UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

OV LOOP, INC., a Delaware corporation, Plaintiff, -v- MASTERCARD INCORPORATED, and MASTERCARD INTERNATIONAL INCORPORATED, both Delaware corporations, Defendants.	CIVIL ACTION NO. 7:23-cv-1773 JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff OV Loop, Inc. ("OV Loop") hereby files this Complaint against Mastercard Incorporated ("Mastercard, Inc.") and Mastercard International Incorporated ("Mastercard International") (collectively "Mastercard" or "Defendants"), and alleges on personal knowledge as to its own acts, and on information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1. This is an action for patent infringement under the Patent Laws of the United States, 35 U.S.C. § 1 *et seq.*, to prevent and enjoin Mastercard, from infringing and profiting, in an illegal and unauthorized manner, and without authorization and/or consent from OV Loop, from U.S. Patent No. 10,032,171 ("Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device") ("the '171 Patent" or the "Patent-in-Suit") and pursuant to 35 U.S.C. § 271, and to recover damages, enhanced damages, attorneys' fees and costs.

2. Mastercard has directly infringed and continues to directly infringe (literally

and/or under the doctrine of equivalents), has contributed to and continues to contribute to infringement of, and has induced and continues to induce infringement of one or more Claims of the '171 Patent. A true and correct copy of the Patent-in Suit is attached hereto as Exhibit A and incorporated here by reference.

3. The '171 Patent was duly and legally issued by the United States Patent and Trademark Office ("USPTO") on July 24, 2018. The '171 Patent was assigned to OV Loop. OV Loop is the sole legal and rightful owner of the Patent-in-Suit. OV Loop seeks injunctive relief and monetary damages.

II. THE PARTIES

4. OV Loop is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business at 73 Holton St., Woburn, Massachusetts 01801.

5. Mastercard Inc. is a corporation organized under the laws of the State of Delaware, with its principal place of business at 2000 Purchase Street, Purchase, New York 10577.

6. Mastercard International is a corporation organized under the laws of the State of Delaware, with its principal place of business at 2000 Purchase Street, Purchase, New York 10577. Mastercard International is a subsidiary of Mastercard Inc.

III. JURISDICTION AND VENUE

7. This is an action for patent infringement arising under the patent laws of the United States of America, 35 U.S.C. § 1, *et seq.*

8. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and

1338(a).

9. This Court has personal jurisdiction over Mastercard because it has engaged in systematic and continuous contacts and business activities in this District. Mastercard has committed acts of patent infringement giving rise to this action within the Southern District of New York, where it maintains a regular and established place of business.

10. Mastercard is subject to this Court's specific and general personal jurisdiction pursuant to its substantial business in this forum, including: (a) at least a portion of the infringements alleged herein; (b) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in this forum state and in this District; and (c) having its principal place of business in this District (Westchester).

11. Venue is proper in this District under 28 U.S.C. § 1400(b) because Mastercard has an established and principal place of business in this District. In addition, Mastercard has committed acts of patent infringement in this District, and OV Loop has suffered harm in this District. Both Mastercard's Global and North American headquarters are located in this District (Westchester) and Mastercard's "Tech Hub" is located in this District (Manhattan). *See* https://www.mastercard.us/en-us/vision/who-we-are/global-locations.html.

IV. FACTUAL ALLEGATIONS

The Old Economy: Card Networks, Issuers, and the Interchange Fee

12. Banks issue credit and debit cards. Banks charge fees for the use of such cards in stores and online, and may collect interest on carried balances.

13. Almost all banks use either Visa or Mastercard as the "network" to process transactions. These networks provide the "payment rails" that the transactions use.

14. When accepting payment through a Visa or Mastercard branded card, the merchant perforce pays a "merchant discount fee" within which includes an "interchange fee," typically set as a percentage of the transaction value. These interchange fees are set by Visa and Mastercard.

15. Issuing banks compete for customers by offering various card products, including credit cards, debit cards, stored value cards, and other prepaid products which may or may not carry additional features including the ability to earn "cash-back" or loyalty incentives, and the like.

16. There are two basic types of retail commerce today—online, or "e-commerce," and "in-store" or traditional "bricks and mortar stores," ("B&M") e.g., the neighborhood CVS. Combined, U.S. e-commerce and B&M sales for 2022 totaled more than $5 Trillion. Today, approximately 85% of all retail transactions take place in B&M retail locations, while circa 15% of such transactions are online. The online commerce retail percentage is growing rapidly, however, year-over-year.

17. Mastercard and Visa transitioned to e-commerce in the 90's and later adopted e-commerce to support their payment network methods on PCs, tablets and mobile devices including via the likes of Apple Pay and Samsung Pay. This was in response to new alternative payment methods that arose such as PayPal, Venmo, BNPL, Alipay, and others.

18. These new payment platforms threaten to undercut and disintermediate, *i.e.*, render irrelevant, Mastercard and Visa's transaction revenue and their existing business model. *See* Mastercard Inc.'s December 31, 2022 10K at 30, available at https://d18rn0p25nwr6d.cloudfront.net/CIK-0001141391/3f400cd7-b9fb- 4732-9e59-c669ea4fe0cc.pdf ("Disintermediation from stakeholders both within and outside of the

payments value chain could harm our business …. Although we partner with fintechs and technology companies (such as digital players and mobile providers) that leverage our technology, platforms and networks to deliver their products, they could develop platforms or networks that disintermediate us from digital payments and impact our ability to compete in the digital economy. These companies may also develop products or services that compete with our customers within the payments ecosystem and, as a result, could diminish demand for our products and services"); *id*. at 21 ("Competition[:] …. Alternative Payments Systems and New Entrants …. Many of these providers, who in many circumstances can also be our partners or customers, have developed payments systems focused on online activity in e-commerce and mobile channels (in some cases, expanding to other channels), and may process payments using in-house account transfers, real-time account-based payments networks or global or local networks. Examples include digital wallet providers (such as Paytm, PayPal, Alipay and Amazon), point of sale financing/buy-now-pay-later providers (such as Klarna, Affirm and Afterpay), mobile operator services, mobile phone-based money transfer and microfinancing services (such as M-PESA) and handset manufacturers").

19. For this reason, Mastercard and Visa have, over the past several years, made a concerted push into the e-commerce payments arena. Both companies have implemented their own online wallet solutions with Masterpass by Mastercard, and Visa Checkout by Visa. They both control and dominate the mobile tokenization services, *see* below, to distribute bank tokens to mobile wallets such as Apple Pay and Samsung Pay. Their size and strength, along with a desire to exclude competitors, have made other Token Service Providers uncompetitive in providing mobile payment tokens to digital wallets. This includes the efforts of banks to build their own cloud-based token solutions for their own banking and payment apps.

20. It is widely accepted that digital, *e.g.*, electronic payments from cards or devices, will become increasingly important in the years to come. That is, consumers will use their phones or smartwatches or other digital devices to purchase goods, both online and in retail, B&M locations. Both Mastercard and Visa view this digital payment business as existentially important to their brands, business, future, and cash flow.

21. This case turns on Mastercard's efforts to control the digital payment space, in part by excluding others, as set forth below.

Digital Wallets and Fraud Prevention

22. A digital wallet application is an application on a mobile device or on the Web loaded with payment information, *e.g.*, credit and debit cards. The Apple Pay application, loaded on the iPhone, is a digital wallet application, as is Samsung Pay application loaded on a Samsung phone. The wallet application need not be hosted on a phone, but can instead reside on a key fob, or an electronic watch, or any other small, electronic device, *e.g.*, a Garmin smartwatch. The wallet functionality can also be used for online shopping from a web browser.

23. One obvious advantage to a digital wallet is that it collects all card and payment information in one place. But that is not the principal benefit of a digital wallet. As now mandated by Mastercard standards, digital wallets **must** communicate with retailers using one-time use cryptograms and obfuscated conventional card data account identifying information, which reveal nothing about the cardholder's actual payment data, as set forth below.

24. This is important. Most credit card fraud does not come from people stealing and using cards. It, rather, comes from people stealing card **data**, the **P**ersonal **A**ccount **N**umber ("PAN"); the expiry date; and the three (Mastercard and Visa) or four (Amex) Card Verification Value ("CVV"). With these data, thieves ("fraudsters") then can purchase items online or

quickly clone a physical card.

25. This is all possible because traditional card data is **static**: it does not change transaction-by-transaction; it does not change over time (except over years). Making payment data "dynamic," so that the data changes with every transaction, or in a short-preset interval (e.g., one hour), has been a pivotal financial technology ("Fintech") goal for decades. Stealing one- time payment data compromises nothing and can dramatically reduce fraud.

26. An early version of transitory data came in "smartcards," that is a payment card equipped with a wafer battery and onboard CPU to generate new dynamic numbers or cryptograms with every use. Smartcards were engineered to change payment data, transaction-by-transaction, or over short time periods and are read by smartcard readers; the dynamic cryptogram used yesterday would not work today. Software installed at the backend of the participating networks/banks would receive the unique one-time use data, check its integrity by running parallel software at the network/bank's backend, and approve the transaction if the transitory data matched. This requires both banks to issue cards with chips on them, and requires merchants to have Point-of-Sale ("POS") terminals to accept chip cards. It required great expense and a long time for the U.S. to migrate to chip enabled POS terminals.

27. Other attempts included trying to make the magnetic stripe data dynamic so there would not be a need to change the merchant POS. However, building a card that can change magnetic stripe data on the fly, as swiped, presents a difficult engineering challenge. POS terminals, *e.g.*, a Hypercom or Verifone terminal, had very tight swipe time and data communication requirements, and the early dynamic magnetic stripe cards would often not satisfy these hurdles. A debit or credit card that works only some of the time is not a marketable product.

Tap to Pay: NFC

28. As all of this was underway, companies were working on tap-to-pay technologies; *e.g.*, one could just tap a mobile device or an enabled card (a "contactless card" ISO14443 standard) against a "contactless" enabled, e.g., "Near Field Communication" ("NFC") enabled, POS reader to initiate a transaction. NFC is a short distance radio transmission. Until several years ago, these tap-to-pay products were not accepted in most merchant locations (fewer than a third of the POS terminals in the U.S. were NFC enabled prior to 2011). This has changed over the past decade with tap-to-pay, or "contactless," payments rapidly increasing in popularity.

MST Emulation

29. In 2012, payment POS pioneers George Wallner and Will Graylin, began working on an additional tap-to-pay communication method, called "Magnetic Secured Transmission," or "MST." With MST, dynamic magnetic stripe data can be generated and transmitted to virtually any POS terminal through the magnetic stripe reader, regardless of whether the terminal had been NFC enabled. The hardware device would emulate the magnetic card swipe data to be read by virtually any POS terminal, including old Micros or NCR terminals and Square magnetic stripe adaptors and conventional Ingenico and Verifone terminals. It did so by sending current through embedded coils of wire that generated pulses of magnetic fields that mimicked (emulated) the swipe data, and communicated these data to the POS terminal, without using NFC. MST thus made "contactless" payments work with almost every legacy POS terminal in the country.

30. In 2015, Messrs. Graylin and Wallner sold their company, LoopPay, to Samsung for roughly $320 million, including post-close earnouts. It became part of Samsung Pay, where Mr. Graylin was the Global Co-GM and helped launch Samsung Pay with the MST technology

built into billions of Galaxy phones starting in 2015, and also Galaxy smartwatches.

Tokenization

31. Transaction security is, of course, vitally important in any card transaction. To enhance security, mobile phones devices working remotely began to use a process called "tokenization."[1] In this process, a chip on your iPhone, known as a "Secure Element" ("SE"), would store the "token" and generate cryptograms to be sent to the POS via NFC, replacing your critical data (PAN; expiry; CVV) and transact this one-time used cryptogram with token to the merchant POS, and onto the card network. That is, the token replaces the static card data, such that the static data was not communicated to the merchant. Corollary software—card network software on card network servers—would decrypt the cryptogram with the "token," and if the two matched, then this transaction went forward. This process replaced the static authorization data with new, transitory data.

32. This is how Apple Pay works today: an iPhone has a physical chip that generates one-time payment data. The iPhone communicates with NFC equipped terminals using short radio bursts. This is a hardware-based solution, the SE chip, coupled with enabling software. The Apple Pay SE and Apple Pay system are proprietary to Apple, since Apple controls the phone hardware and the payment application on the hardware.

HCE

33. In 2014, Google announced a cloud-based tokenization system for mobile wallets on Android devices. This system did **not** require that the mobile device contain a physical SE,

[1] "Tokenization" and "token" are used, somewhat confusingly in the industry, to sometimes refer to the process of obfuscating conventional card data account identifying information and the resulting data used in the conventional data's stead, and that process (and result) combined with the provisioning of cryptographic keys to use in generating cryptograms.

be it a smartphone, which Google was not the manufacturer most of the time of, or a fob, or a smartwatch, etc. Instead, the cloud would provide or emulate an SE, using solutions such as Hardware Security Modules (HSMs) to create tokens and non-permanent cryptographic keys that can be sent to mobile devices and stored in the devices' memory. The cloud system generates digital wallet tokens for the mobile device. In addition to sending a tokenized PAN that changes on every transaction to replace static account identifying data with the token, the cloud system sends the mobile device a non-permanent cryptographic key. With this key, the mobile device can generate and send a POS terminal a 1-time-use cryptogram (data encoded using the key), but not the key itself, along with the tokenized PAN, to use in authenticating a transaction. With the token in hand, the remote cloud system can then identify the key that should have been used to generate the cryptogram and generate its own cryptogram. If the cloud system generated cryptogram and the mobile device cryptogram do not match, then the transaction will not be authorized. Google announced this as an innovative and novel advance in payment technology and security.

34. This cloud-based key generation method and system was invented in 2011 by OV Loop's predecessor and now wholly owned subsidiary SimplyTapp. SimplyTapp coined the phrase "Host Card Emulation," or "HCE," to refer to this technology, which is the term used throughout the industry today. Since 2014, Android phones use HCE, not a chip-based SE.

35. With the prominent exception of Apple, most mobile wallets used for NFC payments now use HCE.

<u>The Plaintiff: OV LOOP</u>

36. Mr. Graylin is a FinTech innovator and serial technology entrepreneur. He founded OV Loop in 2008, as an investor and board member, to develop a mobile

communications "app." He became C.E.O. of OV Loop in 2018 to create a "super-app" company.

37. Mr. Graylin served his country for more than five years as a Nuclear Submarine Officer. He then earned two master's degrees from MIT, and holds a dozen patents for payment related inventions. He also just completed serving seven years on the Board of Directors for Synchrony Financials (NYSE: SYF, the largest private label credit card issuer in the world). Mr. Graylin taught part time at MIT before COVID and is currently an MIT Connection Science Fellow with Dr. Sandy Pentland of the Media Lab. He is also an investor/director/mentor in and to numerous high-tech startups and non-profit organizations including ROCA and Global Unites.

38. Prior to becoming C.E.O. of OV Loop, Mr. Graylin was Global Co-GM of Samsung Pay, after Samsung acquired his company LoopPay, which he founded. He helped launch Samsung Pay with LoopPay's patented MST technology.

39. LoopPay created the world's first contactless digital wallet with 90%+ point-of-sale acceptance. LoopPay and Samsung Pay were at the forefront of contactless payments and created a platform that brought together issuers, merchants and consumers that facilitated a seamless and rewarding digital wallet experience and tokenized contactless payments to over 90% of existing POS terminals.

40. Prior to LoopPay and Samsung Pay, Mr. Graylin was also the founder and former C.E.O. of ROAM Data. ROAM Data was the largest provider of mobile POS solutions for merchant service providers, including competitors of Square. ROAM Data was later acquired by Ingenico, the world's largest POS terminal manufacturer.

41. Prior to ROAM, Mr. Graylin founded WAY Systems, the world's first pocket-sized mobile point-of-sale provider (acquired by Verifone); and EntitleNet, a security software

company, acquired by BEA Systems to become Web Logic Enterprise Security, which later became part of Oracle.

42. Mr. Graylin is also Chief Executive Officer at Indigo Technologies, which delivers ultra-efficient and affordable EVs powered by patented road sensing smart-wheels that provide roomier, smoother, and safer ride experiences with lower carbon footprint and lower cost of ownership.

43. In short, Mr. Graylin is a storied and successful Fintech entrepreneur, who has founded, built, and sold numerous prior technology companies.

OV Loop and its Technology

44. Mr. Graylin has been leading OV Loop directly, as its C.E.O., since 2018, to create a "super-app," including a multi-card digital wallet functional at "bricks and mortar" (retail stores) POS terminals. A super-app is one app that enables e-commerce, retail POS transactions, holds relevant user data and credentials, handles communications and rewards, and coalesces and simplifies the digital life we all lead today.

45. Super-apps have been very successful abroad. For example, China has the largest digital buyer population in the world, amounting to more than 780 million people. In 2020, eighty-two percent of China's Internet users used online payments at least once. The most prevalent Fintech "app" in the country is WeChat, a super-app that facilitates every type of commerce transaction and interaction ranging from large global enterprises to the smallest street vendor. Similarly, Alipay claims to operate with over 65 financial institutions, including Visa and MasterCard, to provide payment services for Taobao and Tmall, as well as over 460,000 online and local Chinese businesses. Tech giant Alibaba's Alipay's payment service alone reaches 678.5 million active users. In 2021, China's Ministry of Industry and Information

Technology (MIIT) mandated the opening up of the "walled garden" ecosystems of major tech companies, leading to the introduction of interoperability of payment QR codes of Alipay and competing WeChat Pay and UnionPay's Cloud QuickPass platforms.

46. None of this is true in this country. Due to a combination of a highly-fractured banking segment (many competitive players), incompatible POS systems that only work with certain payment or rewards solutions, and far too many apps for each brand or merchant, combined with a "walled garden" approach by the big tech wallet platform providers (*e.g.*, Apple), there are significant challenges in unifying and simplifying the commerce experiences for the 250+ million adults in the United States, and many other countries. In fact, while the need has been noted in the press for almost a decade, no one had introduced a digital super-app in this country, including a fully cross-platform digital wallet. Big tech platform providers are beholden to their fractured user base inside their "walled gardens," and financial institutions, large retailers, and telecom companies all compete with one another; thus, it requires a new company that focuses on building the infrastructure for a real digital super-app, that can close the wallet and POS loop for buyers and sellers, across mobile devices, channels, and tender types.

47. Mr. Graylin has been building OV Loop for nearly 5 years to remedy this deficiency, and introduce a digital wallet super-app in this country that would work across all financial institutions, all payment networks, all tender types, and outside of the walled gardens of big tech. This vision necessarily includes the ability to perform both e-commerce and B&M transactions, and to do so completely and securely, in the best interest of the American people and the protection of their payment data. Professor Scott Galloway of New York University said in his November 2021 New York Magazine article, "Super-Apps Are Inevitable," that he is "convinced that constructing a **U.S. super-app is the strategic-imperative of the next decade**

and could result in the first $10 trillion company."

https://nymag.com/intelligencer/2021/11/facebook-metaverse-super-apps.html.

48. To that end, in June 2018, OV Loop acquired SimplyTapp, an Austin-based company founded by Doug Yeager. Mr. Yeager is widely credited as the inventor of Host Card Emulation, "HCE."

49. Yeager invented HCE. He filed the patent application that would later issue as the here asserted '171 Patent on August 30, 2012. OV Loop now owns the '171 Patent.

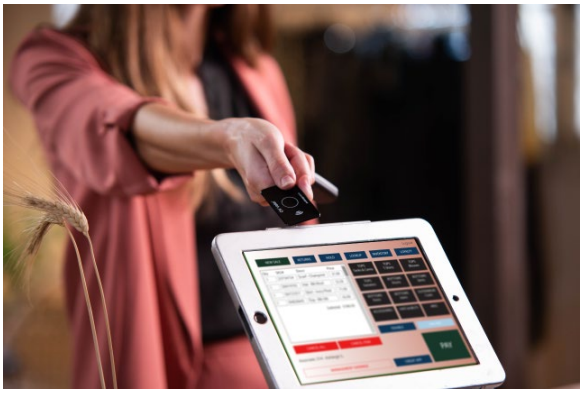
50. OV Loop developed software to implement a full digital wallet solution. It also built hardware, a key fob device, which is configured to pull tokens from the phone-based digital wallet and transmit those tokens via NFC or MST to brick and mortar POS terminals (*e.g.*, buying paper towels at CVS). OV Loop called this hardware device the "OV Valet."

51. Below are images of the OV Valet:

OV Valet being used for an MST purchase

OV Valet in retail packaging

OV Valet being used for an NFC purchase



Promotional image of handing OV Valet to a cashier at a retail POS

<u>OV Loop's '171 Patent</u>

52. In August 2012, OV Loop's predecessor entity, SimplyTapp, filed U.S. Patent Application No. 13/599,647. This patent application matured into U.S. Patent No. 10,032,171,

"Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device," the Patent-in-Suit.

53. OV Loop owns the '171 Patent, and has the full legal right to enforce the '171 Patent.

54. Broadly speaking, the '171 Patent describes the Host Card Emulation approach to mobile card wallets. The sole named inventor, Doug Yeager, is widely credited as the inventor of HCE.

55. Independent Claim 1 reads as follows:

> A method for secure application-based participation in a payment card transaction authorization process by a mobile device, the method comprising:
> at a mobile device, executing an application in an operating system of the mobile device, the application interrogable by an electronic reader, over a first communications channel, for digital credential data corresponding to an account having a corresponding digital credential and configured to request, from a remote computer system hosting the corresponding digital credential, over a wireless network that is separate from the first communications channel, data associated with the account and generate cryptograms requested during interrogations over the first communications channel using the data associated with the account received from the remote computer system, wherein the application does not access a permanent cryptographic key issued for the digital credential during the interrogations;
> requesting by the application, from the remote computer system, over the wireless network, a first set of data associated with the account;
> receiving by the application, from the remote computer system, over the wireless network, the first set of data associated with the account, the first set of data associated with the account usable by the application to formulate an application protocol data unit response, the first set of data comprising a first non-permanent cryptographic

key associated with the account;

locally storing the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;

participating by the application in an interrogation between a point-of-sale (POS) terminal and the mobile device comprising:

receiving at least one POS command communication sent by the POS terminal over the first communications channel, wherein the at least one POS command communication comprises a request for digital credential data to authorize a transaction against the account, the request for digital credential data including a cryptogram request;

generating a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

responding to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response communication from the mobile device to an electronic reader through the communication channel, the at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account;

subsequent to the interrogation, requesting by the application, from the remote computer system, over the wireless network, a second set of data associated with the account;

receiving by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data comprising a second non-permanent cryptographic key associated with the account; and

storing the received second non-permanent cryptographic key as the local cryptographic key associated with the account to change the local cryptographic key associated with the account

between at least two interrogations.

56. Independent Claim 17 reads as follows:

> A system for secure application-based participation by a mobile device in point-of-sale interrogations, the system comprising:
> a mobile device comprising:
> a controller configured to route communications received over a communication channel from an electronic reader;
> a wireless interface to connect to a wireless network that is separate from the communication channel;
> a processor;
> a computer readable storage medium accessible by the processor storing an application executable in an operating system of the mobile device, the application, when executed, interrogable over the communications channel for digital credential data to authorize transactions against an account having a corresponding digital credential hosted at a remote computer system, wherein the application does not have access to a permanent cryptographic key issued for the digital credential and the application is executable to:
> request from the remote computer system, over the wireless network, a first set of data associated with the account;
> receive by the application, from the remote computer system, over the wireless network, the first set of data associated with the account usable by the application to formulate an application protocol data unit response, the first set of data comprising a first non-permanent cryptographic key associated with the account;
> store the first non-permanent cryptographic key at the mobile device as a local cryptographic key associated with the account;
> during an interrogation:

receive at least one point-of-sale (POS) command communication sent by POS terminal to the mobile device over the communications channel, wherein the at least one POS command communication comprises a request for digital credential data, the request for digital credential data including a cryptogram request;

access the local cryptographic key associated with the account;

generate a response cryptogram based on a set of inputs and the local cryptographic key associated with the account, wherein the response cryptogram does not include the local cryptographic key associated with the account used to generate the response cryptogram; and

respond to the at least one POS command communication, wherein responding to the at least one POS command communication comprises sending at least one device response to the electronic reader through the communication channel, the at least one device response communication comprising at least one response application data protocol unit containing the response cryptogram and an account identifier for the account;

subsequent to the interrogation, request from the remote computer system, over the wireless network, a second set of data associated with the account;

receive by the application, from the remote computer system, over the wireless network, the second set of data associated with the account, the second set of data associated with the account comprising a second non-permanent cryptographic key associated with the account; and

store the received second non-permanent cryptographic key as the local cryptographic key associated with the account to change the local cryptographic key associated with the account between

at least two interrogations.

57. Dependent Claim 25 reads as follows:

> The system of claim 17, further comprising the remote computer system, the remote computer system configured to generate non-permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network.

58. The '171 Patent describes a solution to a complex and computer centric problem. Its claims represent novel and distinct improvements to computer systems over the prior approaches known in the art. There is no old-world analogue.

<u>The Mastercard MCBP Standards and MDES System</u>

59. In February 2014, Mastercard announced that it would "publish a specification that leverages Host Card Emulation (HCE) for secure near field communication (NFC) payment transactions." *See* https://newsroom.mastercard.com/press-releases/mastercard-to-use-host-card-emulation-hce-for-nfc-based-mobile-payments/. As Mastercard then explained, "HCE enables payments and other NFC services – including loyalty programs, building access and transit passes – to be delivered without the use of a secure element (SE)." *Id*. Mastercard described its HCE specification as "**mark[ing] a significant industry milestone** that, in addition to MasterCard's longstanding support for embedded and SIM-based SE implementations, will drive greatly expanded availability of mobile contactless payments for consumers." Mastercard's then Group Head of Emerging Payments described HCE as providing "'a very attractive way forward to launch an increased number of NFC-based offerings,'" and explained that Mastercard "'continue[d] to set standards and deliver solutions to [its] partners and customers that deliver great experiences for safe and secure digital payments." *Id*. Mastercard further stated that its "approach combines custom software on the mobile device with highly secure cloud-based

processing," and that it would "publish its secure remote payment specifications during the first half of 2014."

60. Mastercard promptly implemented its HCE specifications.[2] *See, e.g.,* Pandy & M. Crowe, Understanding the Role of Host Card Emulation in Mobile Wallets, Payment Strategies, Federal Reserve Bank of Boston (May 10, 2016), available at https://www.bostonfed.org/publications/payment-strategies/understanding-the-role-of-host-card-emulation-in-mobile-wallets.aspx ("Following the EMV spec, when a payment card is provisioned to a mobile wallet, the token service provider (TSP) tokenizes the PAN and stores the token (whether on the SE, mobile OS, or TEE) in the phone. Additionally, **MasterCard** … **modified their contactless specifications to support single/limited use keys and cloud cryptograms that recognize HCE tokens as valid payment credentials**").

61. These Mastercard standards were implemented no later than the summer of 2014. Mastercard's HCE standards are required: non-compliance is not possible. For example, Mastercard has a set of standards it refers to as "Mastercard Cloud-Based Payments" ("MCBP"), which includes HCE requirements. *See, e.g.,* Mastercard Engage Use Case for Issuers-Technology Partners Building an NFC Issuer Wallet, available at https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/large-enterprises/other/use-case-for-issuers-building-an-nfc-issuer-wallets-04122019.pdf ("An HCE-based payment application is a secure software solution that enables mobile devices for contactless payments through the NFC interface of the device. **MCBP is the Mastercard solution for HCE-based payments**"); *id*. ("The MPA (Mobile Payment Application) is the

[2] Mastercard did not, however, make its detailed specifications public. Mastercard only provides this documentation to entities it decides to collaborate with, and even then, only after these entities enter into formal agreements with Mastercard.

component of the **Mastercard solution for HCE** (Host Card Emulation)-based payments, **called MCBP** (Mastercard Cloud-Based Payments), which resides in the mobile device"); *id*. ("MPA (Mobile Payment Application) is the component of the MCBP solution that resides in the mobile device").

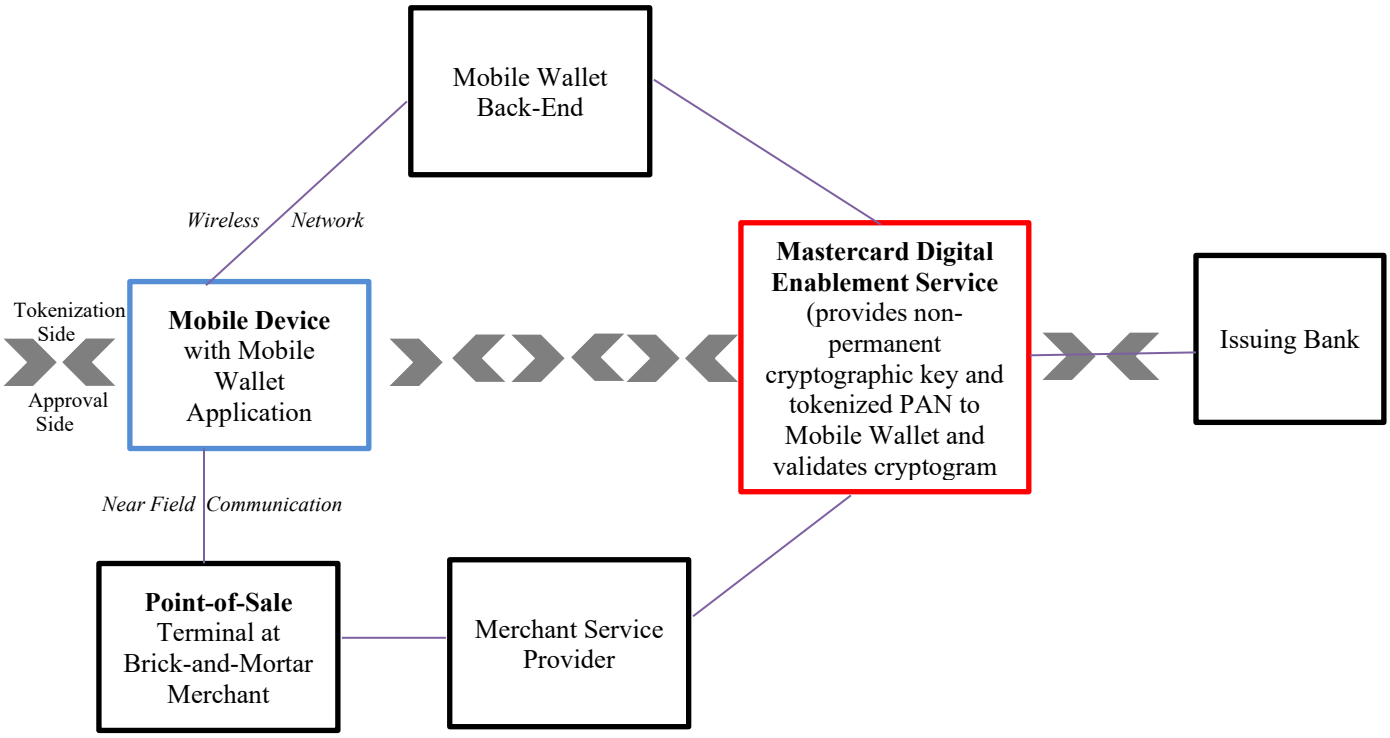
62. In addition to including Mastercard HCE requirements, MCBP governs the Mastercard HCE approval process. Only entities certified and licensed by Mastercard can implement Mastercard's requirements, and so, any mobile wallet working with Mastercard cards, follows Mastercard's specifications, as mandated by Mastercard. *See* Host Card Emulation (HCE) 101, Smart Card Alliance White Paper, available at https://www.securetechalliance.org/wp-content/uploads/HCE-101-WP-FINAL-081114-clean.pdf ("MasterCard … support for payment apps using HCE that **comply** with their contactless payment specifications"). Mastercard is so the gatekeeper for the use of Mastercard branded cards on any digital wallet.

63. Mastercard does not only control and direct the structure of all HCE systems that work with its cards, it also provides the cloud-based system for its HCE solution. Mastercard calls its system for issuing tokenized PANs and cryptographic keys to mobile wallets, and validating mobile wallet POS transactions, Mastercard Digital Enablement Service ("MDES"). *Compare, e.g.,* Mastercard Rules at 420, Dec. 13, 2022, available at https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/mastercard-rules.pdf ("Mastercard Cloud-Based Payments[:] A specification that facilitates the provisioning of Digitized Account data into a Host Card Emulation (HCE) server and the use of the remotely stored Digitized Account data, along with single-use payment credentials, in Transactions effected by a Cardholder using a Mobile Payment Device. The

Mastercard Digital Enablement Service offers Mastercard Cloud-Based Payments as an on-behalf service") *with id*. at 420 ("Mastercard Digital Enablement Service[:] Any of the services offered by the Corporation exclusively to Customers for the digital enablement of Account and/or PTA Account data, including but not limited to … Mastercard Cloud-Based Payments …").[3]

64. MDES' placement within an exemplary Mastercard HCE ecosystem is illustrated below:

[3] *See also, e.g.*, https://developer.mastercard.com/mdes-pre-digitization/documentation/ ("The Mastercard Digital Enablement Service (MDES) is a suite of on-behalf-of (OBO) services that supports the management and generation of digital payment tokens to enable simpler and secure digital payment experiences. MDES was developed to facilitate the transition from consumer account credentials (PAN) to digital credentials (tokens). These digital credentials maybe be: provisioned to mobile devices, enabling consumers to perform payments via existing contactless point-of-sale (POS) systems …"); Mastercard Engage Use Case for Issuers-Technology Partners for Building an NFC Issuer Wallet, available at https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/large-enterprises/other/use-case-for-issuers-building-an-nfc-issuer-wallets-04122019.pdf ("To offer an NFC issuer wallet to consumers, issuers need to connect the NFC issuer wallet to MDES. MDES will manage the digitization process of the consumer PAN (Primary Account Number) and send the digital credentials to the NFC issuer wallet" & "Tokenization is the replacement of a consumer's PAN with an alternate number, reducing the risk of fraud. Digitization is the process that delivers tokenized card credentials to mobile devices or servers for secure digital payments. MDES is the Mastercard suite of services that offers tokenization and digitization, replacing card numbers with tokens and placing these into digital environments, such as NFC wallets, wearables or secure servers").



65. In addition to mandating what an HCE wallet must do, and providing the back-end tokenization and validation system, Mastercard offers a software development kit for the front-end wallet application. *See, e.g.,* https://developer.mastercard.com/product/mobile-payments-sdk/ ("MCBP Mobile Payment SDK[:] Simplifies the development of **Mastercard Cloud-Based Payments (MCBP) application for Android** and iOS devices … **Supports MDES … Supports in-store Contactless** … as per latest MCBP specification …. MCBP Mobile Payment SDK simplifies the development of Mastercard Cloud-Based Payments (MCBP) wallets for Android and iOS platforms. MP SDK is a solution based on MCBP specifications …. Contactless/NFC Payments[:] With MCBP Mobile Payment SDK, it is easy to add Contactless/NFC payment capability into your wallet application. **NFC payment is supported only for Android platform**").

66. The use of cloud-supplied non-permanent cryptographic keys, for use in generating cryptograms for mobile wallet transaction authorization, is central to Mastercard's MCBP

solution and MDES system. *See, e.g.,* Pandy & M. Crowe, Understanding the Role of Host Card Emulation in Mobile Wallets, Payment Strategies, Federal Reserve Bank of Boston (May 10, 2016), available at https://www.bostonfed.org/publications/payment-strategies/understanding-the-role-of-host-card-emulation-in-mobile-wallets.aspx ("MasterCard uses single use keys (SUKs) …. Multiple SUKs can be stored on a mobile device and as they are used additional SUKs are loaded from the cloud card management vendor to the device"); https://developer.mastercard.com/product/mdes ("Customer-initiated transactions use domain-specific tokens with dynamic data (cryptograms)" & "Customer payments are protected at contactless terminals").

67. Mastercard's HCE standards, including its MCBP specifications, track, step-by-step, and limitation-by-limitation, the claims of the long prior '171 Patent. **As a consequence, any platform compliant with the Mastercard MCBP rules perforce will infringe OV Loop's '171 Patent**. Mastercard, through at least its MCBP specification and systems and processes that incorporate MDES, infringes the Patent-in-Suit. *See* below (Claims).

OV Loop and Mastercard

68. In late 2018, OV Loop, through its C.E.O. Graylin, approached Mastercard to obtain Mastercard certification to enable Mastercard branded cards on the OV Valet.

69. As with everyone else, *see* above, absent Mastercard "certification," the OV Valet could **not** host Mastercard branded cards. This gives Mastercard the power to shutter any digital platform it finds competitive or unwelcome.

70. From 2018 forward, OV Loop had dozens of meetings and calls with Mastercard, all designed to secure the card network's approval of OV Valet. In all calls or meetings, Mastercard seemed enthusiastic and supportive. But it never authorized OV Loop to go forward

with Mastercard branded cards. Here is the chronology of calls and meetings:

a. August 3, 2018: email from Will Graylin to Mohamed Abdelsadek (Subject: Time To Catch Up?)

b. December 13, 2018: email from Justin Flood to Will Graylin (Subject: Mastercard Meeting – Contact)

c. December 13, 2018: Will Graylin meeting with Mastercard

d. December 13, 2018: email from Justin Flood to Will Graylin attaching mutual NDA (Subject: RE: Mastercard Meeting – Next Steps)

e. December 19, 2018: email from Justin Flood to Will Graylin (Subject: RE: Mastercard Meeting – Next Steps)

f. December 19, 2018: email from Will Graylin to Justin Flood, John Frontz, Doug Yeager, John Ayers, Kevin Kozak, and Alejandro Imass (Subject: RE: Mastercard Meeting – Next Steps)

g. September 13, 2019: conversation between Doug Yeager and Daniela Castillo

h. September 16, 2019: email from Doug Yeager to Yannis Tsampalis, Daniela Castillo, Bruce Berger, and Hans Reisgies (Subject: connecting Mastercard + Sequent)

i. September 16, 2019: email from Hans Reisgies to Doug Yeager, Yannis Tsampalis, Daniela Castillo, and Bruce Berger (Subject: Re: connecting Mastercard + Sequent)

j. September 17, 2019: email from Hans Reisgies to Doug Yeager, Yannis Tsampalis, Daniela Castillo, and Bruce Berger (Subject: Re: connecting Mastercard + Sequent)

k. September 18, 2019: email from Bruce Berger to Daniela Castillo (Subject: Fwd: connecting Mastercard + Sequent)

l. September 18, 2019: email from Daniela Castillo to Bruce Berger (Subject: Re: connecting Mastercard + Sequent)

m. September 18, 2019: email from Bruce Berger to Daniela Castillo (Subject: Re: connecting Mastercard + Sequent)

n. September 20, 2019: email from Daniela Castillo to Bruce Berger (Subject: Re: connecting Mastercard + Sequent)

o. September 23, 2019: email from Daniela Castillo to Bruce Berger (Subject: Re: connecting Mastercard + Sequent)

p. September 25, 2019: email from Bruce Berger to Daniela Castillo attaching document with answers to recently raised questions (Subject: Re: FW: connecting Mastercard + Sequent)

q. September 26, 2019: telephone call between Bruce Berger and Daniela Castillo

r. September 27, 2019: email from Tom Fifelski to Daniela Castillo attaching documents (Subject: Requested Documents)

s. September 27, 2019: email from John Frontz to Daniela Castillo attaching financials (Subject: Re: Mastercard Application – Confidential Historical Financials)

t. October 25, 2019: email from Doug Yeager to Will Graylin copied to Mastercard (Subject: Re: FW: connecting Mastercard + Sequent)

u. October 31, 2019: email from Daniela Castillo to Doug Yeager and Will Graylin (Subject: Re: connecting Mastercard + Sequent)

v. November 11, 2019: email from Will Graylin to Daniela Castillo, Doug Yeager, and Bill Bachrach (Subject: RE: connecting Mastercard + Sequent)

w. November 12, 2019: email from to Daniela to Will Graylin, Doug Yeager, and Bill Bachrach (Subject: Re: connecting Mastercard + Sequent)

x. November 12, 2019: email from Will Graylin to Daniela Castillo, Doug Yeager, and Bill Bachrach (Subject: Re: connecting Mastercard + Sequent)

y. November 18, 2019: email from Daniela Castillo to Will Graylin (Subject: FW: connecting Mastercard + Sequent)

z. November 18, 2019: email from Will Graylin to Daniela Castillo (Subject: RE: connecting Mastercard + Sequent)

aa. November 22, 2019: email from Daniela Castillo to Will Graylin (Subject: Re: connecting Mastercard + Sequent)

bb. November 22, 2019: email from Will Graylin to Daniela Castillo (Subject: RE: connecting Mastercard + Sequent)

cc. November 26, 2019: email from Daniela Castillo to Will Graylin (Subject:

Re: connecting Mastercard + Sequent)

dd. November 26, 2019: email from Will Graylin to Daniela Castillo (Subject: RE: connecting Mastercard + Sequent)

ee. December 3, 2019: email from Daniela Castillo to Will Graylin (Subject: RE: connecting Mastercard)

ff. December 4, 2019: email from Will Graylin to Daniela Castillo attaching C-Commerce Voice Powered Omni Chat/Wallet presentation (Subject: RE: connecting Mastercard)

gg. December 12, 2019: email from Daniela Castillo to Will Graylin (Subject: FW: connecting Mastercard)

hh. December 13, 2019: Will Graylin meeting with Daniela Castillo and Yannis Tsampalis

ii. December 13, 2019: email from Will Graylin to Daniela Castillo and Yannis Tsampalis (Subject: RE: connecting Mastercard)

jj. February 1, 2020: Email from Yannis Tsampalis attaching three documents (Subject: Follow-Up – process & documentation for OV Loop)

kk. February 14, 2020: email from Will Graylin to Sherri Haymond attaching presentation (Subject: OV Loop update and Investment)

ll. February 24, 2020: email from Sherri Haymond to Will Graylin (Subject: Will<>Sherri – OV Loop update and Investment)

mm. February 26, 2020: Will Graylin meeting with Sherri Haymond

nn. February 26, 2020: email from Will Graylin to Sherri Haymond attaching presentation (Subject: Will<>Sherri – OV Loop update and Investment)

oo. March 4, 2020: email from Will Graylin to Yannis Tsampalis (Subject: Re: follow Up – process & documentation for OV Loop)

pp. March 5, 2020: email from Yannis Tsampalis to Will Graylin (Subject: Re: Follow Up – process & documentation for OV Loop)

qq. March 6, 2020: email from Doug Yeager to Yannis Tsampalis attaching zip file (Subject: DAC paperwork)

rr. March 6, 2020: email from Will Graylin to Yannis Tsampalis (Subject: RE: Follow Up – process & documentation for OV Loop)

ss. June 24, 2020: email from Will Graylin to Rich Clow, Hans Reisgies, Joan Ziegler, Kevin Kozak, Tom Fifelski, and Sherri Haymond (Subject: RE: BofA, OV Loop & Sequent for MDES)

tt. June 25, 2020: email from Rich Clow to Will Graylin, Hans Reisgies, Joan Ziegler, Kevin Kozak, Tom Fifelski, and Sherri Haymond (Subject: RE: BofA, OV Loop & Sequent for MDES)

uu. June 25, 2020: Will Graylin meeting with Chris Kangas

vv. June 25, 2020: email from Chris Kangas to Will Graylin (Subject: hi)

ww. June 25, 2020: email from Will Graylin to Chris Kangas (Subject: RE: hi)

xx. June 29, 2020: email from Will Graylin to Chris Kangas and Sherri Haymond (Subject RE: hi)

yy. June 29, 2020: email from Tom Fifelski to Chris Kangas and Sherri Haymond (Subject: Re: hi)

zz. June 29, 2020: email from Chris Kangas to Tom Fifelski and Sherri Haymond (Subject: RE: hi)

aaa. July 2, 2020: email from Will Graylin to Chris Kangas, Tom Fifelski, Joan Ziegler, Sherri Haymond, Richard Nassar, and Kevin Kozak (Subject: RE: hi)

bbb. July 29, 2020: email from Will Graylin to Sherri Haymond and Chris Kangas (Subject: RE: BofA, OV Loop & Sequent for MDES)

ccc. August 11, 2020: email from Tom Fifelski to Charl Botes and Chris Kangas (Subject: OV/Mastercard project status)

ddd. August 25, 2020: email from Tom Fifelski to Chris Kangas (Subject: Re: OV/Mastercard project status)

eee. August 25, 2020: email form Will Graylin to Tom Fifelski and Chris Kangas (Subject: RE: OV/Mastercard project status)

fff. September 3, 2020: email from Will Graylin to Tom Fifelski, Chris Kangas, and Charl Botes (Subject: RE: OV/Mastercard project status)

ggg. September 7, 2020: email from Will Graylin to Sherri Haymond (Subject: FW: OV/Mastercard project status)

hhh. September 21, 2020: email from Will Graylin to Chris Kangas, Charl Botes,

and Sherri Haymond (Subject: RE: OV/Mastercard project status)

iii. April 25, 2021: email from Will Graylin to Sherri Haymond (Subject: OV Loop & BofA POC on MDES)

jjj. April 25, 2021: email from Sherri Haymond to Will Graylin (Subject: Re: OV Loop & BofA POC on MDES)

kkk. April 25, 2021: email from Will Graylin to Sherri Haymond (Subject: RE: OV Loop & BofA POC on MDES)

lll. June 15, 2021: email from Will Graylin to Sherri Haymond (Subject: RE: OV Loop & BofA POC on MDES)

mmm. June 23, 2021: email from Will Graylin to Sherri Haymond (Subject: RE: OV Loop & BofA PCO on MDES)

nnn. July 22, 2021: email from Donald Chapman to Thyda Chhuan (Subject: Fwd: OV Loop & BofA POC on MDES)

ooo. July 29, 2021: email from Thyda Chhuan to Donald Chapman (Subject: RE: Fwd: OV Loop & BofA POC on MDES)

ppp. July 29, 2021: email from Donald Chapman to Thyda Chhuan (Subject: Re: Fwd: OV Loop & BofA POC on MDES - question)

qqq. August 3, 2021: email from Will Graylin to Donald Chapman and Thyda Chhuan (Subject: Re: Fwd: OV Loop & BofA POC on MDES – question)

rrr. January 12, 2022: email from Donald Chapman to Kimberly Peyton, Kevin Kozak, J. Chiu, Will Graylin, John Ayers, and Luis Silva (Subject: OV Loop demo for MA MDES)

sss. January 18, 2022: email from Kimberly Peyton to Donald Chapman, Kevin Kozak, J. Chiu, Will Graylin, John Ayers, and Luis Silva (Subject: RE: OV Loop demo for MA MDES)

ttt. January 24, 2022: email from Donald Chapman to Kimberly Peyton (Subject: Re: OV Loop demo for MA MDES)

uuu. February 10, 2022: email from Donald Chapman to Kimberly Peyton (Subject: Re: OV Loop demo for MA MDES)

vvv. February 23, 2022: email from Donald Chapman to Kimberly Peyton (Subject: Re: OV Loop demo for MA MDES)

www. February 23, 2022: email from Kimberly Peyton to Donald Chapman and Luis Silva (Subject: Re: OV Loop demo for MA MDES)

71. Over the past three years, Mastercard has expressed great enthusiasm and support for OV Loop and its Valet. Despite this professed enthusiasm, Mastercard made no progress in approving OV Loop or the Valet. Over the years, Mastercard said the right things, but **did** nothing. On information and belief, this was deliberate but disguised obstructionism, given Mastercard's disintermediation concerns.

Mastercard Anti-Competitive Hampering of MCBP Access For OV Loop Digital Wallet

72. Mr. Graylin spent three years trying to get traction with Mastercard and various big banks to secure the ability to load their cards on the OV Valet. They have never said no, but nothing ever happened. Mastercard continued to ask OV Loop to provide more information, and OV Loop did so, but Mastercard never moved OV Loop towards solutions approval and certification to authorize OV Loop to load their tokens into OV Loop's wallet.

73. OV Loop has not been able to get MCBP certification and thus cannot deliver tokens for Mastercard branded payment cards to its end users, thus drastically limiting its ability to earn revenue and gain traction as a mobile wallet solution. The approval process and certification delays have already caused an estimated two and a half years of delay to market and tens of millions in lost revenue along with significant loss in market capitalization.

V. NOTICE OF THE PATENT-IN-SUIT AND MASTERCARDS' KNOWLEDGE OF ITS INFRINGEMENT

74. OV Loop told Mastercard, both in conversations and in writing, that OV Loop invented HCE and owned the '171 Patent. OV Loop identified the named inventor, Doug Yeager, by name. And OV Loop told Mastercard that Mastercard's cloud-based HCE approach infringed. Mastercard was fully on notice of the '171 Patent and its claims, both actually and constructively, and knew (or at the very least should have known) that it infringed.

VI. CLAIM: INFRINGEMENT OF U.S. PATENT NO. 10,032,171

75. OV Loop realleges and incorporates by reference all of the allegations set forth in the preceding paragraphs.

76. Mastercard infringes claims of the ’171 Patent.

a. Direct Infringement

77. Mastercard directly infringes, literally and/or under the doctrine of equivalents, claims of the ’171 Patent. Mastercard, without authority, makes, uses, imports, offers to sell, and/or sells (in/into the United States) instrumentalities that practice inventions covered by claims of the ’171 Patent. Any HCE mobile wallet system or method that complies with Mastercard’s Mastercard Cloud-Based Payments specifications (“MCBP Instrumentalities”) meet all of the elements of claims of the ’171 Patent, including HCE mobile wallet systems or methods that include Mastercard’s Mastercard Digital Enablement Service (“MDES Instrumentalities”). For example, Mastercard uses systems covered by claims of the ’171 Patent by putting MCBP Instrumentalities and MDES Instrumentalities into service, i.e., it controls (directly and/or indirectly), and benefits from, each MCBP Instrumentality and MDES Instrumentality. Mastercard also practices methods covered by claims of the ’171 Patent, solely and/or jointly, by, for example, conditioning third-party (including third-party mobile wallet application providers) participation in, or the receipt of a benefit from, MCBP Instrumentalities and/or MDES Instrumentalities, on the performance of steps covered by the ’171 Patent’s method claims, and establishing the manner or timing of the third-party’s performance, while performing the remaining steps of those method claims itself, through at least its Mastercard Digital Enablement Service (“MDES”).

78. Mastercard’s direct infringement is further exemplified by its making of systems covered by claims of the ’171 Patent. For instance, Mastercard makes a system that meets each

element of Claim 25 of the ’171 Patent. Claim 25 is a system claim and it depends on Claim 17. *See* Exhibit A, Claim 25 (“The system of claim 17”). Claim 25 adds the following element to the system claimed by Claim 17: “further comprising the remote computer system, the remote computer system configured to generate non-permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network.” *Id*. At least MDES includes a Mastercard instrumentality that includes the described “remote system.” Mastercard configures this remote system “to generate non-permanent cryptographic keys associated with the account and send each of the non-permanent cryptographic keys and the account identifier to the mobile device over the wireless network.” This configuration is not complete until the claimed system’s remote system is associated with the account, i.e., the end-user’s payment account. Put differently, the system claimed by Claim 25 is not complete until the “mobile device” with “application” claimed by Claim 17 is connected to the “remote system” described in Claim 25, and this connection is not complete until the remote system is associated with the end-user’s payment account. This remote system-payment account association is the final piece in the assembly of the system claimed by Claim 25. Mastercard is the person who adds this component to the other system components, and so completes the claimed system, i.e., Mastercard makes the system claimed by Claim 25 and so directly infringes at least Claim 25 of the ’171 Patent. Mastercard’s direct infringement of Claim 25 is further illustrated below, using a system that comprises features of MDES and a mobile wallet application provided by a third-party (the Garmin Pay application).

79. Garmin Ltd. (and/or its affiliates) (“Garmin”) manufacture mobile devices (smartwatches) with a mobile wallet application. Garmin calls its mobile wallet Garmin Pay.

For the United States market, Garmin Pay works with hundreds of Mastercard branded payment cards, including Bank of America and Capital One issued cards. *See* https://www.garmin.com/en-US/garminpay/banks/; *see also* https://www.mastercard.us/en-us/personal/ways-to-pay/connected-commerce.html ("The benefits of paying with your favorite credit or debit card, without reaching into your pockets. Use … Garmin Pay™ to make secure payments at thousands of locations with a quick flick of the wrist") (with link to https://explore.garmin.com/en-US/garmin-pay/); https://www.us.hsbc.com/credit-cards/mobile-payments/garmin-pay/ ("Use your HSBC Mastercard® with Garmin Pay™").

80. Garmin Pay, and Garmin Pay transactions that use a Mastercard branded card, comply with Mastercard's Mastercard Cloud-Based Payments ("MCBP") specifications. Garmin Pay and Garmin Pay-Mastercard card transactions are not only MCBP specification compliant, but reliant on MDES, where MDES provides Garmin Pay with non-permanent cryptographic keys and tokenized PANs ("account identifiers") for Mastercard branded cards added to an end-user's Garmin smartwatch, and validates cryptograms for Garmin Pay end-user payments that use Mastercard branded cards. *See* https://newsroom.mastercard.com/press-releases/mastercard-enables-garmin-users-to-run-and-shop-at-a-perfect-pace/ ("Simplicity and security are at the core of the Garmin Pay capability. By using Mastercard's industry-leading token service …."); *compare* https://newsroom.mastercard.com/press-releases/mastercard-partners-with-fit-pay-to-accelerate-the-development-of-payments-enabled-devices-and-wearables/ ("By integrating the Fit Pay platform with the MasterCard Digital Enablement Service (MDES), the companies will work with Wearatec and other innovative manufacturers to bring to Mastercard cardholders a variety of secure contactless payments-enabled devices") *with* https://www.theverge.com/2017/8/31/16215714/garmin-payment-service-ifa-2017 ("Garmin Pay

is actually enabled by FitPay") (Garmin went onto acquire FitPay).

81. In order for MDES to provide Garmin devices with non-permanent cryptographic keys and tokenized PANs, and validate cryptograms for Garmin Pay transactions, the Garmin Pay end-user's payment account that corresponds to his or her Mastercard branded payment card must be associated with MDES. Mastercard software on Mastercard servers makes this association. In this way, Mastercard makes a system that infringes at least Claim 25 of the '171 Patent. The system comprises: (1) "a mobile device" in the form of an end-user's Garmin smartwatch; (2) "an application" in the form of the Garmin Pay application on the end-user's Garmin smartwatch; and (3) a "remote system" in the form of MDES features, where the Garmin smartwatch has the components described in Claim 17, the Garmin Pay application is executable as described in Claim 17, and the MDES features are configured as described in Claim 25. It is Mastercard that completes the assembly of this system, thereby making the system and infringing Claim 25 of the '171 Patent, when it associates the MDES features with a Garmin Pay end-user's payment account. Mastercard has been, is currently, and continues to, directly infringing at least Claim 25 of the '171 Patent in violation of 35 U.S.C. § 271(a), literally or under the doctrine of equivalents.

b. <u>Indirect Infringement</u>

82. Also, Mastercard has been, is currently, and continues to, indirectly infringe, by inducement and/or contributory infringement, claims of the '171 Patent under 35 U.S.C. § 271(b-c).

83. Mastercard actively induces infringement of claims of the '171 Patent under 35 U.S.C. § 271(b). For example, third-parties that make, use, sell, and/or offer to sell mobile wallets within the United States that are MCBP specification compliant directly infringe '171

Patent claims. Mastercard, through activity in the United States, actively induces and aids and abets the infringing acts of these third-parties. For example, Mastercard provides HCE mobile wallet specifications in the form of its MCBP specifications and requires any mobile wallet that works with Mastercard branded cards to comply with its MCBP specifications. Further, Mastercard requires any mobile wallet that works with Mastercard branded cards to be certified by it and provides this certification to the third-parties. More, Mastercard provides cloud-based non-permanent cryptographic key and tokenized PAN generation, and cryptogram validation, technology for third-party HCE mobile wallet applications in the form of MDES, and provides a HCE mobile wallet application software development kit to third-parties, its MCBP Mobile Payment SDK. Further still, Mastercard actively promotes the development of HCE mobile wallets by third-parties and third-party use of such wallets (including the use of such wallets by consumers/end-users). Mastercard does all of this with the specific and actual intent to cause the third-party infringing acts, with notice of the ’171 Patent and knowing that the third-party acts it encourages infringe.

84. Mastercard is liable for contributory infringement under 5 U.S.C. § 271(c). Mastercard offers to sell and/or sells within the United States, and/or imports into the United States, a component(s) of a system, or a system component(s) for use in a process, that constitute a material part of inventions claimed by ’171 Patent claims. Mastercard does this knowing the same to be especially made or especially adapted for use in infringing claims of the ’171 Patent, and not a staple article or commodity of commerce suitable for substantially non-infringing use. For example, Mastercard supplies third-parties with cloud-based non-permanent cryptographic key and tokenized PAN generation, and cryptogram validation, technology for HCE mobile wallet applications in the form of MDES, and provides third-parties with an HCE mobile wallet

application software development kit, its MCBP Mobile Payment SDK, both of which have no substantial non-infringing uses.

c. Willful Infringement

85. Mastercard's infringement of the '171 Patent is willful and deliberate entitling OV Loop to increased damages under 35 U.S.C. § 284 and to attorneys' fees and costs incurred in prosecuting this action pursuant to 35 U.S.C. § 285.

86. Mastercard had pre-suit notice of the '171 Patent and pre-suit knowledge of its infringement. An OV Loop representative specifically identified the '171 Patent to Mastercard and informed Mastercard that its HCE cloud-based tokenization implementation infringed. Mastercard, nonetheless, continued to, and continues to, commit the aforementioned infringing acts. More, Mastercard was again provided notice of the '171 Patent and its infringement of the Patent-in-Suit by this complaint.

87. Mastercard has infringed and continues to infringe the '171 Patent despite the fact that it knew that its conduct amounted to infringement of the '171 Patent. Mastercard has engaged in egregious conduct, including its willful infringement.

d. Harm

88. As a result of Mastercard's infringement, OV Loop has been damaged, and will continue to be damaged, until Mastercard is enjoined from further acts of infringement.

89. Mastercard will continue to infringe unless enjoined by this Court. OV Loop faces real, substantial and irreparable damage and injury of a continuing nature from infringement for which OV Loop has no adequate remedy at law.

VII. PRAYER FOR RELIEF

WHEREFORE, OV Loop demands judgment in its favor and against Mastercard and

relief as follows:

90. Judgment in OV Loop's favor and against Mastercard on all causes of action alleged herein;

91. A judgment that the '171 Patent is valid and enforceable;

92. A judgment that Mastercard has infringed (directly and/or indirectly) one or more Claims of the Patent-in-Suit;

93. A judgment that Mastercard's infringement of the Patent-in-Suit was willful and/or otherwise egregious and exceptional;

94. An accounting for and payment to OV Loop of all damages caused by the infringement of the Patent-in-Suit, which by statute can be no less than a reasonable royalty, including an accounting of all infringing sales and damages not presented at trial, and an award of damages pursuant to 35 U.S.C. § 284 sufficient to compensate OV Loop for Mastercard's past infringement and any continuing or future infringement up until the date that Mastercard is finally and permanently enjoined from further infringement, including compensatory damages;

95. A judgment that the damages to OV Loop with respect to the Patent-in-Suit be increased three times the amount found or assessed pursuant to 35 U.S.C. § 284 and that Mastercard account for and pay to OV Loop the increased amounts;

96. That this be adjudicated an exceptional case and OV Loop be awarded its attorneys' fees in this action pursuant to 35 U.S.C. § 285;

97. That this Court issue preliminary and final injunctions enjoining Mastercard, its officers, directors, agents, servants, employees, attorneys, affiliates, divisions, branches, subsidiaries, parents, and those persons in active concert or participation with any of them, and any other person in active concert or participation with them, from continuing the acts herein

complained of with respect to the infringement of the Patent-in-Suit, and more particularly, that Mastercard and such other persons be permanently enjoined and restrained from further infringing the Patent-in-Suit;

98. That OV Loop be granted pre-judgment and post-judgment interest on the damages caused to it by reason of Mastercard's conduct at the maximum legal rates provided by statute or law;

99. That this Court award OV Loop its costs and disbursements in this civil action, including reasonable attorneys' fees; and

100. That OV Loop be granted such other relief as this Court may deem just and proper under the circumstances.

VIII. DEMAND FOR JURY

Under Rule 38(b) of the Federal Rules of Civil Procedure, OV Loop respectfully requests a trial by jury on all causes of action, claims, or issues so triable.

Dated: March 1, 2023

Respectfully submitted,

By: _____

Spencer Hosie (CA Bar No. 101777)
Diane S. Rice (CA Bar No. 118303)
Darrell R. Atkinson (CA Bar No. 280564)
(Pro hac vice Applications pending)
HOSIE RICE LLP
505 Sansome Street, Suite 1575
San Francisco, CA 94111
Tel: (415) 247-6000
Fax: (415) 247-6001

Attorneys for Plaintiff OV LOOP, INC.