising:

’579 Patent	
	a transaction sequence count information; a device account number; user account information; issuer secrets; issuer keys; issuer-provided device keys; transaction information; and a time of use”
Asserted Claim 7	“device touch ID button interface” “device biometric sensor interface” “a device user-interface selection”
Asserted Claim 8	“swiping of a recognized user skin over a device sensor array” “a skin-contact sensing of an identified user” “a device biometric sensing of a valid user identity” “a device biometric sensing the electronic device is continuously remaining in the proximity possession of a valid user” “an account balance”
Asserted Claim 9	“a device biometric user-sensor” “a device biometric sensing the electronic device is continuously remaining in the proximity contact of a valid user” “payment denial” “an adjustment of a transaction payment”
Asserted Claim 10	“responsive to the preset duration being exceeded, terminating the NFC communications and aborting the transaction”
Asserted Claim 11	“a biometric sensing the electronic device leaving the possession of a user since a last user validation” “the electronic device leaving the user’s possession” “the electronic device leaving the proximity contact of the user” “the electronic device leaving the grasp of the user” “inputting a transaction denial” “inputting an adjustment of the transaction payment”
Asserted Claim 13	“a biometric sense of the device continuously remaining in the proximity contact of a valid user”

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 126 of 156

’579 Patent	
	“denying the priming operation for payment when the electronic device is not sensed as being continuously within the proximity contact of a valid user”
Asserted Claim 14	“a biometric sense of a touch contact of a valid user’s skin on a touch ID button of the electronic device”
Asserted Claim 15	“a touch ID button” “a biometric user-sensor” “a device biometric sensor operable to determine the electronic device continuously remains in contact with a valid user while the electronic device is coming within proximity contact of an NFC recipient” “a sensor array operable to recognize a swiping of a recognized user skin over the sensor array**”** **“**denying a transaction” “adjusting a transaction”
Asserted Claim 16	“an indication of an authorization success” “an indication of an authorization failure” “an option to retry a transaction” “an option to retry a user authorization” “an option to retry validating a user identity” “an indication of a payment failure” an indication of a payment retry option”
Asserted Claim 17	“an account balance”
Asserted Claim 18	“a device biometric recognition of a valid user” “a touching of the device by an identified user” “a swiping of a recognized user skin over a sensor array of the electronic device” “a skin-contact sense of a valid user” “a device biometric recognition of a valid user”
Asserted Claim 20	“a touch ID recognition of a known user” “a biometric recognition of a valid user” “a biometric sensing of a valid users skin” “a biometric detection that the electronic device continuously remains in contact with a valid user”

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 127 of 156

'579 Patent	
Asserted Claim 23	"a sequence counter" "a card security code"

'538 Patent	
Claim	**Term(s) or Phrase(s)**
Asserted Claim 1	"a biometric sensor" "a touch-screen display"
Asserted Claim 5	"device transaction sequence counter count" "a generating at said valid payment information at a payment processing authority includes a processing authority storing of expected device transaction sequence counter count, expected issuer payment information, an expected a device user information, and the device account number" "a device-unique information" "an adjusting of said transaction sequence counter count on a per transaction basis" "comparing of said device-generated limited-use payment information, to a valid transaction payment information generated by said payment processing authority using same secure combination method, and same information elements of a valid payment transaction by said device"
Asserted Claim 6	"a payment processing authority comparing said device generated payment information, and said payment processing authority generated payment information, for a verifying of a limited-use payment as valid" "upon a proper validating of said result, a conveying of original issuer payment information to an original payment method issuer, for a settlement of said transaction"
Asserted Claim 8	"device-internal transaction sequence counter count" "transaction-specific sequence count information"
Asserted Claim 11	"device payment transaction sequence counter count"
Asserted Claim 18	"a transaction sequence counter count" "a card validation value number" "a one-time limited-use card validation value number" "dynamically generating of said cryptogram results in a one-time limited-use card validation value number"

'538 Patent	
	"said cryptogram is used in place of issuer supplied card validation value number, in performing said transaction payment by the device"
Asserted Claim 19	"touch-screen display user-interface" "denying a transaction" "a payment amount adjustment"
Asserted Claim 20	"a device transaction sequence counter count" "dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the payment issuing authority" "said dynamically generating said card validation value number results in a one-time limited-use payment information"
Asserted Claim 23	"transaction sequence count information"
Asserted Claim 24	"device touch-screen display interface"
Asserted Claim 26	"a correct passcode touch entry sequence" "a correct touch gesture" "a touch input sensor recognition of a unique customer identifier" "a touch input of a known device user" "a biometric recognition of a valid user" "a biometric sensing of a valid user's skin touch" "a touch input sensor recognition of a unique customer identifier" "a security question which a valid user could answer correctly" "responsive to receiving an incorrect user response input, offer a reduced number of additional challenge attempts before failing the user authorization at the device, and denying the payment authorization"
Asserted Claim 27	"device transaction sequence counter count"
Asserted Claim 28	"a transaction sequence counter"
Asserted Claim 30	"a transaction sequence counter"

'634 Patent	
Claim	**Term(s) or Phrase(s)**
Asserted Claim 1	"touch-screen display"

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 129 of 156

’634 Patent	
	“issued payment information”
Asserted Claim 3	“device account information” “issued payment information” “payment processing authority”
Asserted Claim 4	“device account information”
Asserted Claim 5	“processing authority secret information” “payment processing authority”
Asserted Claim 6	“payment processing authority”
Asserted Claim 11	“ touch-screen display”
Asserted Claim 12	“biometric touch characteristics”
Asserted Claim 16	“ touch-screen display”
Asserted Claim 17	“device account information” “issued payment information” “payment processing authority”
Asserted Claim 18	“device account information”
Asserted Claim 19	“dynamically generating the limited-use payment information based on payment processing authority secret information.” “payment processing authority”
Asserted Claim 20	“payment processing authority”
Asserted Claim 21	“dynamically generating the limited-use payment information based on payment processing authority secret information” “payment processing authority”
Asserted Claim 22	“payment processing authority”
Asserted Claim 23	“issued payment information” “in response to transmitting said issued payment information, user information and device-specific information, receiving a payment processing authority supplied secret information.” “payment processing authority”
Asserted Claim 24	“device account information” “payment processing authority”
Asserted Claim 25	“device account number”

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 130 of 156

’634 Patent	
	“device account information”
Asserted Claim 26	“device account number”
Asserted Claim 27	“dynamically generating the limited-use payment information based on payment processing authority secret information.” “payment processing authority”
Asserted Claim 28	“limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority” “payment processing authority”
Asserted Claim 29	“touch-screen display” “sequential counter”
Asserted Claim 31	“device account information”
Asserted Claim 32	“device account number” “device account information”
Asserted Claim 33	“device account information”
Asserted Claim 34	“sequential counter”
Asserted Claim 35	“device account information”
Asserted Claim 36	“payment processing authority”
Asserted Claim 37	“dynamically generate the limited-use payment information based on payment processing authority secrets.” “payment processing authority”
Asserted Claim 38	“dynamically generate the limited-use payment information based on payment processing authority secrets” “payment processing authority”
Asserted Claim 39	“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”
Asserted Claim 41	“device account number” “payment processing authority”
Asserted Claim 47	“device account number”
Asserted Claim 49	“touch panel”
Asserted Claim 50	“touch panel”

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 131 of 156

'634 Patent	
Asserted Claim 51	"biometric sensor operable to detect a user touch"
Asserted Claim 52	"touch panel" "biometric sensing of a user touch at the touch panel"
Asserted Claim 53	"touch panel" "biometric recognition of a valid user identification"
Asserted Claim 56	"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"
Asserted Claim 58	"device account number"
Asserted Claim 60	"payment processing authority"
Asserted Claim 64	"device account number"
Asserted Claim 66	"touch screen interface"
Asserted Claim 66	"touch screen interface"
Asserted Claim 67	"touch screen interface"
Asserted Claim 68	"biometric sensor operable to detect a user touch"
Asserted Claim 69	"touch screen interface" "biometric sensing of a user touch at the touch screen interface"
Asserted Claim 70	"biometric recognition of a valid user identification via the touch input"

Google reserves the right to supplement these contentions to identify specific claims that are invalid for lack of enablement as discovery continues, in response to any amendment CardWare may be permitted to make to its infringement contentions, and/or after claim construction.

C. Lack of Written Description under 35 U.S.C. § 112

The Asserted Claims of the Asserted Patents are invalid because they fail to meet the written description requirement of 35 U.S.C. § 112. *See* 35 U.S.C. § 112(6) ("The specification shall contain a written description of the invention, and of the manner and process of making

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 132 of 156

and using it, in such full, clear, concise, and exact terms . . . ."); AIA § 112(a) (same). "Specifically, the description must 'clearly allow persons of ordinary skill in the art to recognize that [the inventor] invented what is claimed. . . . In other words, the test for sufficiency is whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date." *Ariad Pharm., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (citing *Vas–Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1563 (Fed. Cir. 1991)) (internal citations omitted); *id.* at 1349 ("Although many original claims will satisfy the written description requirement, certain claims may not. For example, a generic claim may define the boundaries of a vast genus of chemical compounds, and yet the question may still remain whether the specification, including original claim language, demonstrates that the applicant has invented species sufficient to support a claim to a genus. The problem is especially acute with genus claims that use functional language to define the boundaries of a claimed genus. In such a case, the functional claim may simply claim a desired result, and may do so without describing species that achieve that result. But the specification must demonstrate that the applicant has made a generic invention that achieves the claimed result and do so by showing that the applicant has invented species sufficient to support a claim to the functionally-defined genus."). Because the Asserted Patents does not describe the limitations or combination of limitations of the Asserted Claims in sufficient detail that a person of ordinary skill in the art would recognize that the inventor possessed the full scope of the alleged invention(s) at the time of filing, the Asserted Claims do not meet the written description requirement.

In particular, at least the following terms or phrases are not sufficiently described:

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 133 of 156

’520 Patent	
Claim	**Term(s) or Phrase(s)**
Asserted Claim 1	“device-specific . . . information” “wherein the user provided payment information is communicated wirelessly” “wirelessly receiving a static device account number payment information” “dynamically-generating a one-time limited-use numbers based on at least one of a set of information including: user-identifying information; . . . device information; . . . merchant; facility location; sequence count; payment information; account information; amount; and transaction information” “using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction” “accepting a user input of issued payments information input at a touch screen display of the electronic device” “the memory comprises device-specific and user-specific information”
Asserted Claim 4	“a transaction-specific identifier”
Asserted Claim 5	“a sequence counter” “a sequential parameter” “transaction identifier”
Asserted Claim 10	“the electronic device comprises device-specific and user-specific information” “the issuer provided payment information is communicated wirelessly” “receiving wirelessly a static device account number payment information for storage on the electronic device” “dynamically-generating a one-time limited-use number based on at least one of a set of information including: user-identifying information; . . . device information; . . . merchant; facility location; sequence count; payment information; account information; amount; and transaction information” “using said static device account number and said dynamically generated one-time limited-use number together in the place of

’520 Patent	
	issuer provided payment information for making a payment transaction” “accepting a user input of issued payment information input at a touch screen display of the electronic device”
Asserted Claim 11	“the electronic device is configured to accept the user input by at least one of a means comprising: . . . a biometric input; a proximity contact sensor; optical sensors; an NFC unit; a wireless interface; a wired connection; a USB connection; an RF antenna; an inductor assembly
Asserted Claim 12	“the device-specific information comprises at least one of a set including: device identifiers; . . . device usage sequence counters; and device account numbers”
Asserted Claim 13	“the user-specific information comprises at least one of a set comprising: . . . a passcode; . . . device account numbers; . . . cryptocurrency address; cryptocurrency keys; . . . signature information”
Asserted Claim 14	“rendering on the display of the electronic device the payment method types stored in the electronic device, wherein said rendering comprises rendering with images, alphanumeric characters and iconography including at least one of a set comprising: . . . an issuer logo; card network icons; payment network icons; . . . and a cardholder name”
Asserted Claim 16	“a default payment method”
Asserted Claim 17	“the issuer provided payment information is selected from at least one of a set comprising: . . . device account number; . . . card security codes; card validation values; card identification numbers; . . . a direction of transaction; the payment issuing authority; . . . and card-type information”
Asserted Claim 18	“providing, by the electronic device, at least one of account information; identification; and authorization, for the ATM transaction” “wherein the electronic device comprises a user interface comprising: displays” “recording a user selection from the user interface of the electronic device of a user selected account from which the electronic device is operable to wirelessly convey with an ATM” “recording a user selection from the user interface of the electronic device of a user selected account operation, wherein said user

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 135 of 156

’520 Patent	
	selected account operation is selected from a list of funds transfer operations” “user input information from the user interface includes at least one of a set comprising: . . . operation” “the identification, selection, information and authorizing operations are exchanged wirelessly between the electronic device and the ATM via NFC” “the ATM is configured for performing the user selected account operation using the identification and authorizing information” “wherein the identification and authorizing information exchanged wirelessly between the electronic device and the ATM comprises: statically and dynamically generated limited-use number portions” “wherein said static and dynamic information is combined to perform the user selected ATM operation”
Asserted Claim 19	“the identification and authorizing information is generated from at least one of a set identification and data comprising: ATM accounts; user identification; biometric user identification; device-identifiers; email address; username; transactional information; merchant identifiers; facility location; user accounts; cryptocurrency address; cryptocurrency keys; merchant accounts; online accounts; bank accounts; device account numbers; payment numbers; card issuing authority; and payment-issuer” “ATM accounts” “device account numbers” “further the data includes at least one of time; duration; passwords; passcodes; device position; device motion; device-specifics; secrets; keys; a currency; currency amounts; cryptocurrency amount; transaction limits; transaction records; usage duration; and usage sequence counts” “passcodes” “device position” “device motion” “device-specifics” “transaction records” “usage duration” “usage sequence counts” “biometric user identification”

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 136 of 156

'520 Patent	
	"device-identifiers" "merchant identifiers"
Asserted Claim 20	"a plurality of button-press actions" "passcode sequence" "an action and sequence of motions of the electronic device as performed by a user" "an action of the user to move the electronic device into a specific orientation" "a biometric sensor confirming the electronic device is in a grip of the user" "a biometric sensor confirming the electronic device has remained in the possession of the user" "biometric sensor" "a touch ID button"
Asserted Claim 22	"the limited-use number dynamically generated in the device is based on cryptographically combining data selected from the group consisting of an ATM information, the locality of an ATM reader facility, a date, . . . a count of past transactions, a sequence count, a historical record of transactions, a merchant account, a user's location, an online address, a device-internal secret, a device unique identifier, a payment authority key, a payment issuer authority secret, a method and direction of payment, deposit, transfer and receipt, a cryptocurrency server, a cryptocurrency type, a cryptocurrency private key, a cryptocurrency public key, a cryptocurrency address, a touch gesture, a biometrically sensed user information, . . . passcode"
Asserted Claim 23	"the payment information comprises combining a plurality of static portions, and a plurality of dynamically generated limited-use portions, and wherein the static portion is a token account number with a limited-duration expiration date, to be used in place of issuer provided information"

'579 Patent	
Claim	**Term(s) or Phrase(s)**
Asserted Claim 1	"touch screen display"
Asserted Claim 2	"a device transaction sequence counter"

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 137 of 156

’579 Patent	
Asserted Claim 3	“dynamically generating a cryptogram number” “a device transaction sequence counter” “card validation value”
Asserted Claim 4	“performing payment transactions by the electronic device including the limited-use number”
Asserted Claim 5	“a device transaction sequence counter” “an internet address”
Asserted Claim 6	“a transaction sequence count information”
Asserted Claim 7	“a device biometric sensor interface”
Asserted Claim 8	“touching from an identified valid user” “swiping of a recognized user skin over a device sensor array” “skin-contact sensing of an identified user” “a device biometric sensing of a valid user identity” “an account balance” “a device biometric sensing the electronic device is continuously remaining in the proximity possession of a valid user”
Asserted Claim 9	“a device biometric user-sensor” “a device biometric sensing the electronic device is continuously remaining in the proximity contact of a valid user” “a payment denial” “an adjustment of a transaction payment”
Asserted Claim 10	“responsive to the preset duration being exceeded, terminating the NFC communications and aborting the transaction”
Asserted Claim 11	“inputting a transaction denial” “inputting an adjustment of the transaction payment”
Asserted Claim 13	“a biometric sense of the device continuously remaining in the proximity contact of a valid user” “denying the priming operation for payment when the electronic device is not sensed as being continuously within the proximity contact of a valid user”
Asserted Claim 15	“a sensor array operable to recognize a swiping of a recognized user skin over the sensor array” “a biometric user-sensor”

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 138 of 156

’579 Patent	
	“a device biometric sensor operable to determine the electronic device continuously remains in contact with a valid user while the electronic device is coming within proximity contact of an NFC recipient” “denying a transaction” “adjusting a transaction”
Asserted Claim 16	“an indication of an authorization success” “an indication of an authorization failure” “an option to retry a transaction” “an option to retry a user authorization” “an option to retry validating a user identity” “an indication of a payment failure” “an indication of a payment retry option” All features of claim 16 in combination with the features of claim 15 that were added by amendment on May 20, 2020 (i.e., “obtaining a user payment approval . . .” through the end of claim 15)
Asserted Claim 17	All features of claim 17 in combination with the features of claim 15 that were added by amendment on May 20, 2020 (i.e., “obtaining a user payment approval . . .” through the end of claim 15) “an account balance”
Asserted Claim 18	“touching of the device by an identified user” “skin-contact sense of a valid user” “swiping of a recognized user skin over a sensor array of the electronic device” “a device biometric recognition of a valid user” All features of claim 18 in combination with the features of claim 15 that were added by amendment on May 20, 2020 (i.e., “obtaining a user payment approval . . .” through the end of claim 15)
Asserted Claim 20	“a biometric recognition of a valid user;” “a biometric sensing of a valid users skin;” “a biometric detection that the electronic device continuously remains in contact with a valid user”
Asserted Claim 23	“a card security code”

’538 Patent	
Claim	**Term(s) or Phrase(s)**
Asserted Claim 1	“displaying, on a display of the device, a transaction payment request and at least a portion of an original static issuer-supplied payment account information associated with a payment method” “device-specific static limited-use payment information, associated with said selected payment method” “dynamically generating, by a processor of the device, device-specific limited-use payment information, for said selected payment method” “using said limited-use payment information in place of at least a portion of said selected original issuer-supplied payment information for the transaction” “combining of said dynamically-generated limited-use payment information with said static limited-use payment information, to generate a complete device payment information” “receiving information at said electronic device corresponding to a transaction status of the payment transaction, wherein such transaction status is at least partly dependent on validation of the transmitted complete device payment information by a payment processor authority and a payment issuer authority” “visually conveying the transaction payment authorization status via a user-interface displayed on said display” “a touch-screen display interface”
Asserted Claim 2	“receiving confirmation via said NFC interface of the validity of said complete device payment information from an NFC payment reader facility”
Asserted Claim 3	“receiving said confirmation result of said complete device payment information authentication status from a payment processing authority via at least one interface of a set of interfaces comprising: said device NFC interface, a wireless interface of said device”
Asserted Claim 4	“said device account information will be rejected as invalid when not including a valid device generated limited-use information”
Asserted Claim 5	“the generating of the limited-use payment information utilizes a secure combination of a device transaction sequence counter count, a device account number, a device-unique information, and a payment processing authority recognizable information” “generating at said valid payment information at a payment processing authority includes a processing authority storing of

’538 Patent	
	expected device transaction sequence counter count, expected issuer payment information, an expected a device user information, and the device account number” “wherein an authorizing by said payment processing authority, is a comparing of said device-generated limited-use payment information, to a valid transaction payment information generated by said payment processing authority using same secure combination method, and same information elements of a valid payment transaction by said device” “an adjusting of said transaction sequence counter count on a per transaction basis” “authorizing of a payment information as valid when said processing authority is verifying the limited-use transaction payment information generated by the device, and the processing authority generated valid limited-use payment transaction information, are matching”
Asserted Claim 6	“the generating the limited-use payment information further utilizes a secure combination of said information with a device account number, a device sequence counter count, device-specific information, payment processing authority specific information” “a verifying of said combination by a payment processing authority, performing same secure combination of same information as retained at the authority” “a payment processing authority comparing said device generated payment information, and said payment processing authority generated payment information, for a verifying of a limited-use payment as valid” “upon a proper validating of said result, a conveying of original issuer payment information to an original payment method issuer, for a settlement of said transaction”
Asserted Claim 7	“The method of claim 3, wherein the visual conveying of the transaction status is further comprising at least one, of a set of visual information including: a confirmation result of payment authority authenticating said device-transmitted limited-use payment information, a confirmation result of payment authority authenticating said device-transmitted complete device payment information, an NFC transaction status, a transaction payment amount,

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 141 of 156

’538 Patent	
	a payment facility wherein the transaction was performed, a merchant information, an original issuer payment account information, an original payment issuer information, a request for an authorized-user approval of the transaction, a payment processing status, an issuer payment approval status, and a payment completion status.”
Asserted Claim 8	“an information unique to the user and device which does not pass in the transaction” “at least one payment authority-supplied information which does not pass in the transaction” “wherein the complete device payment information is only valid for use in place of an issuer payment method in authorizable payments when comprising all valid device generated limited-use information elements” “said generating is limiting in-scope-of-use said generated payment information, for said user-selected issuer payment method option, to a unique-per-device unique-per-use one-time transacting by said combining device; by combining said information elements including: said transaction-specific sequence count information, said device-specific information, said user-specific information, and said authority-specific information” “device-internal transaction sequence counter count”
Asserted Claim 11	“device payment transaction sequence counter count”
Asserted Claim 17	“the generating the limited-use payment information utilizes an online transaction information”
Asserted Claim 18	“dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the payment issuer, and wherein the dynamically generating the cryptogram number comprises cryptographically combining a transaction sequence counter count, payment processing authority secrets, and a device account number” “a one-time limited-use card validation value number” “said cryptogram is used in place of issuer supplied card validation value number”

’538 Patent	
Asserted Claim 19	“receiving an input signal at an electronic device, the input signal corresponding to a request for payment of an online payment transaction by said electronic device, via a wireless interface of the electronic device” “a displaying of the payment request notification at a touch-screen display user-interface of the electronic device” “receiving a user input providing for at least one transaction authorization actions, from a set of actions including: … selecting a user information” “denying a transaction” “a payment amount adjustment”
Asserted Claim 20	“dynamically generating the cryptogram number comprises cryptographically combining a device transaction sequence counter count, a user information, a payment account number, information and secrets known to a payment processing authority” “dynamically generating said card validation value number results in a one-time limited-use payment information”
Asserted Claim 21	“a payment processing authority provides said device account number unique for the specific electronic device, in place of payment issuer information, in performing payment transactions by the electronic device” “wherein a using of said static device account number without a valid dynamically generated limited-use number, shall be deniable as invalid, and outside a valid scope of device-limited usage”
Asserted Claim 23	“a payment processing authority verifying and authorizing a transmitted limited-use number based on a time of use, and cryptographically combining a transaction sequence count information; a device account number; a user account information; a payment issuer information; a payment processing authority secrets; a transaction information” “a rejecting by the payment processing authority, on a detecting as invalid at least one verification test, from a set of tests comprising: a mis-matching of the transacted limited-use number, and the authority cryptographically-combined number”
Asserted Claim 25	“the processor is operable to receive an approval and a denial confirmation from an online payment facility of the complete device payment information”
Asserted Claim 26	“identify an authorized valid device user through a human to device inputs, selected from at least one security challenge, of a set of

’538 Patent	
	human to device input challenges comprising: … a touch input sensor recognition of a unique customer identifier” “a correct passcode touch entry sequence” “a correct touch gesture” “a touch input sensor recognition of a unique customer identifier” “a touch input of a known device user” “a biometric recognition of a valid user” “a biometric sensing of a valid user’s skin touch” “a touch input sensor recognition of a unique customer identifier” “a security question which a valid user could answer correctly” “responsive to receiving an incorrect user response input, offer a reduced number of additional challenge attempts before failing the user authorization at the device, and denying the payment authorization”
Asserted Claim 27	“said cryptogram number is created by said device processor cryptographic combination of device transaction sequence counter count, a payment account information, a user information, and information stored in the device and specific to the device and which is not communicated in the transaction” “wherein said transaction sequence counter, said information and said secrets are known to both said device, and to said payment processing authority” “wherein further said static device-specific device account number is known to a payment issuer, and has a device-specific expiration date of limited duration of validity” “wherein the generating said complete combined device payment information comprises a device combining said static device-specific device account number, said device account expiration date, said user information, said payment account information, and said dynamically generated cryptogram” “cryptographically compute” “combine said dynamically generated portion with a static device-specific account number known to a payment processing authority and limited in use to the device use in place of an issuer payment method”
Asserted Claim 28	“a combining of a static device-specific payment account information, a device generated information, and other user and account information stored on the device which is uniquely

’538 Patent	
	identifying the specific user, specific selected account, and the specific device” “a generating of a limited-use payment information by the one or more device processors cryptographically generating at least one one-time limited-use cryptogram numbers” “wherein the one or more device processors are further operable to combine said limited-use static device account information and said one-time use cryptogram number(s) to produce the complete combined device payment information”
Asserted Claim 29	“the executable instructions further cause the one or more processors to dynamically generate a one-time limited-use cryptogram number, via a known cryptographic combination of at least one information unique to the electronic device, and also known to at least one of a payment processing authority and a payment issuer authority, and selected from a set of information known and stored at both said payment authorities, and on said device, including: a transaction sequence counter, a device account number, a device account expiration date, a device secret, a payment processing authority secret, a user information, a payment account information, a payment issuer information, a payment amount, transactional information” “said payment authorities are operable to recognize from the transactional payment information, the correct set of user, device and account specific information to be cryptographically combined into an authority computed cryptogram, for comparing with device transmitted limited-use payment information” “said payment processing authorities are operable to deny as invalid a transaction including a cryptogram not matching an authority computed cryptogram” “said payment authorities are operable to approve as valid a transaction including a cryptogram matching the payment processing authority computed cryptogram”

'538 Patent	
	"said device is operable to receive an approval and a denial status of said transaction, from said payment authorities"
Asserted Claim 30	"dynamically generate a one-time limited-use cryptogram number by a cryptographic combination, of at least one information known to: the device, the payment issuer authority, and a payment processing authority, and unique to the electronic device, and selected from a set of information including: … a user payment account number; … a payment issuer original account information; a payment issuer device account information; a payment processing authority secret; … and a user private information" "said payment processing authority is operable to deny as invalid, a transaction including a cryptogram not matching a payment processing authority computed cryptogram" "said payment processing authority is operable to approve as valid, a transaction including a cryptogram matching the payment processing authority computed cryptogram"

'634 Patent	
Claim	**Term(s) or Phrase(s)**
Asserted Claim 1	"a touch-screen display coupled to the processor;" "dynamically generating, by the processor, limited-use payment information" "wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device" "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"
Asserted Claim 3	"in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device"
Asserted Claim 4	"combining said limited-use payment information and said static device account information, to reduce a combined payment information"

'634 Patent	
Asserted Claim 5	"dynamically generating the limited-use payment information based on payment processing authority secret information"
Asserted Claim 9	"the processor identifying that said user input matches a known authorized user of the electronic device, before said readying said device to perform a payment transaction; and, disallowing the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed."
Asserted Claim 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."
Asserted Claim 12	"The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise known user biometric touch characteristics."
Asserted Claim 13	"13. The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user touch gesture"
Asserted Claim 16	"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" "visually presenting a request for user approval of the payment transaction via touch input at said electronic device; and, subsequent to receiving a user-touch input from an identified user, approving performance of said payment transaction via said electronic device."
Asserted Claim 18	"combining said limited-use payment information and said static device account information, to produce a combined payment information"
Asserted Claim 19	"dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information"

'634 Patent	
Asserted Claim 21	"dynamically generating the limited-use payment information based on payment processing authority secret information"
Asserted Claim 27	"wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information."
Asserted Claim 28	"herein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority"
Asserted Claim 29	"a touch-screen display coupled to the processor" "wherein the electronic device is operable to dynamically generate limited-use payment information based on a sequential counter count from the electronic device"
Asserted Claim 32	"wherein the static device account information comprises a static device account number that is unique to the electronic device"
Asserted Claim 36	"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"
Asserted Claim 37	"wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets"
Asserted Claim 38	"dynamically generate the limited-use payment information based on payment processing authority secrets"
Asserted Claim 39	"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" "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;"
Asserted Claim 41	"the payment authority information comprises a secret information shared by both the electronic device and a payment processing authority"
Asserted Claim 42	"wherein the processing authority information comprises a static device account number"
Asserted Claim 45	"the dynamically generated limited-use payment information comprises a cryptogram number, and further wherein the processor

’634 Patent	
	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.”
Asserted Claim 49	“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”
Asserted Claim 51	“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 a continuous user touch.”
Asserted Claim 52	“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.”
Asserted Claim 53	“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 recognition of a valid user identification.”
Asserted Claim 55	“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.”
Asserted Claim 56	“cause the display of an image representing the user-selectable issued payment account” “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” “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”
Asserted Claim 62	“wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further payment

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 149 of 156

'634 Patent	
	information combination is used in place of at least a portion of fixed payment information associated with said user-selectable issued payment account."
Asserted Claim 68	"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"
Asserted Claim 69	"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"
Asserted Claim 70	"wherein said user input device comprises a touch input of the electronic device and wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification via the touch input"
Asserted Claim 72	"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"

To the extent other Asserted Claims contain one of these terms or phrases, either directly or through being dependent on a claim that does, those Asserted Claims are also invalid under 35 U.S.C. § 112.

V. ELIGIBILITY CONTENTIONS - LACK OF PATENT ELIGIBILITY UNDER 35 U.S.C. § 101

Defendant's eligibility contentions are set forth below and in the attached Exhibits E-H. Defendant incorporates by reference the discussion of the state of the art, set forth in Section I, *supra*, the identification of prior art, set forth in Section II, *supra*, as well as the exhibits attached hereto. Defendant also incorporates by reference its Motion to Dismiss and Reply filed in this litigation, Dkts. 32 and 52, and all supporting exhibits filed therewith. Defendant intends to rely on those materials in challenging the subject-matter eligibility of the Asserted Claims and may rely on additional information identified or learned during this case including through discovery.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 150 of 156

These contentions are subject to revision and amendment pursuant to Federal Rule of Civil Procedure 26(e) to the extent appropriate in light of further investigation and discovery, the Court's construction of the Asserted Claims, the positions taken during expert discovery, and/or any future prosecution history for the Asserted Claims or claims in related patents (including, but not limited to, during *inter partes* review or post-grant review of any claims).

Defendant contends that the Asserted Claims are invalid under 35 U.S.C. § 101 (pre-AIA and AIA) because they are directed to abstract ideas and do not contain an inventive concept sufficient to transform the abstract idea into a patent-eligible invention. *See Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2357-58 (2014). Judicial precedent has "long held that [§ 101] contains an important implicit exception" in that "[l]aws of nature, natural phenomena, and abstract ideas are not patentable." *Id.* at 2354 (2014).

35 U.S.C. § 101 lists four broad categories of patent-eligible subject matter but is subject to "an important implicit exception" that "[l]aws of nature, natural phenomena, and abstract ideas," which form the "basic tools of scientific and technological work," are not eligible for patent protection. *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014) (internal quotation marks omitted). "The 'abstract ideas' category embodies 'the longstanding rule that an idea of itself is not patentable.'" *Id.* at 209 (quoting *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972) (quoting *Rubber-Tip Pencil Co. v. Howard*, 87 U.S. 498 (1874)).

Alice set forth a two-step inquiry. "First, we determine whether the claims at issue are directed to one of those patent-ineligible concepts." *Id.* at 217. In making this inquiry, the claims "must be considered as a whole." *Alice*, 573 U.S. at 218 n.3 (quoting *Diamond v. Diehr*, 450 U.S. 175, 188 (1981)). If the claims recite an abstract idea, the second step requires a "search for an 'inventive concept'— an element or combination of elements that is 'sufficient to

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 151 of 156

ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" *Id.* at 218 (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 73 (2016)). "A claim that recites an abstract idea must include 'additional features' to ensure 'that the claim is more than a drafting effort designed to monopolize the abstract idea.'" *Id.* at 221 (quoting *Mayo*, 566 U.S. at 78) (alterations omitted). The recited "additional features must be more than well-understood, routine, conventional activity." *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 1335, 1339 (Fed. Cir. 2013) (internal quotations omitted). The Asserted Claims fail both steps of the *Alice* analytical framework and thus are patent ineligible.

Representative claims may be used for the *Alice* analysis when the claims are "substantially similar and linked to the same abstract idea." *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat'l Ass'n*, 776 F.3d 1343, 1348 (Fed. Cir. 2014); *Smart Sys. Innovations, LLC v. Chicago Transit Auth.*, 873 F.3d 1364, 1368 n.7 (Fed. Cir. 2017) (concluding that claims "should rise or fall together" when they "contain only minor differences in terminology but require performance of the same basic process") (internal quotation omitted). "[T]he representativeness inquiry must be 'directly tethered to the claim language.'" *Id.* at *11 (quoting *Solutran, Inc. v. Elavon, Inc.*, 931 F.3d 1161, 1168 (Fed. Cir. 2019)). Claim 19 of the '579 Patent is representative of all Asserted Claims because it is directed to the patent-ineligible abstract idea of generating limited-use payment information to perform a payment transaction and further recites only generic computer components and functional, result-oriented limitations. *See* '579 Patent at 24:65-25:24; *see also* Dkts. 32, 52. The Asserted Claims are substantially similar because they each try to encompass the idea of generating limited-use payment information for performing a payment transaction and do so using substantially similar functional limitations to those recited in Claim 19 of the '579 Patent. *See Universal Secure*

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 152 of 156

Registry LLC v. Apple Inc., 10 F.4th 1342, 1349 (Fed. Cir. 2021), *cert. denied*, 142 S. Ct. 2707 (2022) (holding claims "directed to a method for enabling a transaction between a user and a merchant, where the merchant is given a time-varying code instead of the user's secure (credit card) information" directed to an abstract idea and invalid under § 101). Specifically, the Asserted Claims are broadly directed to payment-authorizing actions, limited-use payment information generation actions, and payment information transmission actions. The Asserted Claims recite functional steps to perform transactions using substitute payment information; facilitate transactions using limited-use information in place of issuer-provided payment information; and/or generate substitute payment information for use in place of a user's secure payment information (e.g., all or a portion of an issuer-provided payment account number) and transmit that substitute information to perform a transaction. Like Claim 19 of the '579 Patent, the Asserted Claims otherwise recite generic and conventional computer components (*e.g.*, processor, memory, display, input, and output). In short, these claims exhibit no "meaningful difference" because they disclose "performance of the same basic process" with only immaterial variations. *Accenture Glob. Servs. v. Guidewire Software, Inc.*, 728 F.3d 1336, 1344 (Fed. Cir. 2013) (finding that because the claims contain only "minor differences in terminology [but] require performance of the same basic process," they should rise or fall together).

The limitations of the Asserted Claims, individually or as an ordered combination, do not provide an inventive concept; neither the claims nor the specifications of the Asserted Patents provide for implementing the abstract idea using anything other than conventional technology. Aside from the abstract idea, the Asserted Claims include only well-understood, routine, and conventional components and steps. The Asserted Claims do not improve any aspect of technology, as they recite nothing more than using generic known components and user

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 153 of 156

interfaces to perform well-known functions. The well-understood, routine, and conventional nature of the components and steps of the Asserted Claims are demonstrated by the discussion of the state of the art, set forth in Section I, *supra*, and the identification of prior art and prior art itself, set forth in Section II, *supra*, including the charts attached to this document. The Asserted Claims fail to provide any sort of inventive concept that would transform the abstract idea to which they are directed into patent-eligible inventions. Exhibits E-H attached hereto further detail Defendant's factual and legal bases for their Subject-Matter Eligibility Contentions.

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 154 of 156

DATED: April 3, 2025

By: */s/ Matthias A. Kamber*

Robert W. Unikel (*pro hac vice*)
robertunikel@paulhastings.com
PAUL HASTINGS LLP
71 S. Wacker Drive, Suite 4500
Chicago, IL 60606
Telephone: (312) 499-6000
Facsimile: (312) 499-6100

Matthias A. Kamber
matthiaskamber@paulhastings.com
PAUL HASTINGS LLP
101 California Street, 48th Floor
San Francisco, CA 94111
Telephone: (415) 856-7000
Facsimile: (415) 856-7100

Elizabeth L. Brann (*pro hac vice*)
elizabethbrann@paulhastings.com
PAUL HASTINGS LLP
4655 Executive Drive, Suite 350
San Diego, CA 92121
Telephone: (858) 458-3000
Facsimile: (858) 458-3005

Robert R. Laurenzi (*pro hac vice*)
robertlaurenzi@paulhastings.com
PAUL HASTINGS LLP
200 Park Avenue
New York, NY 10166
Telephone: (212) 318-6000
Facsimile: (212) 319-4090

James V. Razick (*pro hac vice*)
jamesrazick@paulhastings.com
Jason Mikus (*pro hac vice*)
jasonmikus@paulhastings.com
Puja V. Patel (*pro hac vice*)
pujapatel@paulhastings.com
PAUL HASTINGS LLP
2050 M Street NW
Washington, D.C. 20036
Telephone: (202) 551-1700
Facsimile: (202) 551-1705

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 155 of 156

Nathaniel St. Clair, II
Texas State Bar No. 24071564
nstclair@jw.com
JACKSON WALKER LLP
2323 Ross Avenue, Suite 600
Dallas, Texas 75201
Telephone: (214) 953-6000
Facsimile: (214) 953-5822

Katharine Lee Carmona
TX State Bar No. 00787399
kcarmona@jw.com
JACKSON WALKER LLP
100 Congress Avenue, Suite 1100
Austin, Texas 78701
Telephone: (512) 236-2000
Facsimile: (512) 236-2002

Erica Benites Giese
Texas State Bar No. 24036212
egiese@jw.com
JACKSON WALKER LLP
1900 Broadway, Suite 1200
San Antonio, Texas 78215
Telephone: (210) 978-7700
Facsimile: (210) 978-7790

Attorneys for Defendant
GOOGLE LLC

CERTIFICATE OF SERVICE

I hereby certify that on the 3rd day of April, 2025, a true and correct copy of the foregoing document was served electronically on all counsel of record.

/s/ Matthias A. Kamber
Matthias A. Kamber

CARDWARE EXHIBIT 2015
GOOGLE v. CARDWARE IPR2025-01361
Page 156 of 156