

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA
MIAMI DIVISION**

CASE NO. 1:24-cv-20455

LIBERTY PEAK VENTURES, LLC,

Plaintiff,

v.

JURY TRIAL DEMANDED

MASTERCARD INCORPORATED AND
MASTERCARD INTERNATIONAL
INCORPORATED,

Defendants.

PLAINTIFF’S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Liberty Peak Ventures, LLC files this Complaint in this Southern District of Florida (the “District”) against Defendants Mastercard Incorporated and Mastercard International Incorporated (collectively, “Defendants” or “Mastercard”) for infringement of U.S. Patent Nos. 8,851,369 (the “’369 patent”), 8,814,039 (the “’039 patent”), 8,794,509 (the “’509 patent”), 7,953,671 (the “’671 patent”), 9,195,985 (the “’985 patent”), 7,587,756 (the “’756 patent”), 7,668,750 (the “’750 patent”), 8,584,938 (the “’938 patent”), 7,431,207 (the “’207 patent”), and 6,886,101 (the “’101 patent”), which are collectively referred to as the “Asserted Patents.”

THE PARTIES

1. Plaintiff Liberty Peak Ventures, LLC (“LPV” or “Plaintiff”) is a Texas limited liability company located at 812 W. McDermott Drive #1066, Allen, Texas 75013.

2. On information and belief, Defendant Mastercard Incorporated (“MINC”) is a corporation organized under the laws of the state of Delaware, with its principal place of business located at 2000 Purchase Street, Purchase, New York 10577, United States. MINC may be served with process via its registered agents, including at least The Corporation Trust Company,

Corporation Trust Center, 1209 Orange St., Wilmington, Delaware 19801, United States, and/or via MINC's corporate officers. MINC is a publicly traded company on the New York Stock Exchange under the symbol "MA."

3. On information and belief, Defendant Mastercard International Incorporated ("MINT") is a corporation organized under the laws of the state of Delaware, with its principal place of business located at 2000 Purchase Street, Purchase, New York 10577, United States, and having at least one office located in this District, for example, at 801 Brickell Avenue, Suite 1200 and/or 1300, Miami, Florida 33131, United States. MINT may be served with process via its registered agents, including at least C T Corporation System, 1200 South Pine Island Road, Plantation, Florida 33324, United States and/or MINT's corporate officers. MINT is a wholly owned subsidiary of Defendant Mastercard Incorporated.

4. MINC and MINT are collectively referred to as Mastercard in this complaint. According to Mastercard's annual report for the fiscal year ending December 31, 2022, "In this Report on Form 10-K ("Report"), references to the "Company," "Mastercard," "we," "us" or "our" refer to the business conducted by Mastercard Incorporated and its consolidated subsidiaries, including our operating subsidiary, Mastercard International Incorporated, and to the Mastercard brand." *See Annual Report for the Fiscal Year Ended December 31, 2022*, MASTERCARD INCORPORATED, p. 4, available at https://s25.q4cdn.com/479285134/files/doc_financials/2022/AR/MA.12.31.2022-10-K-as-filed.pdf (last accessed Jan. 12, 2024) [hereinafter "2022 Annual Report"].

5. The term "Mastercard Cards" is used herein to refer collectively to all payment, banking, credit, debit and/or prepaid cards and transaction devices, including without limitation proximity integrated chip (PIC) transaction devices, that are Mastercard-branded; offered by

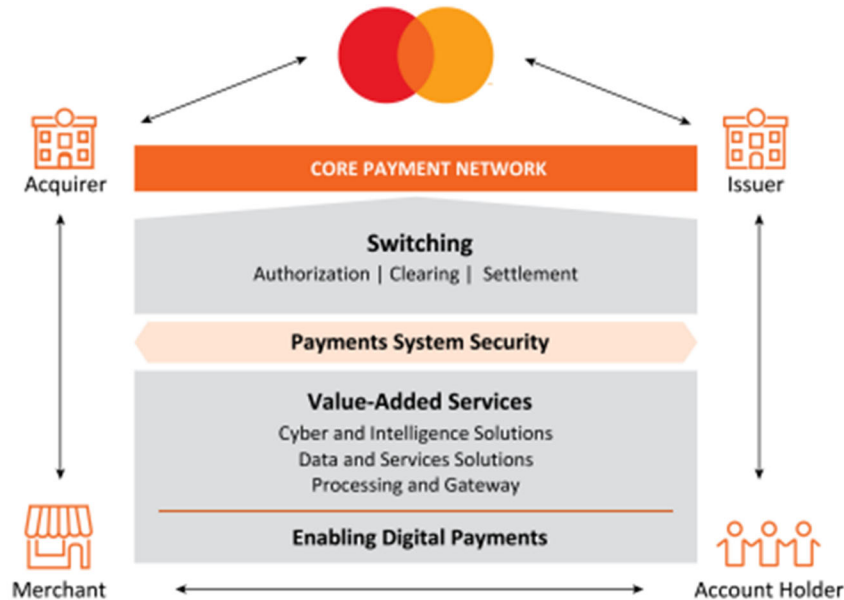
Mastercard; serviced by Mastercard; subject to a license from Mastercard; provisioned by Mastercard; provided by Mastercard; issued by Mastercard or a third-party subject to terms of use required by Mastercard; procured, supplied or made by Mastercard; and/or include the name “Mastercard” on the cards or in advertising for the cards.

6. The term “Mastercard Transaction Instruments” is used herein to refer collectively to Mastercard Cards and transaction instruments that are made, sold, provided, licensed and/or issued by Mastercard, including for example, on behalf of or via direction and control of third parties; related products, methods, and/or services for card payments using a physical banking, payment, credit, debit, or prepaid card having an embedded chip or smartcard, and systems operative to implement such methods and/or services; mobile payment systems (e.g., mobile wallets) and methods using Mastercard Cards and/or transaction instruments to conduct transactions over the internet and/or mobile devices, including, for example, smart phones, tablets, and computers; and products, systems and methods provisioned, directly or indirectly, by Defendants with tokens that can be used in the place of or in combination with primary account numbers to conduct transactions.

7. According to the 2020 Annual Report, “Mastercard is a technology company in the global payments industry” and “connect[s] consumers, financial institutions, merchants, governments, digital partners, businesses and other organizations worldwide by enabling electronic payments instead of cash and checks and making those payment transactions safe, simple, smart and accessible.” *Id.* at 6. Mastercard states that it “make[s] payments easier and more efficient by providing a wide range of payment solutions and services using our family of well-known and trusted brands, including Mastercard®, Maestro® and Cirrus®.” *Id.* Additionally, Mastercard states that it “operate[s] a multi-rail payments network that provides choice and flexibility for consumers,

merchants and our customers.” *Id.* Mastercard uses its “proprietary core global payments network, [to] switch (authorize, clear and settle) payment transactions” and “sets the standards and ground-rules for [its] core global payments network [to] balance value and risk across all stakeholders and allow[] for interoperability among them.” *Id.*

8. Mastercard states that it “enable[s] a wide variety of payment capabilities (including integrated products and value-added services and solutions) over [its] multi-rail network among account holders, merchants, financial institutions, businesses, governments and others, offering [its] customers one partner for their payment needs.” *Id.* at 10. Mastercard’s “core payment network links issuers and acquirers around the globe to facilitate the switching of transactions, permitting account holders to use a Mastercard product at tens of millions of acceptance locations worldwide.” *Id.* Mastercard further states that its “core payment network supports what is often referred to as a ‘four-party’ payments network and includes the following participants: account holder (a person or entity who holds a card or uses another device enabled for payment), issuer (the account holder’s financial institution), merchant and acquirer (the merchant’s financial institution).” *Id.* Mastercard’s 2022 Annual report includes the following graphic depicting “a typical transaction on [Mastercard’s] core payment network and [Mastercard’s] role in that transaction, which includes payment security, value-added services and the enablement of digital payments.”



Id.

9. As a part of Mastercard’s “multi-layered approach to protect the global payments ecosystem, [Mastercard] work[s] with issuers, acquirers, merchants, governments and payments industry associations to develop and put in place technical standards (such as EMV standards for chips and smart payment cards) for safe and secure transactions and [Mastercard] provide[s] solutions and products that are designed to ensure safety and security for the global payments ecosystem.” *Id.*

10. Mastercard states that it provides products and services that include “open banking solutions” and Mastercard’s “core payment network.” *Id.* at 8, 10. Mastercard’s products and services further include point-of-sale (“POS”) products such as “commercial credit, debit and prepaid payment products and solutions that meet the payment needs of large corporations, midsize companies, small businesses and government entities.” *Id.* at 13. Mastercard’s payment-related services and products include “digital payment services,” “products that make it easier for merchants to accept payments and expand their customer base,” and “contactless payment solutions.” *Id.* at 14. Mastercard also provides “issuer solutions designed to provide customers with a complete processing solution to help them create differentiated products and services and allow

quick deployment of payments portfolios across banking channels.” *Id.* at 16. Additionally, Mastercard provides gateway-related services and products, including “[p]ayment gateways that offer a single interface to provide e-commerce merchants with the ability to process secure online and in-app payments;” and “[m]obile gateways that facilitate transaction routing and processing for mobile-initiated transactions” *Id.* at 16.

11. Mastercard states that it “is headquartered in the United States,” and indicates that as of December 31, 2022, approximately 34% of Mastercard’s 29,900 global employees were employed in the United States. *Id.* at 17. Further, Mastercard indicates that during 2022, approximately 33% of Mastercard’s US \$22.237 billion in global net revenue was generated from activity inside the United States. *Id.* 37-38, 47; *see also id.* at 103. Mastercard’s global net revenue from payments was approximately US \$14,358. *Id.* at 54.

12. “Mastercard has concluded it has one reportable operating segment, ‘Payment Solutions.’ *Id.* at 113. “Mastercard’s Chief Executive Officer has been identified as the chief operating decision-maker.” *Id.* “All of the Company’s activities are interrelated, and each activity is dependent upon and supportive of the other.” *Id.* Accordingly, all significant operating decisions are based upon analysis of Mastercard at the consolidated level. *Id.*

13. EMV specifications are developed and managed by EMVCo, which “is a global technical body that facilitates worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV Specifications and related testing processes.” *See Overview of EMVCo*, EMVCo, <https://www.emvco.com/about-us/overview-of-emvco/> (last visited Jan. 16, 2024). EMVCo “enable[s] the development and management of specifications to address the challenge of creating global interoperability amongst different countries and to deliver the adoption of secure technology to combat card fraud, while enabling innovation in the payments

industry.” *Id.* Importantly, Mastercard co-owns EMVCo, along with five other member organizations, who each serve on EMVCo’s Board of Managers. *See id.*

14. On information and belief, Mastercard utilizes, induces, and/or requires its partners, issuers, acquirers, merchants, customers and/or clients to utilize EMV processes documented in the EMV specifications during any transaction in connection with Mastercard products, methods, and/or services, for example, transactions using an account for any of the Mastercard Cards, including without limitation contactless payments using a physical card or mobile device.

15. Mastercard utilizes, induces, and/or requires partners, issuers, acquirers, merchants, customers and/or clients to utilize EMV specifications specifically directed to the tokenization process at least, for example, for EMV compliant mobile wallets. Mastercard additionally utilizes, induces, and/or requires partners, issuers, acquirers, merchants, customers and/or clients to utilize EMV specifications to make use of EMV 3D Secure Authentication.




16. The Asserted Patents cover Mastercard’s products, methods and/or services related to offering, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from accounts, transactions and payments, for example, via Mastercard developer accounts, Mastercard Cards and associated accounts, which products, methods and/or services are designed, developed, manufactured, distributed, sold, offered for sale, and/or used by Defendants and/or their customers, licensees, partners, issuers, acquirers, merchants, consumers, and/or clients.

17. On information and belief, Defendants, on their own and/or via alter egos, agents, subsidiaries, partners, and affiliates, maintain a corporate and commercial presence in the United States, including in Florida and this District, via at least their 1) physical offices in Florida, including this District; 2) Mastercard’s online presence (e.g., Mastercard.com and/or Mastercard.us) that

provides Mastercard's clients and consumers with access to and/or markets Mastercard's products, methods, and/or services, including those identified as infringing herein; and 3) consumers and clients of Mastercard who utilize, for example, Mastercard Cards and associated products, methods and/or services, at the point of sale, including via contactless payment methods, in numerous merchant physical and online sites, e.g., retail stores, restaurants, and other service providers accepting Mastercard Cards. As can be seen below, Mastercard provides services on a global scale for individuals, consumers, financial institutions, governments, and businesses.

Unlocking potential

We reshape the digital economy so everyone — individuals, financial institutions, governments and businesses — can realize their ambitions.



OUR TECHNOLOGY

Innovation – then, now, always

For more than 50 years, Mastercard has pioneered technology to make payments simpler, smarter and safer.

See what's next →

A FORCE FOR GOOD

Investing in what matters

We believe in committing our time, energy and passion to supporting local projects and addressing global challenges.

See how we give back →

CONNECTION IS PRICELESS

Connecting everyone to Priceless possibilities

By connecting individuals, businesses and organizations in more than **210 countries** and territories today, we're unlocking opportunity for more people in more places for generations to come.

Who we serve?



Consumers
Learn more →



Small &
medium
businesses
Learn more →



Government
& public
sector
Learn more →



Large
enterprises
Learn more →



Banks &
credit
unions
Learn more →



Our purpose

We work to connect and power an inclusive digital economy that benefits everyone, everywhere by making transactions safe, simple, smart and accessible. Using secure data and networks, partnerships and passion, our innovations and solution help individuals, financial institutions governments and businesses realize their greatest potential. Our decency quotient, or DQ, drives our culture an everything we do inside and outside of our company.

See About Mastercard, MASTERCARD, <https://www.mastercard.com/global/en/vision/who-we-are.html> (last visited Jan. 17, 2024).



CONTACTLESS

Tap & Go® Payments

A faster, safer way to make everyday purchases with your contactless-enabled card or device. It's like having exact change wherever you go, but even more convenient than cash.

Get started →

Tap on your device



SAMSUNG Pay

More about safety and security

Whether paying online, in-store, via mobile or a wearable, Mastercard provides valuable security benefits to help keep you protected.

Learn more →

Apple Pay

Apple Pay is an easy, secure and private way to pay – in-store, online and even in your favorite apps with your card on your iPhone, Apple Watch, iPad and Mac.

Google Pay

Enjoy convenient and secure checkout with your phone everywhere Google Pay and contactless payments are accepted. Just Tap & Go, knowing that your payments are safely encrypted before, during and after every purchase.

Samsung Pay

Samsung Pay offers a simple and secure way to pay for secure mobile payments with your compatible Samsung devices.

See Contactless Payments, MASTERCARD, <https://www.mastercard.us/en-us/personal/ways-to-pay/contactless.html> (last visited Jan. 17, 2024).

18. Such services associated with Mastercard Transaction Instruments (e.g., Mastercard Cards) include systems and methods for processing digital transactions via online transactions and mobile payment solutions. *See, e.g., 2022 Annual Report, pp. 9, 16.* Defendants, on their own and/or via related entities, their parent, alter egos, agents, subsidiaries, partners and/or affiliates, maintain at least one office in this District, for example, located at 801 Brickell Avenue, Suite 1200 and/or 1300, Miami, Florida 33131, United States. On information and belief, this office is a location where Defendants, on their own and/or via related entities, their parent, alter egos, agents,

subsidiaries, partners and/or affiliates, maintain employees, including, for example, employees who develop and/or provide Mastercard’s payment products, methods, and/or services, which include without limitation systems used for payment via Mastercard Cards and/or other products, methods, and/or services that infringe the Asserted Patents. *See, e.g., Global Locations*, MASTERCARD, <https://www.mastercard.us/en-us/vision/who-we-are/global-locations.html> (last visited Jan. 17, 2024) (showing a “Regional Headquarters” located in Miami, Florida); *Search Jobs at Mastercard*, MASTERCARD, <https://careers.mastercard.com/us/en/search-results?qcity=Miami&qstate=Florida&qcountry=United%20States%20of%20America> (last visited Jan. 17, 2024) (showing 9 Mastercard jobs available in Miami, Florida); *Humberto G. Fleites*, LINKEDIN, <https://www.linkedin.com/in/humberto-g-fleites-3313b828> (last visited Jan. 18, 2024) (showing an “Humberto G. Fleites” profile that lists job titles including “Director, Product Management, C&I” and “Director, Product Development and Innovation, LFI” at Mastercard, showing a total of “7 years 6 months” at Mastercard, listing locations that include “Miami, Florida, United States,” and describing experience in the “Miami/Fort Lauderdale Area” of Florida that includes being “Global business owner for the 8-digit BIN initiative” transitioning from a 6-digit to 8-digit BIN, “[r]esponsible for all BIN management & efficiency activities across Mastercard,” and working “to ensure all Mastercard products and services are ready for 8-digit BIN,” said BIN being the first part of the primary account number (PAN) that appears on a payment card and identifies the card issuer). Additionally, Mastercard provides, enables, and/or induces the use of tap-and-go contactless payments for public transit in Miami, Florida. *Mastercard Gets Miami Commuters Tapping on Public Transit*, MASTERCARD, <https://www.mastercard.com/news/press/2019/august/mastercard-gets-miami-commuters-tapping->

on-public-transit/ (last visited Jan. 17, 2024). Accordingly, Defendants do business, including committing infringing acts, in the U.S., the state of Florida, and in this District.

JURISDICTION AND VENUE

19. This action arises under the patent laws of the United States, namely 35 U.S.C. §§ 271, 281, and 284-285, among others.

20. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

A. Defendant MINC

21. On information and belief, Defendant MINC is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Florida Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Florida and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Florida residents and residents of this District vicariously through and/or in concert with its related entities, alter egos, intermediaries, agents, distributors, partners, subsidiaries, clients, customers, affiliates, and/or consumers.

22. For example, MINC owns and/or controls multiple subsidiaries and affiliates, and at least one, including, but not limited to, Defendant MINT, has a significant business presence in the U.S. and in Florida. MINC, via its own activities and via at least wholly owned subsidiary MINT, has at least one office in Miami, Florida, in this District, at 801 Brickell Avenue, Suite 1200 and/or 1300, Miami, Florida 33131, United States. *See Global Locations*, MASTERCARD,

<https://www.mastercard.us/en-us/vision/who-we-are/global-locations.html> (last visited Jan. 17, 2024) (showing a “Regional Headquarters” located in Miami, Florida); *Search Jobs at Mastercard*, MASTERCARD, <https://careers.mastercard.com/us/en/search-results?qcity=Miami&qstate=Florida&qcountry=United%20States%20of%20America> (last visited Jan. 17, 2024) (showing 9 Mastercard jobs available in Miami, Florida). Miami-Dade Property Appraiser search results show that Defendant MINC’s direct and/or indirect subsidiary Mastercard International LLC, a Delaware limited liability company, is listed as the owner of the property at Mastercard’s office at 801 Brickell Avenue, Suite 1200 and/or 1300, Miami, Florida 33131, United States. *See Tangible Personal Property (TPP) Account Information*, MIAMI-DADE PROPERTY APPRAISER, <https://www.miamidade.gov/Apps/PA/PAOnlineTools/TPPAccountSearch/#/results> (last visited Jan. 17, 2024) (search for “Mastercard” under “Business Name” drop-down menu). On information and belief, Mastercard International LLC is the same as Mastercard International, LLC, a Delaware limited liability company, the name of said Mastercard International, LLC, having been changed to Mastercard Technologies, LLC, a Delaware limited liability company, said Mastercard Technologies, LLC, having managing member Mastercard International Services, Inc., a Delaware corporation, said Mastercard International Services, Inc. being a wholly owned subsidiary of Defendant MINC. On information and belief, MINT is registered to do business in Florida and is 100% owned by Defendant MINC. On information and belief, Mastercard’s at least one office employs numerous residents of the state of Florida and/or this District.

23. Such a corporate and commercial presence in Florida, including in this District, by Defendant MINC furthers the development, design, manufacture, distribution, sale, and use of MINC’s and Mastercard’s infringing products, methods, and/or services, including without

limitation those in connection with Defendants' offering gateway, payment processor, and/or transaction processor products, methods, and/or services; Defendants' tokenization products, methods, and/or services; EMV compliant POS products and services, for example, products, methods, and/or services for securing RFID transactions involving a PIC transaction device and/or mobile wallets using host card emulation; Defendants' provisioning EMV compliant payment applications to mobile wallets on behalf of card issuers; Defendants' providing processing, authorization, clearing and settlement services to its card issuer customers; Defendants' providing card issuance solutions for banks and financial institutions; and/or Defendants' offering, providing, issuing, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing, controlling and/or deriving substantial revenue from financial transactions, including without limitation those associated with Mastercard Transaction Instruments (e.g., Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, acquirers, merchants, partners, developers, customers, consumers, and clients, including Defendants' payment processing, authentication, authorization, validation, and fraud detection products, methods and/or services. Through direction and control of its related entities, alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and/or consumers, MINC has committed acts of direct and/or indirect patent infringement within Florida, this District, and elsewhere in the United States, giving rise to this action and/or has established minimum contacts with Florida such that personal jurisdiction over MINC would not offend traditional notions of fair play and substantial justice.

24. On information and belief, MINC directs and controls and/or otherwise directs and authorizes all activities of its related entities, alter egos, intermediaries, agents, subsidiaries, and

affiliates, including, but not limited to Defendant MINT, Mastercard International LLC, Mastercard International, LLC, Mastercard Technologies, LLC, and/or Mastercard International Services, Inc. *See, e.g.*, 2022 Annual Report, p. 113 (““Mastercard has concluded it has one reportable operating segment, ‘Payment Solutions.’ Mastercard’s Chief Executive Officer has been identified as the chief operating decision-maker. All of the Company’s activities are interrelated, and each activity is dependent upon and supportive of the other. Accordingly, all significant operating decisions are based upon analysis of Mastercard at the consolidated level.”) Via its own activities and via at least these entities, MINC has substantial business operations in Florida, which include without limitation the provision of products and/or services, for example, payment processing services, to various entities including without limitation partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and/or consumers. MINC has placed and continues to place infringing products and/or services for offering, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from Mastercard developer accounts, commercial transactions via Mastercard Transaction Instruments (e.g., Mastercard Cards) and associated accounts, including without limitation related mobile, contactless, and online payment systems, into the U.S. stream of commerce. MINC has placed such products, methods, and/or services into the stream of commerce with the knowledge and understanding that such products, methods, and/or services are, will be, and continue to be sold, offered for sale, and/or used in this District and the State of Florida. *See Litecubes, LLC v. Northern Light Products, Inc.*, 523 F.3d 1353, 1369-70 (Fed. Cir. 2008) (“[T]he sale [for purposes of § 271] occurred at the location of the buyer.”).

25. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391 and/or 1400(b). As alleged herein, Defendant MINC has committed acts of infringement in this District. As further

alleged herein, Defendant MINC, via its own operations and employees located there and via ratification of Defendant MINT's presence and/or the presence of other subsidiaries as agents and/or alter egos of MINC, has a regular and established place of business, in this District at least at an office located at 801 Brickell Avenue, Suite 1200 and/or 1300, Miami, Florida 33131, United States. Accordingly, MINC may be sued in this district under 28 U.S.C. § 1400(b).

B. Defendant MINT

26. On information and belief, Defendant MINT is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Florida Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Florida and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Florida residents and residents of this District vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. For example, MINT, including as an agent and alter ego of parent company MINC, is has a regular and established place of business at Mastercard's office at 801 Brickell Avenue, Suite 1200 and/or 1300, Miami, Florida 33131, United States. *See Global Locations, MASTERCARD, <https://www.mastercard.us/en-us/vision/who-we-are/global-locations.html> (last visited Jan. 17, 2024) (showing a "Regional Headquarters" located in Miami, Florida).* Miami-Dade Property Appraiser search results show that Defendant MINC's direct and/or indirect subsidiary Mastercard International LLC, a Delaware limited liability company, is listed as the owner of the property at Mastercard's office at 801 Brickell Avenue, Suite 1200 and/or 1300, Miami, Florida 33131, United States. *See Tangible Personal*

Property (TPP) Account Information, MIAMI-DADE PROPERTY APPRAISER, <https://www.miamidade.gov/Apps/PA/PAOnlineTools/TPPAccountSearch/#!/results> (last visited Jan. 17, 2024) (search for “Mastercard” under “Business Name” drop-down menu). The at least one office in Miami, Florida, employs numerous residents of the state of Florida and/or this District that develop and/or provide products, methods, and/or services that include MINC and/or MINT offering, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from services related to Mastercard developer accounts and/or Mastercard Transaction Instruments (e.g., Mastercard Cards) and associated accounts, including without limitation related mobile, contactless, and online payment systems, for Mastercard’s customers, consumers, and clients in Florida and this District. Additionally, on information and belief, Mastercard payment applications are stored on mobile devices, smart phones, tablets and/or computer chips embedded on Mastercard Transaction Instruments (e.g., Mastercard Cards) used in transactions in Florida and in this District. Mastercard payment applications utilize tokenization processes for facilitating transactions, including, for example, payments.

27. On information and belief, MINC and MINT conform to applicable standards (e.g., EMV standards) and/or require any entity that accesses or uses a Mastercard product and/or service, for example, all issuer, acquirer, and/or merchant systems interfacing with MINC and MINT systems, to conform to the applicable standards (e.g., EMV standards) when effecting payment transactions. Through direction and control of its alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and/or consumers, MINT has committed acts of direct and/or indirect patent infringement within Florida, this District, and elsewhere in the United States, giving rise to this

action and/or has established minimum contacts with Florida such that personal jurisdiction over MINC would not offend traditional notions of fair play and substantial justice.

28. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391 and/or 1400(b). Defendant MINT has committed acts of infringement in this District. As further alleged herein, Defendant MINT, via its own operations and employees located there and/or via ratification of its subsidiaries as agents and/or via alter egos of MINT, has a regular and established place of business, in this District at least at an office located at 801 Brickell Avenue, Suite 1200 and/or 1300, Miami, Florida 33131, United States. Accordingly, MINT may be sued in this district under 28 U.S.C. § 1400(b).

29. Upon information and belief, Defendants MINC and MINT each have significant ties to, and presence in, the State of Florida and this District making venue in this District both proper and convenient for this action.

THE ASSERTED PATENTS AND TECHNOLOGY

30. The Asserted Patents cover various aspects of products (e.g., systems, networks, devices, technology, and/or applications), methods (e.g., processes), and services that include: Mastercard Cards; Mastercard Transaction Instruments; Defendants' offering gateway, payment processor, and/or transaction processor products, methods, and/or services (including without limitation Mastercard Identity Check, EMV 3-D Secure and/or card-not-present services for eCommerce websites, hosted payment forms and/or mobile apps); Defendants' tokenization products, methods, and/or services (e.g., Network and/or PCI tokenization services that can replace card numbers with tokens); EMV compliant POS products (e.g., Mastercard Mobile Point-of-Sale (MPOS) solutions that enable mobile devices to accept payments, including, but not limited to, Tap on Phone and Cloud Commerce) and services, for example, products, methods, and/or services for securing RFID transactions involving a PIC transaction device and/or mobile wallets using host

card emulation (e.g., in connection with Google Pay and Samsung Pay mobile wallets); Defendants' provisioning EMV compliant payment applications to mobile wallets on behalf of card issuers; Defendants' providing processing, authorization, clearing and settlement services to its card issuer customers; Defendants' providing card issuance solutions for banks and financial institutions (e.g., licensing EMV contactless cards to financial institutions and/or provisioning EMV compliant payment applications for consumers' cards onto mobile wallets); and Defendants' offering, providing, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing, controlling and/or deriving substantial revenue from accounts (e.g., Mastercard developer accounts), financial transactions, including without limitation those associated with Mastercard Transaction Instruments (e.g., Mastercard Cards), associated accounts, and related products, methods, and/or services for Defendants' licensees, acquirers, merchants, partners, developers, customers, consumers, and clients, including Defendants' payment processing, authentication, authorization, validation, and fraud detection products, methods and/or services (e.g., Mastercard's products used for payment transactions involving Mastercard Cards, Mastercard's account processing and/or registration platform, Mastercard's payment processing solutions, Mastercard's payment processing network and/or Mastercard's payment-related platforms), referred to herein collectively as the "Accused Instrumentalities."

31. The Asserted Patents cover Accused Instrumentalities of Defendants that provide, facilitate, maintain, transact, authenticate, validate, authorize, clear, settle, and/or process financial data, financial transactions, mobile payments, contactless payments, and/or online payments using Mastercard Transaction Instruments (e.g., Mastercard Cards) and related access to Mastercard's payment products, methods, and/or services (e.g., solutions, systems, devices, networks, APIs, software development kits, and/or other product solutions) licensed by Defendants to their

licensees, issuers, acquirers, partners, developers, consumers, customers, and/or clients. Defendants use the Accused Instrumentalities to process financial data and transactions. Additionally, Defendants use the Accused Instrumentalities to issue or to facilitate the issuance and/or registration of accounts (e.g., for Mastercard developers and/or cardholders of Mastercard Cards) by, for, and/or to Defendants' licensees and partners, developers, consumers, customers, and/or clients of Defendants. Developers and/or Cardholders can then use the accounts to access products and/or services, for example, to conduct or facilitate financial transactions (e.g., make purchases via mobile payment, contactless payment, or online payments). Defendants provide their payment solutions (e.g., products, methods, and/or services) to process such payments. Defendants use the Accused Instrumentalities to provision EMV compliant payment applications to mobile wallets on behalf of card issuers. Defendants use the Accused Instrumentalities to provide processing, authorization, clearing and settlement services to their card issuer customers. Defendants use the Accused Instrumentalities to provide card issuance solutions for banks and financial institutions, for example, by licensing EMV contactless cards to financial institutions and provisioning EMV compliant payment applications for consumers' cards onto mobile wallets. Defendants use the Accused Instrumentalities to provide EMV 3-D Secure services for eCommerce websites, hosted payment forms and/or mobile apps. Defendants use the Accused Instrumentalities to provide tokenization products, methods, and/or services, for example, Network and/or PCI tokenization services that can replace card numbers with tokens. At the point of purchase, Defendants use the Accused Instrumentalities to provide EMV compliant POS products, methods, and/or services, for example, Mastercard Mobile Point-of-Sale (MPOS) solutions, Tap on Phone and/or Cloud Commerce, which can be used for securing RFID transactions involving a PIC transaction device and/or mobile wallets using host card emulation in connection with Google Pay and Samsung Pay

mobile wallets. Defendants also use the Accused Instrumentalities to provide digital solutions, including offering mobile wallets for contactless payments to cardholders (directly and/or via Defendants' issuers, licensees, partners, developers, consumers, customers and/or clients) which are installed onto a mobile device of a cardholder. Such mobile wallets include an appropriate smartcard (e.g., Mastercard smartcard), API, and/or app installed on the mobile device (and in some cases, the software is native to the device). Defendants use the Accused Instrumentalities to provide to cardholders (directly and/or via Defendants' issuers, licensees, partners, developers, consumers, customers and/or clients) embedded chip or smartcard technology that is integrated into a physical card, with Defendants' payment application software, API, or firmware installed. In other instances, the Accused Instrumentalities may be utilized in online purchases conducted over a network (e.g., the Internet) and/or when the user of the payment card account or a Mastercard developer is registering, activating, or maintaining an account.

32. On information and belief, Defendants' services in connection with Mastercard Transaction Instruments (e.g., Mastercard Cards) utilize the Europay, Mastercard, and Visa (EMV) standards in processing, securing, and authenticating financial transactions. For example, Defendants provide, or direct and control users and subscribers of its payment services to provide payment applications that use EMV standards to process payments. In some cases, the payment applications reside on a user's mobile device, allowing the user to make payments via accounts for Mastercard Transaction Instruments (e.g., Mastercard Cards) without presenting the physical card at the time of payment (referred to herein as a "mobile payment"). Defendants' mobile payments can be facilitated by using mobile wallet applications such as Google Pay, Samsung Pay, which include software, APIs, or firmware provided by Defendants.



MDES Token Connect

Overview

The MDES Token Connect API provides a set of inbound web requests to allow issuers to securely push Account information to eligible token requestors and create new tokens. Wallets, Merchants, Payment Service Providers are collectively referred to as token requestors. This documentation is a technical specification of the MDES Token Connect API.

MDES Token Connect API provides the following services to issuers:

Service	Description
<code>getEligibleTokenRequestors</code>	Returns the list of token requestors that are enabled for one or more account ranges of the issuer. For each returned token requestor, metadata (such as name, image asset ID, Token Connect capabilities) is also supplied.
<code>getAsset</code>	Returns the logo of a token requestor, in PNG and SVG format.
<code>pushMultipleAccounts</code>	Triggers issuer-initiated digitization of a card or financial account to a target token requestor. The issuer obtains a receipt for their request, as well as the token requestor URI(s) where they should redirect the consumer to complete the provisioning.

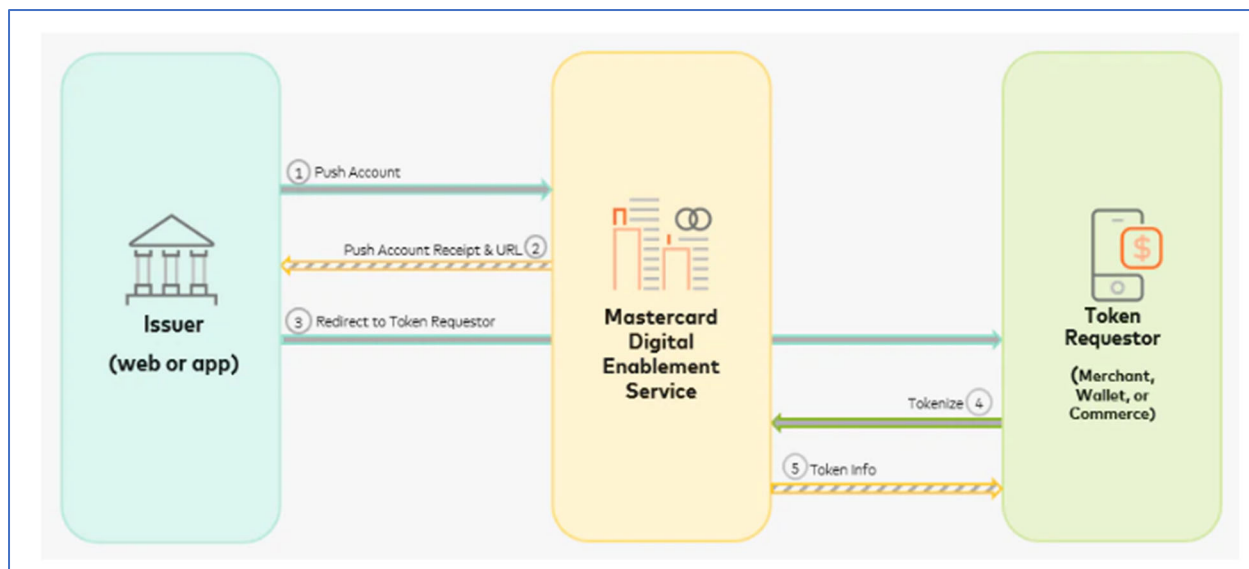
Key Benefits

Issuers

- **Push Provisioning:** Appeal to digital account holders by providing a new service to push provision payment cards and accounts into all participating token requestors with a single integration.
- **Scalable and Interoperable Framework:** No need for multiple proprietary APIs between issuers and token requestors. Once you are connected to the Token Connect framework, you can connect with any MDES token requestor that has implemented the service.

Cardholders

- **Instant:** Account holders can use their digital card account as soon as they have been approved and before their plastic card has been shipped.
- **Convenient:** Load new cards into favorite merchants and digital wallets simply and easily. Rather than entering their card details manually, cardholders simply select the card or account they want to digitize and choose from an up-to-date list of enabled merchants, digital wallets and commerce platforms.
- **Secure:** Payments that are provisioned are tokenized so account holders can shop online, in-apps and in-stores knowing their transaction is secure.



MDES Token Connect, MASTERCARD, <https://developer.mastercard.com/mdes-token-connect/documentation/> (last visited Jan. 19, 2024).

33. Mobile wallets may be implemented as an application (or “app”) on a mobile device, e.g., a mobile phone, tablet, or smartwatch. In some implementations, mobile wallets utilize Host Card Emulation, where, instead of storing Defendants’ payment application in a Secure Element on the host device, it is stored in the host CPU or remotely, e.g., in the cloud. In either case, mobile payments are made wirelessly, without contact needed between payment device and payment terminal, via, for example, Near Field Communication (“NFC”) protocols or Magnetic Secure Transmission (MST), as explained below. A user holds the mobile device close to the payment terminal in order to establish communication between the payment application and the payment terminal. These wireless methods utilized with EMV deliver secure transactions between a payment terminal and the mobile device.

EMV

EMV stands for Europay, MasterCard, and Visa. It's the technical standard for payments using Smart Cards which are cards with an embedded chip. These cards can be contact cards that need to be inserted in a terminal or contactless cards that can be read using NFC technology. Google Pay payments are presented to the payment terminal as EMV contactless payments.

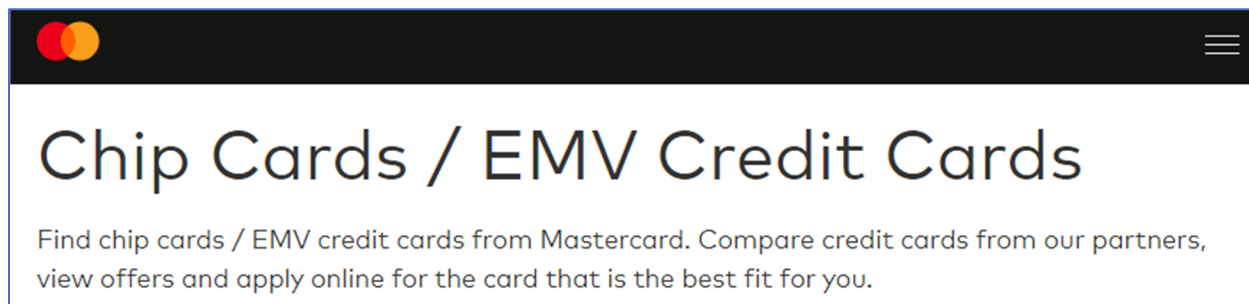
<https://support.google.com/pay/merchants/answer/7151369?hl=en>

Field Communication (NFC) and Magnetic Secure Transmission (MST). MST is Samsung's innovative technology that delivers secure transactions for new EMV chip and NFC terminals, as well as traditional, magnetic strip terminals, enabling consumers to use

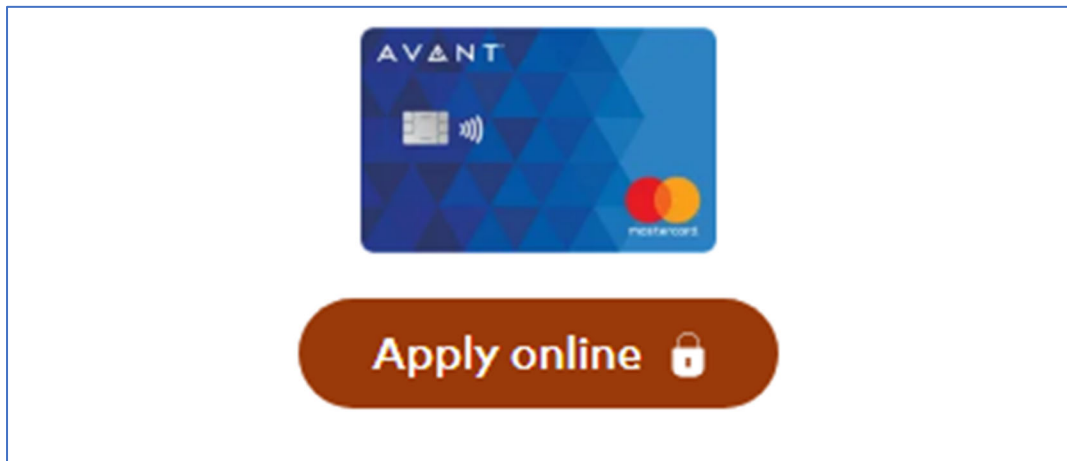
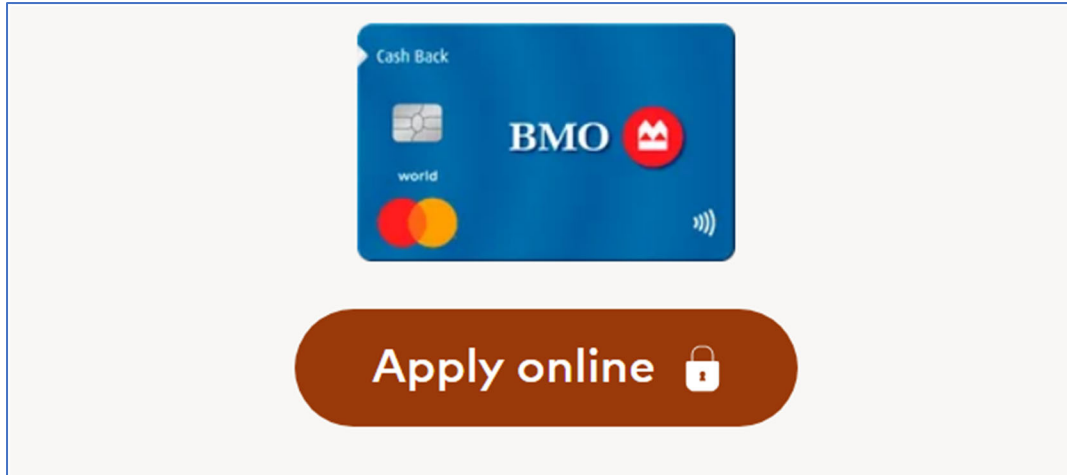
<https://news.samsung.com/us/samsung-pay-partners-global-pos-providers-accelerate-mobile-payments-adoption/>

34. On information and belief, Defendants directly and/or indirectly provide their payment technology to their licensees, issuers, acquirers, partners, developers, merchants, clients, consumers, customers, cardholders, and/or other users at least for utilization in transactions involving Mastercard Transaction Instruments (e.g., Mastercard Cards). These payment products utilize Mastercard's provisioning services to implement digital wallet services (e.g., Google Pay and Samsung Pay) that provide a distribution channel by which Defendants' payment applications (e.g., via the Secure Element on the mobile device) can be accessed and used.

35. As can be seen below in screenshots from Mastercard's website, Mastercard offers various credit solutions to its customers.



The screenshot shows the top portion of a Mastercard website page. At the top left is the Mastercard logo (two overlapping circles, one red and one yellow). At the top right is a hamburger menu icon (three horizontal lines). Below the logo and menu is a large heading: "Chip Cards / EMV Credit Cards". Underneath the heading is a sub-heading: "Find chip cards / EMV credit cards from Mastercard. Compare credit cards from our partners, view offers and apply online for the card that is the best fit for you."



See Chip Cards / EMV Credit Cards, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Feb. 2, 2024).

Mastercard® processing provides a versatile and distinctive range of payment services and solutions for every stage of the payment journey

Mastercard Prepaid
Management Services

**Mastercard Payment
Transaction Services**

Mastercard Payment Gateway
Services

A configurable platform that enables issuers and acquirers to seamlessly integrate their customers' needs into their offerings. We provide our customers with global capabilities to deliver solutions at the local level.

Issuer Processor

- Credit Processing
- Debit Processing
- Prepaid Processing (Program Management)

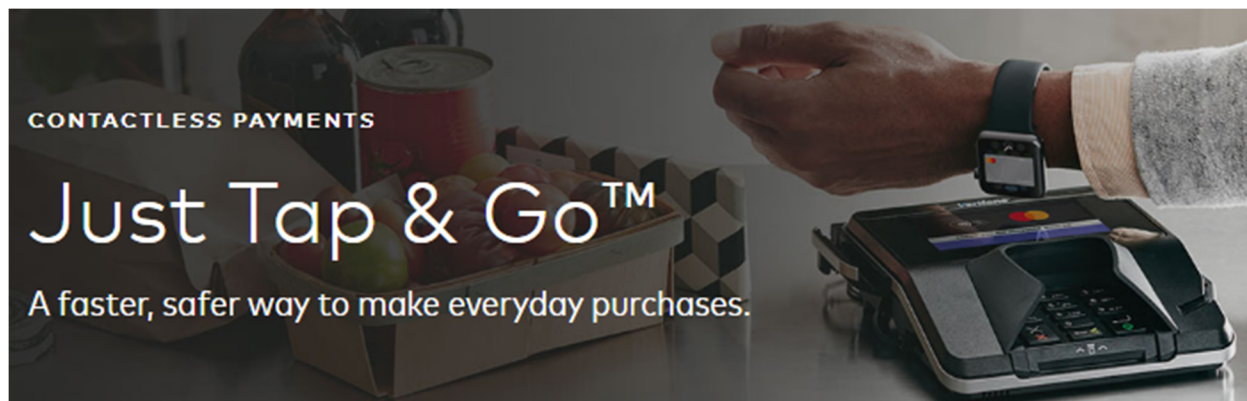
Acquirer Processor

- Switching Services (Use & Pay)
- Acquirer Processing - White Label ATM
- Acquirer Processing - Terminal Driving
- Acquirer Processing - Payment Gateway Services

An exceptional suite of services

- Merchant Management
- Customer Service
- Card and Account Management
- Data and Reporting
- Fraud and Risk Services

Innovative, agile, secure, reliable, MASTERCARD, <https://sea.mastercard.com/en-region-sea/business/issuers/products-and-solutions/payment-innovations/processing-solutions.html> (last visited Jan. 19, 2024).

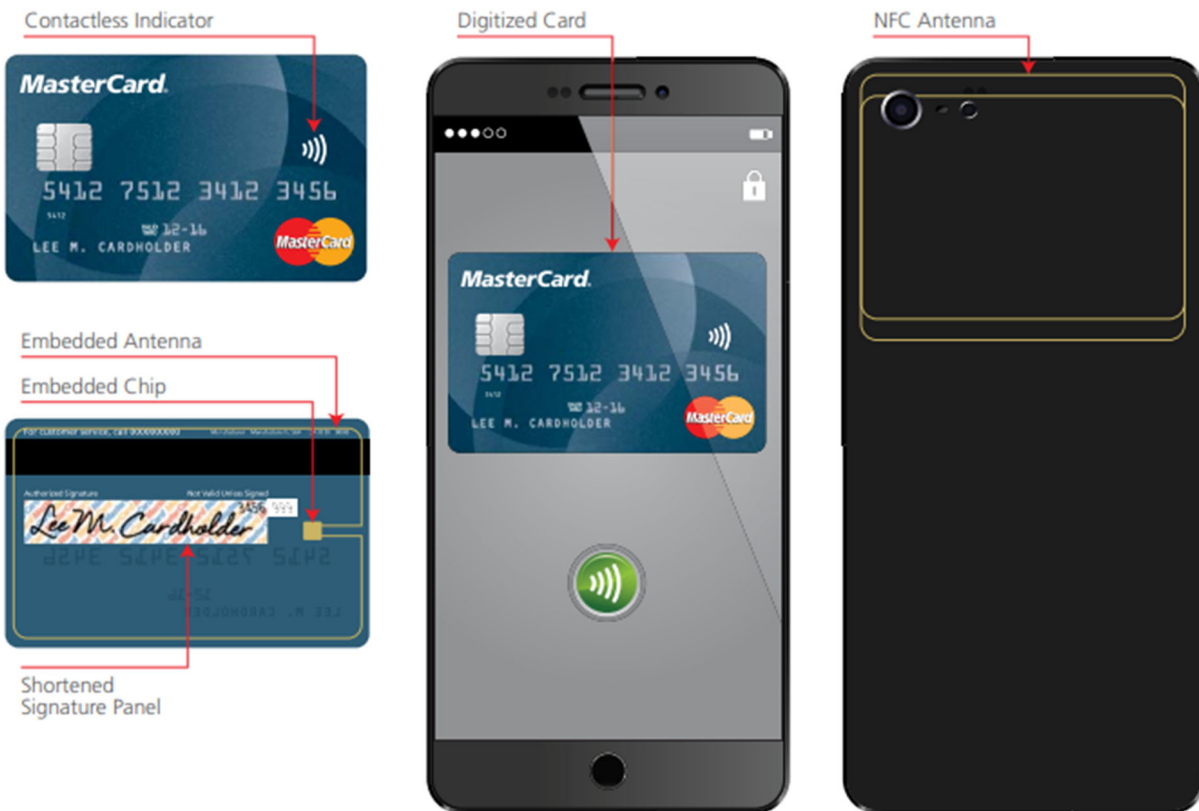


It's like having exact change wherever you go, but even faster and more convenient than cash. Use anywhere you see the Contactless symbol at checkout.



Contactless Payments, MASTERCARD, <https://www.mastercard.us/en-us/personal/ways-to-pay/contactless.html> (last visited Jan. 19, 2024).

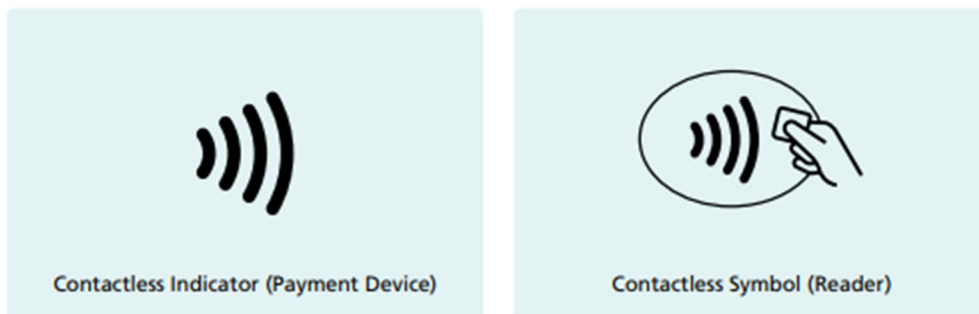
36. As indicated below, Defendants' payment applications reside, for example, on microchips embedded on Mastercard Transaction Instruments (e.g., Mastercard Cards), which allow the cardholder to tap the card to a reader and complete a transaction wirelessly without contact between the card's magnetic stripe and the reader.



Contactless capability is denoted by the universal **Contactless Indicator** (see below) which is present on all contactless cards and form factors or should be displayed on the screen of contactless mobile devices.

A **Contactless Symbol** is present on all contactless readers to indicate compliance with EMV Contactless Communication Protocol, and the Contactless Symbol must be used to indicate the "read area" on the reader where the payment device should be tapped.


Any payment device with a Contactless Indicator will work on any reader with a Contactless Symbol. This global interoperable acceptance is an important part of the MasterCard contactless payment proposition




Contactless Toolkit for Issuers, MASTERCARD,

https://www.mastercard.com/contactless/doc/MC_Contactless_Toolkit_Issuers.pdf (last visited Jan. 19, 2024).

37. On information and belief, the Accused Instrumentalities include at least Defendants’ payment card (e.g., banking, credit, debit, and prepaid card) related products, methods, and/or services for contactless payments that utilize EMV standards for contactless payment. *See, e.g., Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024).

38. Defendants’ Mastercard Transaction Instruments (e.g., Mastercard Cards) include EMV compliant contactless payment functionality indicated by the “Contactless Indicator”  which appears prominently on the cards.

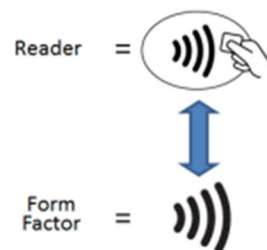
39. The Contactless Indicator “represents compatibility with a Point of Sale (POS) terminal or reader which is compliant with the EMV Contactless Communication Protocol” and in payment-related environments consumers may use their compliant card or device on a POS terminal or reader bearing the “Contactless Symbol”  as explained below.

Using the Contactless Indicator and Contactless Symbol together in Traditional Payment Environments

The Contactless Indicator may be used for transactions beyond payments on consumer-held form factors (card, key fob, mobile device) or a contactless reader, terminal, or other “point of transaction” device.

When shown on a traditional bank card or equivalent payment-related form factors, the Contactless Indicator represents compatibility with a Point of Sale (POS) terminal or reader which is compliant with the EMV Contactless Communication Protocol.

Payment-related transaction environments use the Contactless Symbol on POS terminal or reader.



<https://www.emvco.com/wp-content/uploads/2020/02/EMVCo-Contactless-Indicator-Reproduction-Requirements-Nov-2019.pdf>

40. On information and belief, a process referred to as “tokenization,” which is also part of the EMV standards, is also utilized by Defendants in authorizing transactions for Mastercard

Transaction Instruments (e.g., Mastercard Cards), via online payments, in-app payments, and mobile payments. As explained below, a “payment token” is a “surrogate value for a PAN” (a primary account number). In tokenization, “Payment Tokens are requested, generated, issued, provisioned, and processed as a surrogate for PANs.”

Payment Token	A surrogate value for a PAN that is a variable length, ISO/IEC 7812-compliant numeric issued from a designated Token BIN or Token BIN Range and flagged accordingly in all appropriate BIN tables. A Payment Token must pass basic validation rules of a PAN, including the Luhn check digit. Payment Tokens must not collide or conflict with a PAN.
Payment Tokenisation	A specific form of tokenisation whereby Payment Tokens are requested, generated, issued, provisioned, and processed as a surrogate for PANs as described by the processes defined in this technical framework.

<https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/EMVCo-Payment-Tokenisation-Specification-Technical-Framework-v2.0.pdf>

41. Via mobile wallet applications, such as Google Pay and Samsung Pay, tokenization is implemented by Defendants assigning a “virtual account number” or token that “securely links the actual card number to a virtual card on the user’s Google Pay-enabled device” or Samsung Pay-enabled device.

Tokenization

Google Pay facilitates the assignment of a “virtual account number,” also called a token, that securely links the actual card number to a virtual card on the user’s Google Pay-enabled device. A token is unique to the card number it represents. The app user’s mobile device keeps an encryption key in memory that it uses to decrypt limited-use and single-use keys (also called cryptograms) for contactless transactions (NFC payments).

<https://support.google.com/pay/merchants/answer/7151299?hl=en>

42. Defendants, as providers and/or licensors of solutions (e.g., products, methods, and/or services) to account issuers for Mastercard Transaction Instruments (e.g., Mastercard Cards), merchants involved in transactions associated with Mastercard Transaction Instruments, and/or merchant acquirers involved in transactions associated with Mastercard Transaction Instruments, act on behalf of and/or direct and control the activities of third parties, including, but not limited to, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, consumers, and/or cardholders, in the operation of the Mastercard Transaction Instruments using Mastercard's payment solutions (e.g., products, methods, and/or services). Defendants act on behalf of and/or direct and control the infringing activities of third parties by conditioning and permitting the use of Mastercard Transaction Instruments (and the benefits derived therefrom) upon performance by one or more of those third parties of a step or steps or by use by those third parties of certain claimed apparatuses or systems of the Asserted Patents. *See Akamai Techs. V. Limelight Networks*, 797 F.3d 1020, 1023-24. Moreover, by establishing and maintaining their payment products, methods, and/or services, Defendants further act on behalf of and/or direct and control the activities of third parties in infringing the Asserted Patents. For example, Defendants directly employ or require that third parties conform to EMV contactless standards in performing various EMV contactless transactions. *See, e.g., Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024).

43. Additionally, Defendants, as providers and/or licensors of solutions, products, methods, and/or services to account issuers for Mastercard Transaction Instruments (e.g., Mastercard Cards), merchants involved in transactions associated with Mastercard Transaction Instruments, and/or merchant acquirers involved in transactions associated with Mastercard

Transaction Instruments, act on behalf of and/or direct and control the activities of third parties in connection with the operation of mobile wallets. This is described below with respect to the mobile wallet Google Pay.

(c) GPC's Role. While Google Pay enables you to store your Payment Instruments and transmit their information to merchants or transit providers, neither GPC nor Google processes Google Pay transactions with such Payment Instruments, and neither exercises control over: the availability or accuracy of payment cards, payments, refunds, chargebacks; the provisioning (or addition) of cards to Google Pay; or other commercial activity relating to your use of Google Pay. For any concerns relating to the foregoing, please contact your Payment Instrument's issuer. You acknowledge and agree that your transactions through Google Pay are transactions between you and the merchant and not with GPC, Google, or any of their affiliates. For disputes relating to payment transactions conducted using Google Pay, contact your Payment Instrument's issuer or the appropriate merchant. Neither GPC nor Google is a party to your registered Payment Instruments' cardholder agreements or other terms of use, and neither is involved in issuing credit or determining eligibility for credit. GPC does not make any representation or verify that any of your Payment Instruments are in good standing or that the issuer of your Payment Instrument will authorize or approve any transaction with a merchant or transit provider when you use Google Pay in connection with that transaction.

https://payments.google.com/payments/apis-secure/u/0/get_legal_document?ldo=0&ldt=googlepaytos&ldl=und#SafeHtmlFilter_US

As an example of how Defendants act on behalf of and/or direct and control third parties in connection with mobile wallets, Defendants provision third-party mobile wallets with Defendants' own credentials and EMV payment applications, e.g., via Mastercard's push provisioning digital wallets. *See, e.g., MDES Token Connect*, MASTERCARD, <https://developer.mastercard.com/mdes-token-connect/documentation/> (last visited Jan. 19, 2024) (describing "Push Provisioning" using Mastercard Digital Enablement Service (MDES) Token Connect.).

44. Accordingly, Defendants use at least agreements, the required implementation of specified protocols, and/or design of products, software, and/or applications to condition participation in an activity or receipt of a benefit, for example, access to and use of Mastercard's

products, methods, and/or services, upon performance of a step or steps of a patented method and establish the manner or timing of that performance.

45. The Accused Instrumentalities of Defendants infringe at least claims of the '671 patent, which provide technological solutions and improvements addressing security concerns surrounding the provisioning of credentials to, and transactions performed using, digital wallets. Though conventional methods for securing financial transactions utilized personal identifiers, such as PINs, such identifiers could be easily duplicated or discovered. Even with the use of electronic wallets and more intelligent instruments, there remained a need to further safeguard electronic transactions against evolving threats. In at least one exemplary embodiment, the '671 patent addresses the need for securing RFID transactions by establishing a challenge from a computer-based system sent to an intelligent token of a client. The token generates a challenge response that is received by the computer-based system. Credentials, assembled by the computer-based system, include a key. In a given transaction, a client may make a request to the computer-based system including at least a portion of the assembled credentials. The computer-based system may validate the portion of the assembled credentials with the key and provide access to a transaction service. Utilizing systems and methods such as these, the '671 patent's claims allow issuers of Mastercard Transaction Instruments (e.g., Mastercard Cards) to secure direct and safe transactions between consumers and merchants.

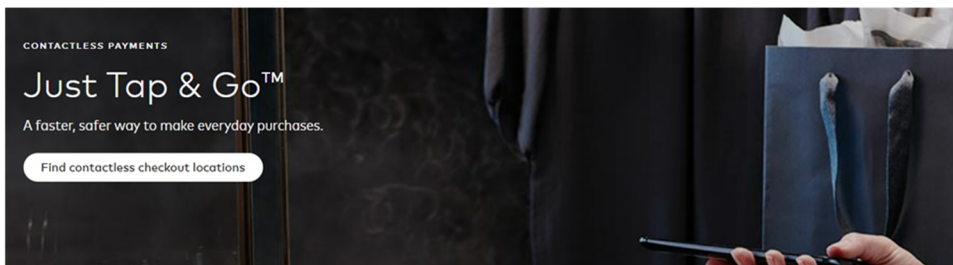
46. Defendants infringe the '671 patent via Defendants' computer-based systems that provide processing, authorization, clearing and settlement services to its card issuer customers and/or via direction and control of third parties in connection with these systems.

47. The MasterCard payment ecosystem effects contactless payment transactions. MasterCard requires customers to conform to the EMV standards when provisioning cards to mobile wallets and effecting contactless transactions.

A new era of payments
and security

Mastercard® EMV chip technology offers smarter, more secure and more efficient payments

<https://sea.mastercard.com/en-region-sea/business/issuers/products-and-solutions/payment-innovations/chip-emv.html>



It's like having exact change wherever you go, but even faster and more convenient than cash. Use anywhere you see the Contactless symbol at checkout.

<https://www.mastercard.us/en-us/consumers/payment-technologies/contactless.html>

1.1 Eligibility to be a Customer

An entity eligible to be a Customer may apply to become a Customer. No entity may participate in Activity until that entity is approved to be a Customer, has executed the applicable Licenses for the proposed Activity in a form acceptable to the Corporation, and has paid all associated fees and other costs.

1.6 The License

Each Customer agrees, and by use of any one or more of the Marks agrees, to comply with all provisions of the License pertaining to use of the Marks and with the Standards of this Corporation as may be in effect from time to time.

In the event of an inconsistency between a Standard and a provision in a License, the Standard prevails and the License is deemed to be amended so as to be consistent with the Standard. Each Customer must assist the Corporation in recording any License granted to the Customer if required in the country in which the Customer is Licensed or otherwise upon request of the Corporation.

2.2.1 Customer Responsibilities

At all times, each Customer must:

1. Be entirely responsible for and Control all aspects of its Activities and Digital Activities, and the establishment and enforcement of all management and operating policies applicable to its Activities and Digital Activities, in accordance with the Standards;

<https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/mastercard-rules.pdf>

Acquirer	Issuer
A Customer in its capacity as an acquirer of a Transaction.	A Customer in its capacity as an issuer of a Card or Account.

6.1 Card Issuance—General Requirements

An Issuer must operate each of its Programs in accordance with the Standards as may be in effect from time to time.

Point-of-Sale (POS) Terminal

An attended or unattended device located in or at a Merchant’s premises, including an MPOS Terminal, that enables a Cardholder to effect a Transaction for the purchase of products or services sold by such Merchant with a Card and/or Access Device, or attended device located in the premises of a Customer or its authorized agent that facilitates a Manual Cash Disbursement Transaction, including a Bank Branch Terminal. A POS Terminal must comply with the POS Terminal security and other applicable Standards.

Third Party Processor (TPP) Program Service

- Terminal operation with electronic data capture deployment

7.1.2 Third Party Processor

All TPPs must comply with applicable Standards, including these Service Provider Rules, in order to remain in good standing as a TPP.

<https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/mastercard-rules.pdf>

Access Device

A device other than a Card that has successfully completed all applicable Mastercard certification and testing requirements, if any, and:

- Uses at least one Payment Application provisioned to the device by or with the approval of a Customer to provide access to an Account;
- Supports the transmission or exchange of magnetic stripe or chip data containing a dynamic cryptogram to or with a Terminal, as applicable, by implementing the EMV Contactless Specifications (Book D) to effect Transactions at the Terminal without requiring direct contact of the device to the Terminal; and
- May also support the transmission of magnetic stripe data containing a dynamic cryptogram to a Terminal to effect Transactions identified by the Acquirer in Transaction messages as magnetic stripe Transactions.

A Cirrus Access Device, Maestro Access Device, and Mastercard Access Device is each an Access Device. Also see Mobile Payment Device.

Contactless Transaction

A Transaction in which data is exchanged between the Chip Card or Access Device and the Terminal through the reading of the chip using the contactless interface, by means of radio frequency communications. Also see EMV Mode Contactless Transaction, Magnetic Stripe Mode Contactless Transaction.

Chip Card (Smart Card, Integrated Circuit Card, IC Card, or ICC)

A Card with an embedded EMV-compliant chip containing memory and interactive capabilities used to identify and store additional data about a Cardholder, an Account, or both.

EMV Mode Contactless Transaction

A Contactless Transaction in which the Terminal and the chip exchange data, enabling the chip to approve the Transaction offline on the Issuer’s behalf or to request online authorization from the Issuer, in compliance with the Standards.

<https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/mastercard-rules.pdf>

2.1 Acquirer Authorization Requirements

In the U.S. Region, the Rule on this subject is modified as follows.

An Acquirer must support POS balance inquiry for all prepaid Debit Mastercard and prepaid Maestro Accounts.

2.1.1 Acquirer Host System Requirements

An Acquirer in the U.S. Region must ensure that its POS Terminal host systems and those of its Service Providers:

1. Are capable of processing Contact Chip Transactions and Contactless Transactions (including both EMV Mode Contactless Transactions and Magnetic Stripe Mode Contactless Transactions);
2. Support the transmission of Contact Chip Transaction and Contactless Transaction messages in accordance with the Standards;
3. Support PIN (both online and offline), signature, and no Cardholder verification method (CVM) as CVM options for Chip Transactions, regardless of whether each Hybrid POS Terminal connected to the Acquirer host system supports all of these options;
4. Support all mandatory and applicable conditional data subelements within DE 55 (Integrated Circuit Card [ICC] System-Related Data); and
5. Have been approved by the Corporation, with respect to each Interchange System network interface, as enabled for Contact Chip Transaction and Contactless Transaction processing.

7.6 Hybrid Terminal Requirements

In addition to complying with Rule 7.2, a Hybrid Terminal must:

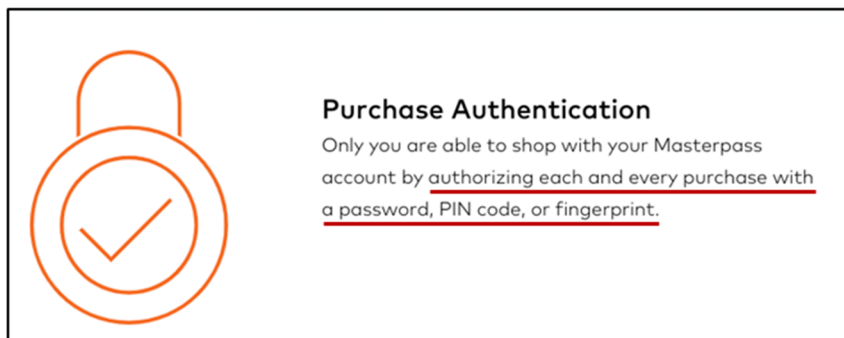
1. Read required data from the chip when present in Chip Cards, and either transmit or process, as appropriate, all required data for authorization processing;
2. Complete the Transaction using the EMV chip if present;

The Acquirer must comply with the MPOS Terminal requirements set forth in the *MiChip Requirements* manual, the EMV chip specifications, and section 4.10 of the *Security Rules and Procedures* manual.

<https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/transaction-processing-rules.pdf>

48. Defendants also infringe the '671 patent via Defendants' computer-based systems that conduct user enrollment processes for mobile wallet payments associated with Mastercard Transaction Instruments (e.g., Mastercard Cards); and/or via direction and control of third parties in connection with these systems.

49. Before provisioning a user's mobile wallet with payment credentials, MasterCard first conducts a user enrolment process, which includes forwarding a challenge to the user's mobile device (intelligent token). This challenge is used for identification and verification (ID&V) of the user, and for device attestation to determine the device is in a trusted state.



<https://masterpass.com/en-us/>

EMV

EMV stands for Europay, MasterCard, and Visa. It's the technical standard for payments using Smart Cards which are cards with an embedded chip. These cards can be contact cards that need to be inserted in a terminal or contactless cards that can be read using NFC technology. Google Pay payments are presented to the payment terminal as EMV contactless payments.

Google Pay Merchant Help: EMV, GOOGLE,

<https://support.google.com/pay/merchants/answer/7151369?hl=en> (last visited Oct. 12, 2023).

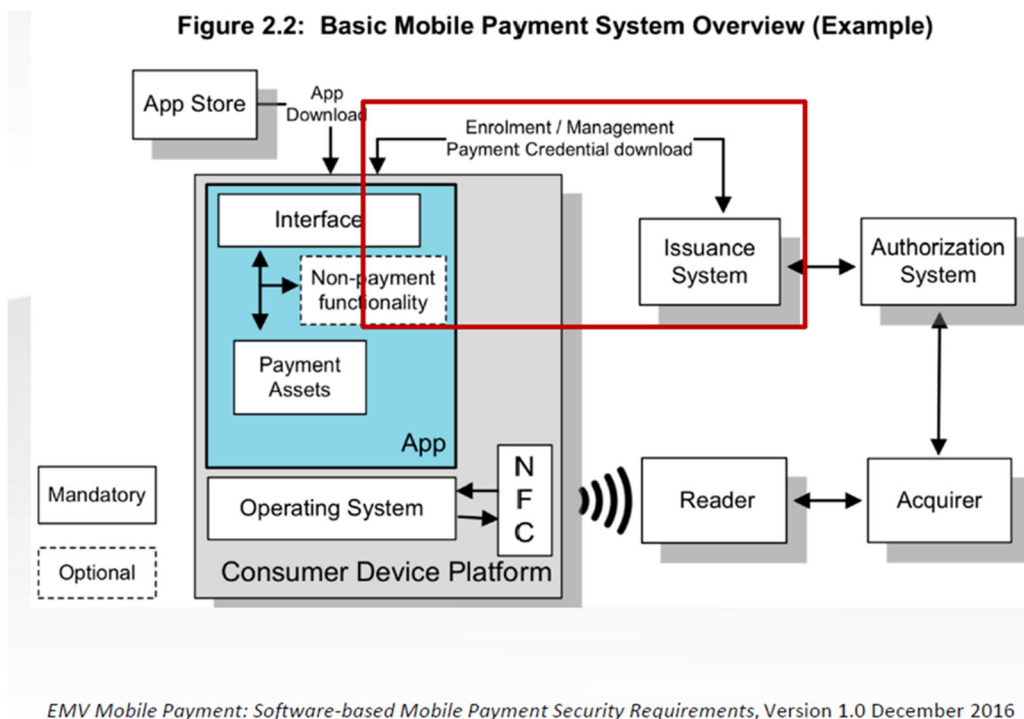
Field Communication (NFC) and Magnetic Secure Transmission (MST). MST is Samsung's innovative technology that delivers secure transactions for new EMV chip and NFC terminals, as well as traditional, magnetic strip terminals, enabling consumers to use

Samsung Pay Partners with Global POS Providers to Accelerate Mobile Payments Adoption,

SAMSUNG, <https://news.samsung.com/us/samsung-pay-partners-global-pos-providers-accelerate-mobile-payments-adoption/> (April 19, 2016) (last visited Oct. 12, 2023).

50. Such systems of Defendants directly and indirectly infringe the '671 patent by enabling and conducting mobile payments that utilize mobile wallets, such as Google Pay and Samsung Pay. Defendants act on behalf of and/or direct and control third parties, including issuers and/or vendors, to configure the mobile wallets of cardholders to conform to EMV standards. As part of utilizing a consumer's mobile wallet, Defendants act on behalf of and/or direct and control the activities of third parties, including issuers and/or vendors, to conduct an enrollment process,

which forwards a challenge to a cardholder's mobile device, i.e., an intelligent token, as shown below.



51. As described below, the challenge is used in the enrollment process for identification and verification of the consumer, as a user of the mobile wallet, and for device attestation to determine that the device is in a trusted state. Furthermore, Defendants receive this challenge response.

3.3 User Enrolment

User enrolment enables the cardholder to request the registration of their Software Card. It is an important life cycle event, normally conducted remotely (e.g. OTA), at the time a consumer wishes to enrol a payment card to the Mobile Application. Some Identification and Verification (ID&V) considerations that need to be taken into account are:

- There must be defined and established Identification and Verification (ID&V) requirements to be used during the user enrolment process.
- The user enrolment process must verify through remote device attestation whether the device is in a trusted state before releasing protected data to or storing private information on the Consumer Device.

EMV Mobile Payment: Software-based Mobile Payment Security Requirements, Version 1.0 December 2016

52. Defendants further assemble credentials, including encryption keys, to be used when effecting transactions, referred to as “provisioning” below.

3.4 Provisioning and Credential Issuance

Following enrolment, provisioning and credential issuance is defined as the configuration of the Software Card within the Mobile Application to be ready for use, including an initial set of card credentials and possibly device risk parameters.

- The Mobile Application must connect to the cloud-based system to obtain payment credentials such as keys, tokens, parameters.
- The Mobile Application must allow the credential manager to refresh/update the card data elements on subsequent connections to the cloud-based system.

EMV Mobile Payment: Software-based Mobile Payment Security Requirements, Version 1.0 December 2016

53. In a given transaction, Defendants receive a request from the consumer’s mobile wallet, which includes the assembled credentials, such as the application primary account number (PAN or also token) and an Application Cryptogram, which is encrypted with the provided key. Defendants validate the consumer’s credentials using the provided key.

54. Once the mobile wallet is validated, as described below, the transaction is allowed to proceed.

be useful for clarity. The ARQC is a cryptogram generated by the card from transaction data using an issuer key stored in the card and known at the issuer authorisation system. The issuer uses this key to authenticate the ARQC and thereby authenticate the card. This process is termed ‘online card authentication’ or simply ‘card authentication’.

EMV Integrated Circuit Card Specifications for Payment Systems: Book 3, Application Specification, Version 4.3, November 2011

55. The Accused Instrumentalities of Defendants infringe one or more claims of the ’985 patent, which provide methods and systems for authorizing payment transactions for

customers with more than one transaction instrument representing a single transaction account. In the '985 patent, customer-level transaction data may be determined to be common to more than one instrument, and such data may be analyzed in order to authorize a payment transaction. Data elements may be verified across multiple records for an individual customer. One advantage of such verification is that it improves the accuracy of transaction risk calculations, for example, by reducing the probability of errors during fraud detection. Other advantages include providing merchants with comparison results at the data element level to assist in a decision-making process. In at least one exemplary embodiment of the '985 patent, a computer system may receive an authorization request from a merchant for a transaction. Such a transaction may be initiated by using a transaction instrument corresponding to a user. The computer system may determine a second transaction instrument corresponding to the user. To authorize the transaction, the computer system may analyze transaction data that corresponds to transaction data associated with the second transaction. The '985 patent allows for increased security and confidence during a transaction and reduces the number of incorrectly declined transactions due to authorization errors as well as providing an increase in customer satisfaction.

56. Defendants infringe the '985 patent via Defendants' set of card issuance solutions for banks and financial institutions, including without limitation processing and support for mobile wallets, and EMV-compliant payment applications used in conjunction with mobile wallets, including Google Pay and Samsung Pay and/or via direction and control of third parties in connection with these payment applications. As an example, Mastercard provides a complete set of credit and card issuance solutions for banks and financial institutions. *See, e.g., Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024); *Innovative, agile, secure, reliable*, MASTERCARD,

<https://sea.mastercard.com/en-region-sea/business/issuers/products-and-solutions/payment-innovations/processing-solutions.html> (last visited Jan. 19, 2024); *Contactless Payments*, MASTERCARD, <https://www.mastercard.us/en-us/personal/ways-to-pay/contactless.html> (last visited Jan. 19, 2024).

57. The MasterCard payment ecosystem effects RF payment transactions. MasterCard requires customers to conform to the EMV standards when effecting RF transactions. *See, e.g.*, evidence *supra* for the ‘671 patent relating to Mastercard requiring conformance to the EMV standards.

58. Mastercard also provisions EMV compliant payment applications for consumers’ cards onto mobile wallets, including Google Pay and Samsung Pay. In connection with transaction instruments and/or the mobile wallets that Mastercard provisions, at least one Mastercard computer system performs the steps of claim 1 of the ‘985 patent. *See, e.g., What is Push Provisioning and why does it matter?*, MASTERCARD, https://developer.mastercard.com/blog/what_is_push_provisioning/ (last visited Jan. 19, 2024); *MDES Token Connect*, MASTERCARD, <https://developer.mastercard.com/mdes-token-connect/documentation/> (last visited Jan. 19, 2024); *Google Pay Merchant Help: EMV*, GOOGLE, <https://support.google.com/pay/merchants/answer/7151369?hl=en> (last visited Oct. 12, 2023); *Samsung Pay Partners with Global POS Providers to Accelerate Mobile Payments Adoption*, SAMSUNG, <https://news.samsung.com/us/samsung-pay-partners-global-pos-providers-accelerate-mobile-payments-adoption/> (April 19, 2016) (last visited Oct. 12, 2023).

59. As required by Mastercard for use with mobile wallets, Mastercard offers tokenization to all its card issuer customers. MasterCard requires that issuers wishing to support mobile payments comply with all standards applicable to tokenization, including the EMV

Tokenization

standard.

<p>6.1.4 Tokenization of Accounts</p> <p>With respect to the Tokenization of Accounts, all of the following applies:</p> <ol style="list-style-type: none">1. The Corporation has the sole right to designate a Mastercard Token Account Range to an Issuer.
<ol style="list-style-type: none">2. Each Mastercard Token must be allocated by the Corporation, unless the Corporation has expressly approved otherwise.3. The Tokenization of an Account primary account number (PAN) must be performed in compliance with all applicable Standards, including but not limited to the Mastercard Token Service Provider Standards.4. Mastercard must be provided the mapping between the PAN assigned to a Card, and each Mastercard Token associated with the Account for use by the authorized user of the Card.5. An Account PAN must be Tokenized whenever a Mobile Payment Device, Access Device, or other non-Card method is used, in addition to a Card, to provide access to an Account.6. The PAN of a Mastercard Card or Access Device or any Maestro Card or Access Device for which Maestro is the primary Payment Application must not be replaced by, mapped to, or Tokenized with any PAN issued from an Issuer Identification Number (IIN) reserved by the ISO Registration Authority for a competing payment network. Refer to the current <i>ISO Register Of Issuer Identification Numbers</i> for more information.7. The Mastercard Token cryptogram must be validated during the authorization of all Transactions involving Tokenized Accounts. <p>An Issuer wishing to support the Tokenization of its Accounts for use on a Mobile Payment Device must:</p> <ol style="list-style-type: none">1. Comply with all technical specifications and other Standards applicable to Tokenization and Digitization;2. Complete all testing and certifications as may be required by the Corporation from time to time in connection with Tokenization and Digitization;

<https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/mastercard-rules.pdf>

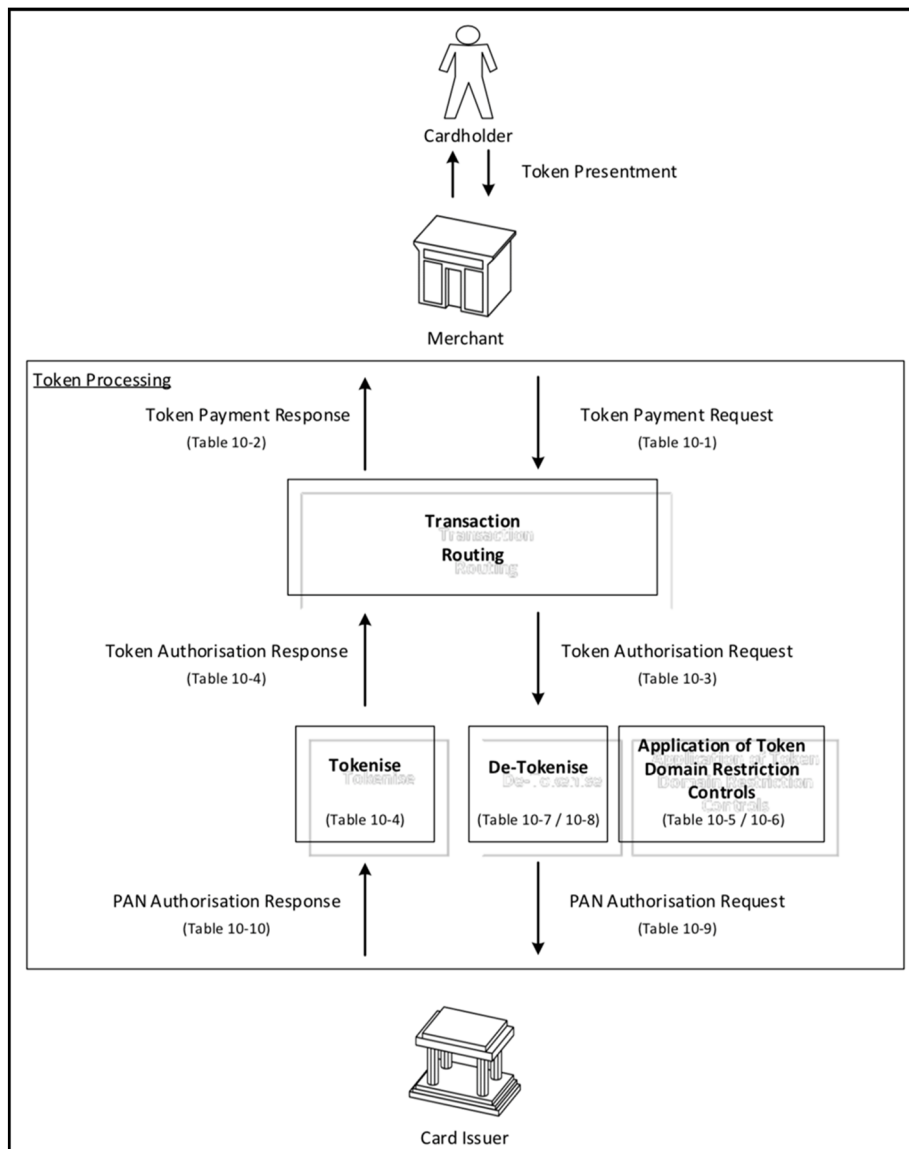
60. Defendants, via their token service, create virtual account numbers, referred to as tokens in the mobile wallet context, for provisioning to mobile wallets and initiating transactions associated with Mastercard Transaction Instruments (e.g., Mastercard Cards). Transactions associated with Mastercard Transaction Instruments made online by consumers may also utilize virtual account numbers via “tokenization,” as shown below in relation to Google Pay.

Tokenization

Google Pay facilitates the assignment of a "virtual account number," also called a token, that securely links the actual card number to a virtual card on the user's Google Pay-enabled device. A token is unique to the card number it represents. The app user's mobile device keeps an encryption key in memory that it uses to decrypt limited-use and single-use keys (also called cryptograms) for contactless transactions (NFC payments).

<https://support.google.com/pay/merchants/answer/7151299?hl=en>

61. When a consumer conducts a transaction using a mobile wallet, a tokenized account number is sent to Mastercard for de-tokenization and authorization. As shown below, tokenized account numbers (i.e., a first transaction instrument) are processed, i.e., de-tokenized, and then sent to the card issuer as a PAN authorization request.



Token Payment Request: includes the request that originates from the point of interaction with the Merchant (such as a Terminal, website or application) and the response that provides the results of the authorisation decision

EMV Payment Tokenisation Specification, Technical Framework v2.0, September 2017

62. Upon receipt of a Payment Token, Defendants, via their token service, convert the token into the corresponding account number (PAN) of the user, pursuant to the EMV specifications.

63. Mastercard analyzes the transaction data associated with a transaction in order to authenticate the transaction. For example, in a given transaction, Defendants receive a request from

a merchant for a transaction initiated using a first transaction instrument corresponding to a user (e.g., the consumer's mobile wallet, which includes assembled credentials, such as the application primary account number (PAN) and/or a token, which may be a tokenized version of the PAN, and an Application Cryptogram, which is encrypted with the provided key). As described below, Defendants validate the transaction data using a second transaction instrument corresponding to the user of the first transaction instrument (e.g., a provided key).

Table 10 contains existing data elements necessary for an ICC transaction.

Data Element	Condition
Acquirer Identifier	Present for Terminal Type = '1x' or '2x' if Merchant Identifier or Terminal Identifier does not implicitly refer to a single acquirer
Amount, Authorised * 12	
Amount, Other *	Present if cashback used for current transaction
Application Effective Date	Present if in ICC
Application Expiration Date	Present if not in Track 2 Equivalent Data
Application PAN *	Present if not in Track 2 Equivalent Data
Application PAN Sequence Number *	Present if in ICC
Enciphered PIN Data	Present if CVM performed is 'enciphered PIN for online verification'
Merchant Category Code	Present for Terminal Type = '2x' if Merchant Identifier or Terminal Identifier does not implicitly refer to a single merchant category

EMV Integrated Circuit Card Specifications for Payment Systems, Book 4, Cardholder, Attendant, and Acquirer Interface Requirements, Version 4.3, November 2011

8.1.2 Application Cryptogram Algorithm

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

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

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

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

64. Once the mobile wallet is validated, as described below, the transaction is allowed to proceed and the Mastercard issuer will respond to the merchant with an authorization message.

be useful for clarity. The ARQC is a cryptogram generated by the card from transaction data using an issuer key stored in the card and known at the issuer authorisation system. The issuer uses this key to authenticate the ARQC and thereby authenticate the card. This process is termed 'online card authentication' or simply 'card authentication'.

EMV Integrated Circuit Card Specifications for Payment Systems: Book 3, Application Specification, Version 4.3, November 2011

65. Data analyzed by Defendants indirectly, directly and in some cases jointly with (i.e., on behalf of and/or via direction and control of) issuers, merchants, acquirers, cardholders and/or customers, in association with the transaction include, without limitation, transaction amounts, expiration dates, transaction limits, personal identification numbers (PINs), information regarding cardholder accounts, and/or information included in a cryptogram. Upon receipt of data from Defendants, the issuer authorizes or declines the transaction, and if the transaction is authenticated,

Mastercard transmits a response to the merchant with an authorization message as explained below in relation to an EMV-type transaction.

10.9 Online Processing

Purpose:

Online processing is performed to ensure that the issuer can review and authorise or reject transactions that are outside acceptable limits of risk defined by the issuer, the payment system, or the acquirer.

be useful for clarity. The ARQC is a cryptogram generated by the card from transaction data using an issuer key stored in the card and known at the issuer authorisation system. The issuer uses this key to authenticate the ARQC and thereby authenticate the card. This process is termed 'online card authentication' or simply 'card authentication'.

EMV Integrated Circuit Card Specifications for Payment Systems: Book 3, Application Specification, Version 4.3, November 2011

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

66. As a further example of how Defendants infringe the '985 patent, Mastercard, directly and/or indirectly, allows merchants to use and store a token in place of customer credit card information. Accordingly, at least some of the card numbers stored by Mastercard's customers (merchants) are tokens, rather than actual card numbers.

67. Mastercard allows merchants to use Card-on-File (COF) transactions in which a multi-pay card token (a tokenized card number—that is, a first transaction instrument) associated with a user can be used as the source value in a payment request (i.e., an authorization request). *Card on File – Card Tokenization*, MASTERCARD, <https://www.mastercard.us/en-us/checkout/card-on-file.html> (last visited Jan. 18, 2024).

68. When a token is used for the transaction, Mastercard processing will know it is a tokenized number and determine that a secondary transaction instrument (the original card number) corresponds to the user.

69. Mastercard analyzes the transaction data by checking some of the submitted data against the issuer's cardholder information. Based on checking some of the submitted data against the issuer's cardholder information, a response indicates if the transaction has been authorized or declined.



The Brighterion integration within Mastercard Gateway can now deliver a unified ecosystem enabling acquirers to proactively detect, prevent, and mitigate fraudulent activities, ensuring enhanced security for both acquiring customers and their enterprise merchants.

This move is part of Mastercard Gateway's evolution beyond a traditional gateway provider to commerce facilitator. In this role Mastercard Gateway can orchestrate a dynamic offering providing seamless and secure payment experiences for merchants and their consumers.

Each transaction sent by Mastercard Gateway to Brighterion is evaluated within its perimeter in two paths: the AI model, and the rules set by the customer.

The AI model checks against multiple transaction indicators and compares them to patterns identified in historical customer and Mastercard data as correlated with fraudulent use. The model is monitored to evaluate when retraining is necessary.

The second framework established by Mastercard Gateway and Brighterion assesses the transaction with a Rules Management tool. Customers can use a variety of rules within the supported templates, as well as establish their own based on the business specifics.

1. Customer sets the rules and thresholds within the Brighterion User Interface when establishing the solution
2. When a transaction is being initiated by a cardholder, relevant information is transmitted by Mastercard Gateway to Brighterion
3. Brighterion evaluates the transaction data using models and rules and generates a real-time response of Accept or Reject
4. 'Accept': the Gateway actions the payment accordingly and sends the transaction to the issuer
5. 'Reject': the Gateway actions the payment accordingly and sends a decline response to the customer
6. The transaction score and rules are provided to the Gateway in real time and viewable via the portals

Mastercard Gateway and Brighterion – the right partnership matters, MASTERCARD, <https://www.mastercard.com/content/mastercardcom/gateway/expertise/insights/Gateway-Brighterion-partnership-matters.html> (last visited Feb. 2, 2024).

70. ‘The Accused Instrumentalities of Defendants infringe one or more claims of the ’756 patent, which provide methods and systems for securing the transfer of data between a proximity integrated circuit (PIC) payment device (e.g., a smartcard, fob, tag, mobile device, smart phone, tablet, etc.) and a merchant system. According to the ’756 patent, the term “smartcard” is “any integrated circuit transaction device containing an integrated circuit card payment application” and is “not limited by size or shape of the form factor.” *See* ’756 patent, 7:43-54. Conventional payment devices, including ones using smartcard and RF technologies, had a need for systems and methods that were secured against fraud and did not increase the time needed to complete a transaction. *See* ’756 patent, 4:30-36. In exemplary embodiments, a merchant system determines a merchant action analysis result based on authentication of a PIC transaction device using at least an Offline Data Authentication (ODA) technique, a transaction process restriction, or a merchant risk management factor. The action analysis result indicates whether to deny the transaction or approve the transaction, either offline or online. A PIC transaction device determines a card action analysis result indicating whether to approve the transaction. Based on at least one of the merchant action analysis result and the card action analysis result, the merchant system requests an authorization response from a PIC issuer system.

71. Defendants infringe one or more claims of the ’756 patent via at least Mastercard (e.g., through at least one or more subsidiaries and/or brands) directly and/or indirectly making, providing, and selling EMV compliant POS systems and devices.

72. The MasterCard payment ecosystem secures transactions utilizing PIC transaction devices. MasterCard requires customers to conform to the EMV standards when effecting chip card transactions. *See, e.g.*, evidence *supra* for the '671 patent relating to Mastercard requiring conformance to the EMV standards.

73. These POS systems and devices perform a method of securing a transaction utilizing a PIC transaction device, including acting on behalf of and/or directing and controlling third parties which use the Mastercard EMV compliant POS systems and/or devices and/or provide the systems and/or devices to consumers, such as at least providing merchant systems, to issuers, acquirers, merchants, and/or consumers in connection with Mastercard products, methods, and/or services.

EMV
EMV stands for Europay, MasterCard, and Visa. It's the technical standard for payments using Smart Cards which are cards with an embedded chip. These cards can be contact cards that need to be inserted in a terminal or contactless cards that can be read using NFC technology. Google Pay payments are presented to the payment terminal as EMV contactless payments.

Google Pay Merchant Help: EMV, GOOGLE,

<https://support.google.com/pay/merchants/answer/7151369?hl=en> (last visited Oct. 12, 2023)

(emphasis added).

Field Communication (NFC) and Magnetic Secure Transmission (MST). MST is Samsung's innovative technology that delivers secure transactions for new EMV chip and NFC terminals, as well as traditional, magnetic strip terminals, enabling consumers to use

Samsung Pay Partners with Global POS Providers to Accelerate Mobile Payments Adoption,

SAMSUNG, <https://news.samsung.com/us/samsung-pay-partners-global-pos-providers-accelerate-mobile-payments-adoption/> (April 19, 2016) (last visited Oct. 12, 2023).

74. Examples of Mastercard's EMV compliant POS systems and/or devices include Mastercard Mobile Point-of-Sale (MPOS) solutions that enable mobile devices to accept payments, including, but not limited to, Tap on Phone and Cloud Commerce, and services, for example, products, methods, and/or services for securing RFID transactions involving a PIC transaction device (e.g., Mastercard Card) and/or mobile wallets using host card emulation (e.g., in connection with Google Pay and Samsung Pay mobile wallets).



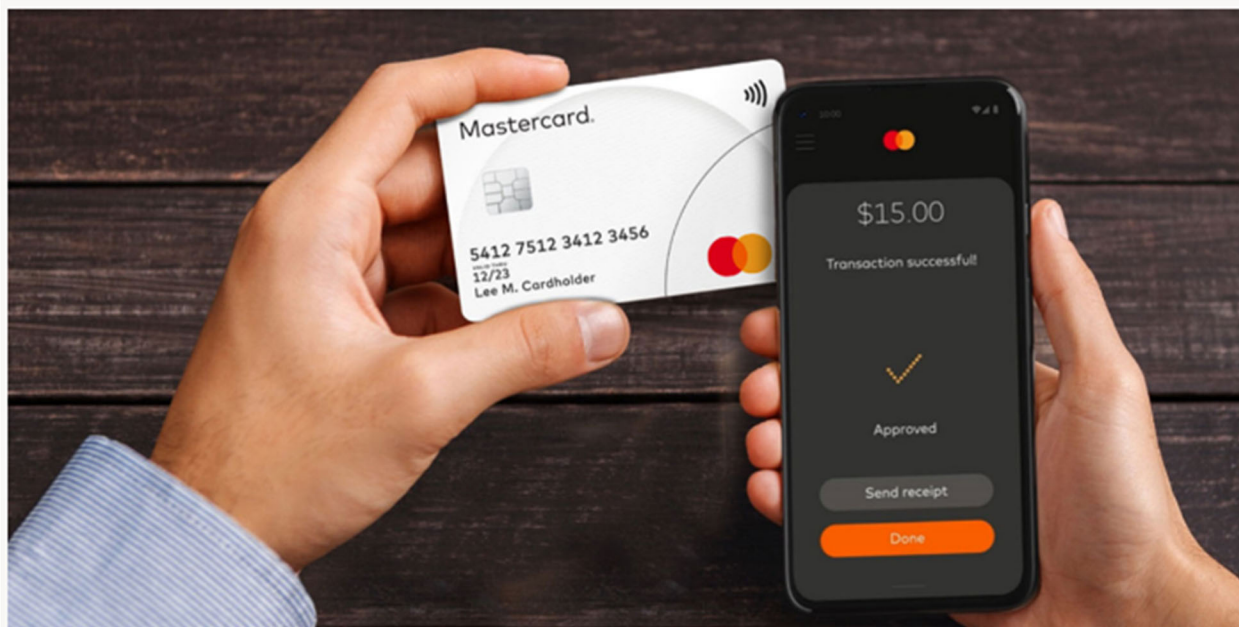
FOR ACQUIRERS, SERVICE PROVIDERS AND MERCHANTS

Mobile Point-of-Sale solutions (MPOS)

Benefit from our simple, low-cost acceptance solutions that use mobile devices to drive best-in-class consumer experiences.

[Become a partner](#) [Partner Directory →](#)

A promotional banner for Mastercard Mobile Point-of-Sale (MPOS) solutions. The banner features the Mastercard logo at the top left, followed by the text "FOR ACQUIRERS, SERVICE PROVIDERS AND MERCHANTS". Below this is the main headline "Mobile Point-of-Sale solutions (MPOS)" in a large, bold font. Underneath the headline is a sub-headline: "Benefit from our simple, low-cost acceptance solutions that use mobile devices to drive best-in-class consumer experiences." At the bottom of the banner, there are two call-to-action buttons: "Become a partner" in a red pill-shaped button and "Partner Directory →" in a white button with a right-pointing arrow. The background of the banner shows a blurred image of a person's shoulder and arm.



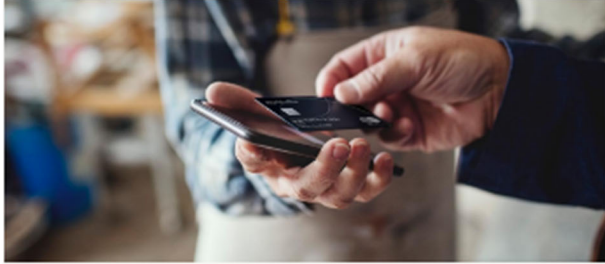
Putting payments at your fingertips

Our smart, simple and safe mobile payment solutions enable smartphones and tablets to accept payments.

By eliminating the need for traditional terminal hardware, we've created a simplified payments ecosystem that benefits large and small businesses — and their customers.

Mobile Point-of-Sale solutions

Meet the next generation of Point-of-Sale (POS) technology. From traditional mobile POS, which still relies on hardware to software-based solutions like Tap on Phone, we are making payment acceptance fast and easy. Cloud Commerce, our cloud native, software-based solution is the newest evolution that allows you to start accepting instantly.



SOFT POS

Tap on Phone

Provides merchants with a simple and cost-effective contactless payment acceptance solution that uses the smartphone they already own.

[Learn more](#)



SOFT POS

Cloud Commerce

Mastercard's cloud native, software-based acceptance solution combines Tap on Phone, Pay by Link, Click to Pay and more, enabling simple physical and digital merchant acceptance.

[Learn more](#)

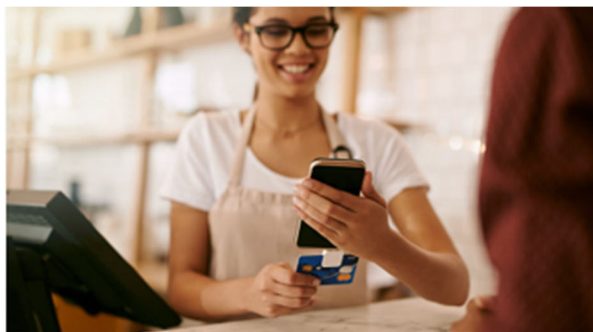


MPOS USING HARDWARE

Software-based PIN Entry on COTS (SPOC)

PIN on Glass, also known as Software-based PIN Entry on COTS (Commercial Off-the-Shelf Device) (SPoC), is a software-based solution that enables EMV contact and contactless transactions with PIN entry on a merchant's consumer device, when combined with a secure card reader/dongle for PIN.

[Learn more](#)



MPOS USING HARDWARE

Traditional MPOS

Traditional Mobile POS uses card reader accessories that attach to the audio port, USB port, proprietary connector or via Bluetooth on mobile devices. These accessories offer magnetic stripe, EMV chip card and/or contactless acceptance and are sometimes referred to as "dongles." Other accessories referred to as "sleeves" generally wrap around or encase the mobile device and may be capable of performing magnetic stripe, EMV chip and NFC-contactless transactions with PIN verification.

[Learn more](#)

See Mobile Point-of-Sale solutions (MPOS), MASTERCARD,

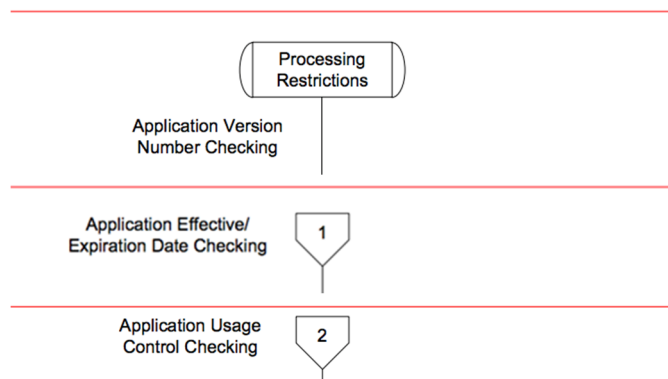
<https://www.mastercard.com/global/en/business/overview/start-accepting/mobile-pos.html> (last visited Jan. 19, 2024).

75. Mastercard’s mobile point-of-sale solutions and/or EMV-compliant merchant systems and devices (e.g., payment terminals), determine a first action analysis result based at least in part on one of an Offline Data Authentication, a risk management factor, and a process restriction analysis. For example, this occurs as part of an EMV mode transaction after a “GET PROCESSING OPTIONS” command, as exemplified by Kernel 2 applicable to MasterCard.

3.4.3 EMV Mode

For an EMV mode transaction, after the GET PROCESSING OPTIONS command, the Kernel continues with the following steps:

1. It determines which form of Offline Data Authentication to perform.
2. It reads the data records of the Card (using READ RECORD commands). If the same transaction involving the same Card is recognized in the Kernel’s internal log of torn transactions, then an attempt is made to recover the transaction – see section 3.7.
3. It performs Terminal Risk Management and Terminal Action Analysis, and selects a cardholder verification method for the transaction.
4. It requests an *Application Cryptogram* from the Card by issuing a GENERATE AC command. If a response is not received from the Card, the Kernel considers the transaction as “torn”, and stores the transaction details in its internal log of torn transactions, before terminating – see section 3.7.
5. It performs Offline Data Authentication as appropriate.



Processing of the outcome provided by the Kernel	The Kernel indicates whether a transaction is approved offline, declined offline, authorized online, or if another action is required.
--	--

EMV® Contactless Specifications for Payment Systems, Book C-2, Kernel 2 Specification, Version 2.7, April 2018

76. As explained below, the EMV-compliant merchant systems and devices request an application cryptogram from a transaction device (e.g., using the GENERATE AC Command), which may be for approving/denying the transaction, or for online approval, as exemplified by Kernel 2 applicable to Mastercard.

3.4.3 EMV Mode

For an EMV mode transaction, after the GET PROCESSING OPTIONS command, the Kernel continues with the following steps:

1. It determines which form of Offline Data Authentication to perform.
2. It reads the data records of the Card (using READ RECORD commands). If the same transaction involving the same Card is recognized in the Kernel's internal log of torn transactions, then an attempt is made to recover the transaction – see section 3.7.
3. It performs Terminal Risk Management and Terminal Action Analysis, and selects a cardholder verification method for the transaction.
4. It requests an *Application Cryptogram* from the Card by issuing a GENERATE AC command. If a response is not received from the Card, the Kernel considers the transaction as “torn”, and stores the transaction details in its internal log of torn transactions, before terminating – see section 3.7.
5. It performs Offline Data Authentication as appropriate.

5.4 Generate AC

5.4.1 Definition and Scope

The GENERATE AC command sends transaction-related data to the Card, which then computes and returns an *Application Cryptogram*. Depending on the risk management in the Card, the cryptogram returned by the Card may differ from that requested in the command message. The Card may return an AAC (transaction declined), an ARQC (online authorization request), or a TC (transaction approved).

Table 5.10—Generate AC Reference Control Parameter

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0							AAC
0	1							TC
1	0							ARQC

EMV® Contactless Specifications for Payment Systems, Book C-2, Kernel 2 Specification, Version 2.7, April 2018

77. As exemplified by Kernel 2, specific to Mastercard, the transaction device, at the direction of the terminal, determines a card action analysis result indicating at least one of approving the transaction offline, approving the transaction online, and denying the transaction.

78. The transaction device (e.g., Mastercard Card), at the direction of the terminal, transmits the card action analysis result, as exemplified by Kernel 2 applicable to Mastercard.

79. Based on the result of the merchant action analysis and the card action analysis, the terminal transmits an online processing request to the card issuer, as exemplified by Kernel 2 applicable to Mastercard.

A.1.117 Outcome Parameter Set

Tag: 'DF8129'
 Template: —
 Length: 8
 Format: b
 Update: K
 Description: This data object is used to indicate to the Terminal the outcome of the transaction processing by the Kernel. Its value is an accumulation of results about applicable parts of the transaction.

Outcome Parameter Set		
Byte 1	b8-5	Status
		0001: APPROVED
		0010: DECLINED
		0011: ONLINE REQUEST
		0100: END APPLICATION
		0101: SELECT NEXT
		0110: TRY ANOTHER INTERFACE
		0111: TRY AGAIN
		1111: N/A
		Other values: RFU
	b4-1	Each bit RFU

Online authorization and transaction logging	<p>The transaction may need to be authorized online. The Terminal sends the online authorization request to the issuer. Upon completion of the transaction, it stores the clearing record and prepares the batch file for submission to the acquirer.</p> <p>The authorization request and clearing record include different data depending on whether the transaction was completed in mag-stripe mode or EMV mode.</p>
--	--

EMV® Contactless Specifications for Payment Systems, Book C-2, Kernel 2 Specification, Version 2.7, April 2018 (emphasis added)

80. Once the terminal receives the Authorization Response, it will restart the Entry Point and determine whether to approve or decline the transaction, based on a Predetermined Rule and an Outcome from the First Merchant Action Analysis.

Requirements – Final Outcome Processing

8.1.1.21 If the Outcome parameter Removal Timeout has a value other than zero, then the reader shall start a timeout function using the value of the parameter and reset the timeout indicator to 0.

When the reader is informed by the terminal of the results of an online authorisation request, it shall stop the timeout function.

If the timeout occurs, the reader shall:

- Send a User Interface Request with the following parameters:
 - Message Identifier: '17' ("Card Read OK. Please Remove Card")
 - Status: Card Read Successfully
- Set the timeout indicator to 1.

Requirements – Online Response – Restart

The following requirement applies if the Outcome is Online Request and the retained Start parameter is any value other than 'N/A'.

8.1.1.22 If either of the following is true:

- the value of the Online Response Data parameter is 'Any',
- or the value of the Outcome parameter Online Response Data is 'EMV Data' and at least one of the following data elements is present:
 - Issuer Authentication Data (Tag '91')
 - Issuer Script Template (Tag '71', '72')

then the reader shall activate Entry Point at the Start indicated by the retained Start parameter.

6 Outcomes and Parameters

An Outcome is the primary instruction from the kernel or Entry Point on how processing should be continued. The parameters allow the kernel to indicate choices, such as messages to be displayed and whether the kernel wishes to be restarted after an online authorisation.

Start D	Kernel Activation	Activated by the reader to handle issuer responses after an Online Request Outcome with parameter Start = D.
----------------	-------------------	---

https://www.emvco.com/wp-content/uploads/2017/05/Book A Architecture and General Rqmts v2 6 Final_20160422011856105.pdf ; <https://www.emvco.com/wp-content/uploads/2017/05/BookB Entry Point Specification v2 6 20160809023257319.pdf>

Outcome	Description	Kernel	Entry Point	Reader/ Terminal
Approved	The kernel is satisfied that the transaction is acceptable with the selected contactless card application and wants the transaction to be approved. This is the expected Outcome for a successful offline transaction. This might also occur following reactivation of a kernel after an online response.	Creates Outcome, passes to Entry Point	<ul style="list-style-type: none"> • Processes selected Outcome parameters • Passes Outcome to reader as a Final Outcome 	Processes the Final Outcome
Declined	The kernel has found that the transaction is not acceptable with the selected contactless card application and wants the transaction to be declined. This might also occur following reactivation of a kernel after an online response.			
Online Request	The transaction requires an online authorisation to determine the approved or declined status. If the kernel wishes to be restarted when the response has been received (e.g. to receive issuer update data), then this is indicated in the parameters.			

EMV® Contactless Specifications for Payment Systems, Book A, Architecture and General Requirements, Version 2.6, March 2016

81. The Accused Instrumentalities of Defendants infringe at least claims of the '750 patent, which provide technological solutions and improvements for securing transactions, including using a transaction counter corresponding to the number of transactions conducted using a transaction device. Conventional systems and methods utilizing RFID transactions had a need to complete such transactions quickly. In exemplary embodiments, the '750 patent addresses this need by receiving at a merchant system a financial transaction request from a transaction device, where the request includes a transactions counted value. This value indicates a number of financial transactions performed using the transaction device. The request is forwarded to a transaction processor for approval or denial. A transaction is denied if the transactions counted value exceeds a maximum transactions value. In other exemplary embodiments, the '750 patent describes transmitting a financial transaction request from a Radio Frequency (RF) transaction device (e.g., a card or mobile wallet) to an RFID reader (e.g., a merchant system), and incrementing a transactions counted value at the RF transaction device.

82. Defendants infringe one or more claims of the '750 patent via Mastercard's directly and/or indirectly making, providing, and/or selling EMV compliant systems and devices to effect RF payment transactions (e.g., via at least one or more subsidiaries and/or brands), including acting on behalf of and/or directing and controlling third parties in connection with the use of those systems and/or devices. These POS systems and devices perform a method of securing RFID transactions, for example, with mobile wallets using host card emulation (e.g., Google Pay and Samsung Pay).

83. The MasterCard payment ecosystem effects RF payment transactions. MasterCard requires customers to conform to the EMV standards when effecting RF transactions. *See, e.g.*, evidence *supra* for the '671 patent relating to Mastercard requiring conformance to the EMV standards.

84. MasterCard supports host card emulation (HCE) based mobile wallets.

MasterCard Drives Host Card Emulation (HCE) Momentum with Mobile Payment Deployments in More than 15 Countries

Cloud-Based Projects in Key Markets around the Globe Enable Consumers to Make Contactless Payments from their NFC-enabled Phones

To tweet this news, copy and paste <http://news.mstr.cd/1DLjD4t> to your Twitter handle with the hashtags #HCE and #MobilePayments

PURCHASE, NY – February 24, 2015 – Consumers around the globe continue to use mobile devices rather than dip or swipe payments cards for more of their MasterCard purchases. In less than a year since announcing support for Host Card Emulation (HCE) and cloud-based software for both secure contactless and remote payment transactions, MasterCard today announced projects are currently underway in more than 15 countries. These projects provide consumers with more options for payment experiences across their Android devices.

<https://newsroom.mastercard.com/press-releases/mastercard-drives-host-card-emulation-hce-momentum-with-mobile-payment-deployments-in-more-than-15-countries/>

EMV

EMV stands for Europay, MasterCard, and Visa. It's the technical standard for payments using Smart Cards which are cards with an embedded chip. These cards can be contact cards that need to be inserted in a terminal or contactless cards that can be read using NFC technology. Google Pay payments are presented to the payment terminal as EMV contactless payments.

Google Pay Merchant Help: EMV, GOOGLE,

<https://support.google.com/pay/merchants/answer/7151369?hl=en> (last visited Oct. 12, 2023)

(emphasis added).

Field Communication (NFC) and Magnetic Secure Transmission (MST). MST is Samsung's innovative technology that delivers secure transactions for new EMV chip and NFC terminals, as well as traditional, magnetic strip terminals, enabling consumers to use

Samsung Pay Partners with Global POS Providers to Accelerate Mobile Payments Adoption, SAMSUNG, <https://news.samsung.com/us/samsung-pay-partners-global-pos-providers-accelerate-mobile-payments-adoption/> (April 19, 2016) (last visited Oct. 12, 2023) (emphasis added).

85. Further examples of Mastercard's EMV compliant POS systems and devices include Mastercard Mobile Point-of-Sale (MPOS) solutions that enable mobile devices to accept payments, including, but not limited to, Tap on Phone and Cloud Commerce, and services, for example, products, methods, and/or services for securing RFID transactions involving a PIC transaction device and/or mobile wallets using host card emulation (e.g., in connection with Google Pay and Samsung Pay mobile wallets). *See Mobile Point-of-Sale solutions (MPOS)*, MASTERCARD, <https://www.mastercard.com/global/en/business/overview/start-accepting/mobile-pos.html> (last visited Jan. 19, 2024).

86. When a MasterCard application stored in a mobile wallet (e.g., via Mastercard's mobile point-of-sale solutions) is brought into the proximity of EMV-compliant merchant reader (e.g., payment terminals), these readers receive a financial transaction request comprising an Application Cryptogram for an online authorization (ARQC) and a Token (tokenized Primary Account Number (PAN)). This is exemplified by Kernel 2 applicable to Mastercard.

87. The Application Cryptogram is encrypted using a Limited use Key (LUK) from the device. The LUK includes an Application Transaction Counter (ATC) which indicates the number of transactions performed by the RF transaction device at the time the LUK was generated.

88. A Mastercard application stored in a mobile wallet transmits the Application Cryptogram for online authorization (ARQC) and the Primary Account Number (PAN) to Mastercard. This is exemplified by Kernel 2 applicable to Mastercard.

89. The point-of-sale terminal (e.g., reader) receives a response to the transaction request from the issuer. The response may indicate that the issuer has declined the transaction due to thresholds of the LUK being exceeded, e.g., number of transactions indicated by ATC being more than 1 or some other number.

limited-use key

Basically, the limited-use key (LUK) - also called the [single-use key \(SUK\)](#) - is the password that joins the [token](#) with the actual card number, and, without it, the token can not be validated by the token service provider and matched to the actual card number to successfully complete a purchase. No other master key data is stored on the device. If the device is rebooted and has no network connection, it cannot decrypt LUKs / SUKs and, therefore, cannot be used for in-store transactions.

limited-use key, GOOGLE,

<https://support.google.com/pay/merchants/answer/7151225?hl=en>

(last visited Oct. 18, 2023) (emphasis added)

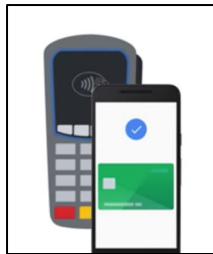
	LUK Parameters	Issuer available values for current	STIP Values for Current	Issuer available Valid values for previous	STIP Values for Previous	Comments
Must be the same across Wallets	TTL	15 days				Time to live in days after which replenishment will be triggered from the device
	<u>Number of Transactions (NOT)</u>	<u>15 transactions</u>				<u>NOT after which replenishment will be triggered from the device</u>

Figure 23 – LUK Configuration provided by VISA for Android Pay [29]

Visa, “Visa Europe Payment Token Service Android Pay Member Implementation Guide for Issuers,” Visa, 2016, reference available at: <https://www.royalholloway.ac.uk/media/5618/rhul-isg-2018-6-techreport-shanamicallef.pdf> (emphasis added)

providers. Typically, these would be the use of static PANs used solely for HCE apps and dynamic data for individual transactions, such as using limited-use session keys which are only valid for a single transaction (each application transaction counter [ATC] value), as allowed for within the existing EMV payment specifications. Also note, that session keys can be used with tokenised PANs. Either way, transaction-specific data (token or session keys) will need to be distributed and managed.

[https://www.gsma.com/digitalcommerce/wp-content/uploads/2014/11/GSMA-HCE-and-Tokenisation-for-Payment-Services-paper WEB.pdf](https://www.gsma.com/digitalcommerce/wp-content/uploads/2014/11/GSMA-HCE-and-Tokenisation-for-Payment-Services-paper_WEB.pdf) (emphasis added)



Google Help, YOUTUBE, <https://www.youtube.com/watch?v=Z5M5n8ZOBfg> (last visited Oct. 18, 2023)

Ms. Vasu: With Apple Pay it was a secure element implementation. And with the Android ecosystem, it is highly fragmented. In the case of Apple Pay, Apple owned the device, the operating system (OS) and they had full control over the real estate on the device. Whereas, with Android Pay, Google has more than 300 original equipment manufacturer partners. They have different partners who have control over the real estate, and to provision it on to the secure element is literally a struggle. So the shift in the industry was to move to a host card emulation where the token was provisioned in the cloud. But there are some security concerns as far as provisioning and keeping the credentials in the cloud. So even though it is a static token, the implementation model uses what is known as a limited use key. The limited use key is dynamic in nature, and it has certain parameters or thresholds like the number of transactions, the transaction amount, the usage, etc. So once these thresholds are reached, the token becomes invalid, until a new limited use key is sent back to the device. The token with the limited use key resides in the reloadable memory of the device, and that is how it gets protected, and that is how it is different from a secure element implementation.

Madhu Vasu, Senior Director, Innovation and Strategic Partnerships, Visa Inc, available at:

<https://www.kansascityfed.org/~media/files/publicat/pscp/2015/sessions/2015-psr-conf-session4-paneldiscussion.pdf?la=en> (emphasis added)

90. If the transaction is declined due to the LUK thresholds being exceeded, the terminal will deny the transaction request.

First Final Outcome	POS System Processing
<i>Online Request</i>	<ul style="list-style-type: none"> • The POS System advises the cardholder that an online transaction is in progress. An initial message to the cardholder might have been displayed as a result of the kernel including a User Interface Request with the Outcome. If a PIN CVM is required, then the message directs the cardholder to enter the PIN. • The terminal initiates an online authorisation request, using the data record provided with the Outcome. If the CVM is online PIN, then the terminal processes and submits the encrypted online PIN. • The terminal receives the online response or might determine that the request was unable to go online. • If the Start parameter was any value other than 'N/A', then: <ul style="list-style-type: none"> • The terminal makes available the transaction disposition in the online response together with all of the EMV TLV data elements present. • The reader reactivates Entry Point by continuing with 'Requirements – Online Response – Restart' on page 69. • <u>The terminal determines the transaction disposition, based on the online response indication (with Unable To Go Online a decline).</u> • The terminal advises the cardholder of the transaction outcome. • If a cardholder receipt is required, the terminal prints it or provides it electronically (e.g. email). • The terminal captures CVM signature or online PIN if requested. • The terminal prepares a clearing record if transaction disposition is "approved". • Once complete, continue with 'Requirements – New Transaction Preparation and Start' on page 64.

EMV® Contactless Specifications for Payment Systems, Book A, Architecture and General Requirements, Version 2.6, March 2016 (emphasis added)

Additionally, MasterCard and Visa modified their contactless specifications to support single/limited use keys and cloud cryptograms that recognize HCE tokens as valid payment credentials.⁷

Payment Strategies, FEDERAL RESERVE BANK OF BOSTON, <https://www.bostonfed.org/-/media/Documents/PaymentStrategies/understanding-the-role-of-host-card-emulation-in-mobile-wallets-brief-rmay-2016.pdf> (last visited Oct. 18, 2023)

91. The Accused Instrumentalities of Defendants infringe at least claims of the '039 patent. The '039 patent discloses that, at the time of the invention, there were problems with conducting transactions from remote locations (e.g., in connection with transactions conducted in taxis, by home delivery merchants, during concerts, at farmers markets, etc.) In such remote locations, means for the merchant to access financial institutions and obtain payment authorizations quickly were generally unavailable for the conventional systems at the time of the invention. For example, merchants would either manually or electronically record account numbers for a transaction instrument at the time of sale of goods or services and then would request authorization

at a later time, including after the customer or merchant had already left the point of sale. Merchants were also required to pay “card not present” fees, because of the higher risks associated with such transactions, which included fraudulent use of the customer’s account number.

92. To overcome these problems, the claims of ‘039 patent provide technological solutions and improvements addressing a merchant securely receiving immediate payment authorization for a customer’s transaction instrument at the point of sale in exchange for goods and services purchased by the customer. In exemplary embodiments, the ‘039 patent addresses the need to enable merchants to request and receive payment authorization at the point and time of sale of goods and services to the merchant’s customer. A query is sent by a computer-based system to a payment system directory that locates a candidate payment system for processing of a requested payment transaction by receipt of related payment information from a point-of-sale device. A payment authorization request is sent by the computer-based system to the identified candidate payment system. The computer-based system receives the payment authorization from the candidate payment system and sends it to the point-of-sale device.

93. The Accused Instrumentalities of Defendants infringe one or more claims of the ‘509 patent, which provide technological solutions and improvements for facilitating payment transactions. Conventional methods for payment transactions, particularly RFID transactions, had problems supporting multiple payment systems. The ‘509 patent discloses a computer-based system that queries a payment system directory and selects the appropriate payment system. The directory may contain algorithms or rules to allow the selection of a payment system based upon payment information, the type of transaction, or the transaction instrument issuer. Payment information may include a proxy account number. Once the payment system is selected, an authorization request with payment information is sent to the payment system. Payment authorization is received by the

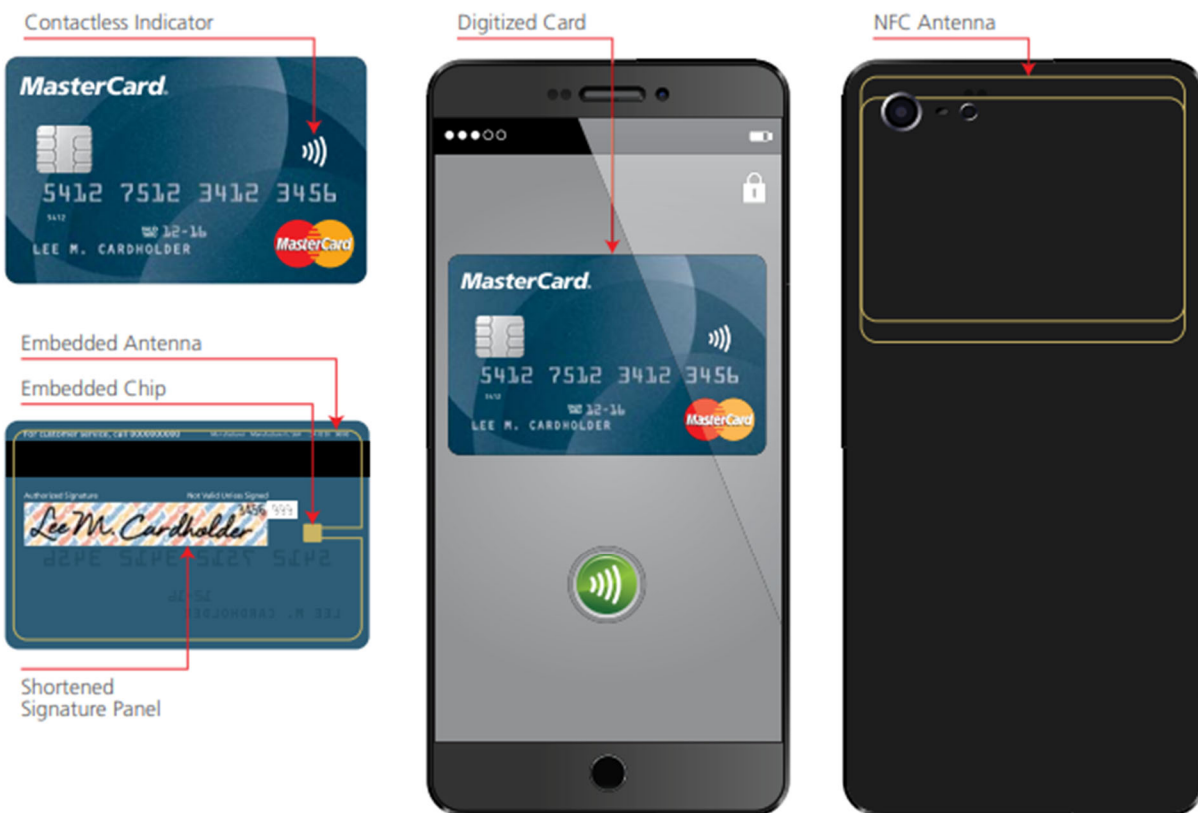
computer-based system. Systems and methods of the '509 patent, such as these, allow a payment system directory to identify a payment system that is mutually supported and appropriate for a particular transaction.

94. Defendants infringe one or more claims of each of the '039 patent and '509 patent by providing services and/or their computer-based systems (e.g., Mastercard contactless EMV cards, Mastercard's payment network, including without limitation products, methods, and/or services offered under various subsidiary and brand names) for transaction processing associated with Mastercard Transaction Instruments (e.g., Mastercard Cards), including, for example, via transactions conducted using an EMV payment application issued to a user and stored in a mobile wallet. Defendants also infringe one or more claims of each of the '039 patent and '509 patent via Defendants' action on behalf of and/or direction and control of third parties in connection with their activities including processing transactions associated with Mastercard Transaction Instruments (e.g., Mastercard Cards) using Mastercard's computer-based systems. Mastercard's services and computer-based systems include, without limitation, those advertised on Mastercard's website. As an example, Mastercard provides a complete set of credit and card issuance solutions for banks and financial institutions. *See, e.g., Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024); *Innovative, agile, secure, reliable*, MASTERCARD, <https://sea.mastercard.com/en-region-sea/business/issuers/products-and-solutions/payment-innovations/processing-solutions.html> (last visited Jan. 19, 2024); *Contactless Payments*, MASTERCARD, <https://www.mastercard.us/en-us/personal/ways-to-pay/contactless.html> (last visited Jan. 19, 2024).

95. The MasterCard payment ecosystem facilitates transactions at POS devices. MasterCard requires customers to conform to the EMV standards when effecting contactless chip

card and mobile wallet transactions. *See, e.g.*, evidence *supra* for the ‘671 patent relating to Mastercard requiring conformance to the EMV standards.

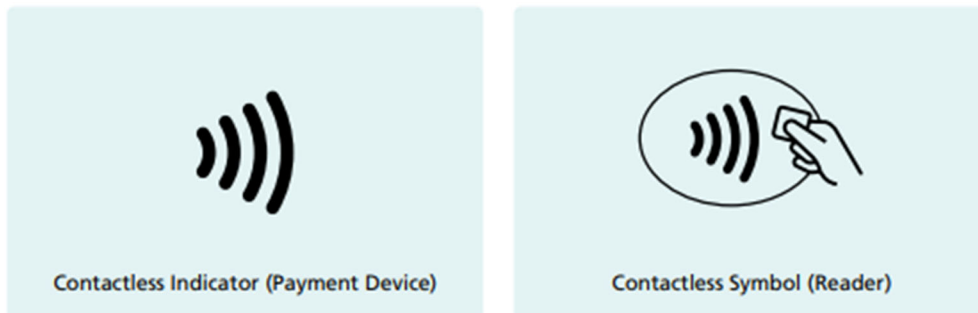
96. Mastercard also makes, sells, provides, issues and/or provisions EMV contactless cards (e.g., to and/or for financial institutions and/or in connection with mobile wallets). These EMV contactless cards comprise claimed systems and perform claimed methods of the ’039 patent and ’509 patent. For example, the EMV contactless cards perform the steps of claim 1 of the ’039 patent and claim 1 of the ’509 patent.



Contactless capability is denoted by the universal **Contactless Indicator** (see below) which is present on all contactless cards and form factors or should be displayed on the screen of contactless mobile devices.

A **Contactless Symbol** is present on all contactless readers to indicate compliance with EMV Contactless Communication Protocol, and the Contactless Symbol must be used to indicate the "read area" on the reader where the payment device should be tapped.

Any payment device with a Contactless Indicator will work on any reader with a Contactless Symbol. This global interoperable acceptance is an important part of the MasterCard contactless payment proposition



Contactless Toolkit for Issuers, MASTERCARD,

https://www.mastercard.com/contactless/doc/MC_Contactless_Toolkit_Issuers.pdf (last visited Jan. 19, 2024).

97. Mastercard also provisions EMV compliant payment applications for consumers' cards onto mobile wallets, including without limitation Google Pay and Samsung Pay. The mobile wallets perform the steps of claim 1 of the '039 patent and claim 1 of the '509 patent. *See, e.g., What is Push Provisioning and why does it matter?*, MASTERCARD, https://developer.mastercard.com/blog/what_is_push_provisioning/ (last visited Jan. 19, 2024); *MDES Token Connect*, MASTERCARD, <https://developer.mastercard.com/mdes-token-connect/documentation/> (last visited Jan. 19, 2024); *Google Pay Merchant Help: EMV*, GOOGLE, <https://support.google.com/pay/merchants/answer/7151369?hl=en> (last visited Oct. 12, 2023);

Samsung Pay Partners with Global POS Providers to Accelerate Mobile Payments Adoption, SAMSUNG, <https://news.samsung.com/us/samsung-pay-partners-global-pos-providers-accelerate-mobile-payments-adoption/> (April 19, 2016) (last visited Oct. 12, 2023).

98. In response to a command from a point-of-sale terminal, Defendants, via Mastercard’s computer-based system (e.g., at least a portion of and/or any combination of Mastercard’s payment products, systems, devices, Mastercard Transaction Instruments, and Mastercard Cards) that operates the payment application provisioned, at least in part, by Defendants, query an onboard payment system directory, as indicated below.

The basic functions of the POS System include:

- communication with contactless cards
- application selection and kernel activation

EMV® Contactless Specifications for Payment Systems, Book A, Architecture and General Requirements, Version 2.6, March 2016

99. Each transaction device may support one or more applications (payment systems), and each payment system is associated with an Application Identifier (AID). Examples of Mastercard AIDs are provided below.

COMPLETE LIST OF APPLICATION IDENTIFIERS (AID)					
List of AID's with their description.					
AID (Application Identifier)	Vendor	Country	Name	Description	Type
A00000000401	Mastercard International	United States	MasterCard PayPass	AEPM (Association Européenne Payez Mobile)	EMV
A0000000041010	Mastercard International	United States	MasterCard Credit/Debit (Global)	Standard MasterCard	EMV
A00000000410101213	Mastercard International	United States	MasterCard Credit	Standard MasterCard	EMV
A00000000410101215	Mastercard International	United States	MasterCard Credit	Standard MasterCard	EMV

<https://www.eftlab.com/knowledge-base/211-emv-aid-rid-pix/>

100. The payment application stored in a mobile wallet, for example, provides an identification of each supported candidate payment system, including without limitation Mastercard candidate payment systems, which Mastercard provides to purchasers and issuers via Mastercard's card payment products, methods, and/or services associated with Mastercard Transaction Instruments (e.g., Mastercard Cards) and to acquirers involved in transactions associated with Mastercard Transaction Instruments.

101. A Mastercard card application stored in a mobile wallet sends transaction information to the issuer bank, through the payment system, for authorization. The transaction information includes an online request (ARQC) and the PAN. This is exemplified by Kernel 2 applicable to MasterCard.

102. Mastercard stores a token, in a mobile wallet, in place of the PAN. For example, MasterCard requires that pass-through mobile wallets support tokenization.

9.2.6 Pass-through DWO Functional Requirements for Use on a Mobile Payment Device and Access Device

Each of the following, when required by the Corporation to be performed, must be performed in accordance with the Standards.

A Pass-through DWO must ensure that each Mobile Payment Device or Access Device used in connection with the Pass-through Digital Wallet can perform all of the following in accordance with the Corporation's minimum Standards:

1. Identification and Verification (ID&V), pursuant to a Token Implementation Plan deemed acceptable by the Corporation;

9.2.4 Pass-through DWO Tokenization

A Pass-through DWO must:

- Support a Mastercard Token; and
- Present a Mastercard Token if the Issuer, at the time of provisioning, Tokenized the Account.

<https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/mastercard-rules.pdf>

103. Mastercard payment applications (e.g., via Mastercard Transaction Instruments) transmit a payment authorization request through the payment system for online processing, as exemplified by Kernel 2 applicable to Mastercard.

5.4 Generate AC

5.4.1 Definition and Scope

The GENERATE AC command sends transaction-related data to the Card, which then computes and returns an *Application Cryptogram*. Depending on the risk management in the Card, the cryptogram returned by the Card may differ from that requested in the command message. The Card may return an AAC (transaction declined), an ARQC (online authorization request), or a TC (transaction approved).

EMV® Contactless Specifications for Payment Systems, Book C-2, Kernel 2 Specification, Version 2.7, April 2018

104. Mastercard Transaction Instruments (e.g., Mastercard applications stored in mobile wallets) receive authorization through the candidate payment system.

5.5.6 Transaction Disposition

The POS System is responsible for indicating the transaction disposition to the cardholder. The transaction disposition may be obtained directly from the Outcome (if **Approved** or **Declined**), or it may be necessary that an online authorisation be completed first. The manner of indication may be via a message, vending of goods, granting or denying access, or other functions.

An online authorisation will either result in a response with a Response Code and possible EMV TLV data, or will timeout and be considered as unable to go online.

In EMV mode environments, typical EMV TLV data elements that may be present are Authorisation Response Code (Tag '8A'), Issuer Authentication Data (Tag '91'), and Issuer Script Template (Tag '71', '72').

EMV® Contactless Specifications for Payment Systems, Book A, Architecture and General Requirements, Version 2.6, March 2016

105. Mastercard payment applications (e.g., via Mastercard Transaction Instruments) send the authorization (Transaction Certificate) to the POS terminal, as exemplified by Kernel 2 applicable to MasterCard.

5.4 Generate AC

5.4.1 Definition and Scope

The GENERATE AC command sends transaction-related data to the Card, which then computes and returns an *Application Cryptogram*. Depending on the risk management in the Card, the cryptogram returned by the Card may differ from that requested in the command message. The Card may return an AAC (transaction declined), an ARQC (online authorization request), or a TC (transaction approved).

Table 5.10—Generate AC Reference Control Parameter

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0							AAC
0	1							TC
1	0							ARQC

EMV® Contactless Specifications for Payment Systems, Book C-2, Kernel 2 Specification, Version 2.7, April 2018

106. The Accused Instrumentalities of Defendants infringe one or more claims of the '369 patent, which provide technological solutions and improvements for facilitating payment transactions. Conventional methods for payment transactions, particularly RFID transactions, had problems supporting multiple payment systems. In exemplary embodiments, the '369 patent provides systems and methods that can be used by smartcards, including contactless Mastercard Transaction Instruments (e.g., Mastercard Cards) and mobile wallets. The smartcard receives a payment request for a transaction. The smartcard determines a first payment system for processing the transaction, where such determination includes a query for payment directory information stored on the smartcard. The smartcard transmits to a point-of-sale device (POS) an identification of the payment system. The system and methods of the '369 patent, such as these, allow a payment system

directory to identify a payment system that is mutually supported and appropriate for a particular transaction.

107. Defendants infringe the '369 patent via their computer-based systems for transaction processing of Mastercard Transaction Instruments (e.g., Mastercard Cards), including Defendants' EMV payment application issued to a user and stored in a smartcard (e.g., a mobile wallet or contactless card). Defendants, by their own activities, on behalf of third parties, and/or via direction and control of third parties, provide contactless Mastercard Transaction Instruments (e.g., Mastercard Cards) and mobile wallet payment applications configured with smartcards that receive payment requests from POS terminals.

108. As an example, Mastercard provides a complete set of credit and card issuance solutions for banks and financial institutions. *See, e.g., Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024); *Innovative, agile, secure, reliable*, MASTERCARD, <https://sea.mastercard.com/en-region-sea/business/issuers/products-and-solutions/payment-innovations/processing-solutions.html> (last visited Jan. 19, 2024); *Contactless Payments*, MASTERCARD, <https://www.mastercard.us/en-us/personal/ways-to-pay/contactless.html> (last visited Jan. 19, 2024).

109. MasterCard requires customers to conform to the EMV standards when effecting chip card and mobile transactions. *See, e.g.,* evidence *supra* for the '671 patent relating to Mastercard requiring conformance to the EMV standards.

110. By their own actions, on behalf of third parties, and/or via direction and control of third parties, Defendants make, sell, provide, issue, and/or provision smartcards and also act on behalf of and/or direct and control the activities of third parties in connection with smartcards.

As an example, Mastercard provisions EMV compliant payment applications for consumers' cards onto mobile wallets, including without limitation Google Pay and Samsung Pay. *See, e.g., What is Push Provisioning and why does it matter?*, MASTERCARD, https://developer.mastercard.com/blog/what_is_push_provisioning/ (last visited Jan. 19, 2024); *MDES Token Connect*, MASTERCARD, <https://developer.mastercard.com/mdes-token-connect/documentation/> (last visited Jan. 19, 2024); *Google Pay Merchant Help: EMV*, GOOGLE, <https://support.google.com/pay/merchants/answer/7151369?hl=en> (last visited Oct. 12, 2023); *Samsung Pay Partners with Global POS Providers to Accelerate Mobile Payments Adoption*, SAMSUNG, <https://news.samsung.com/us/samsung-pay-partners-global-pos-providers-accelerate-mobile-payments-adoption/> (April 19, 2016) (last visited Oct. 12, 2023).

111. Mastercard Transaction Instruments receive payment requests from POS terminals, as exemplified by Kernel 2 specific to Mastercard. For example, in a Kernel 2 application (i.e., a Mastercard transaction) a card responds to an Application Cryptogram (AC) command from the terminal, as indicated below.

3.4.3 EMV Mode

For an EMV mode transaction, after the GET PROCESSING OPTIONS command, the Kernel continues with the following steps:

1. It determines which form of Offline Data Authentication to perform.
2. It reads the data records of the Card (using READ RECORD commands). If the same transaction involving the same Card is recognized in the Kernel's internal log of torn transactions, then an attempt is made to recover the transaction – see section 3.7.
3. It performs Terminal Risk Management and Terminal Action Analysis, and selects a cardholder verification method for the transaction.
4. It requests an Application Cryptogram from the Card by issuing a GENERATE AC command. If a response is not received from the Card, the Kernel considers the transaction as “torn”, and stores the transaction details in its internal log of torn transactions, before terminating – see section 3.7.
5. It performs Offline Data Authentication as appropriate.

EMV® Contactless Specifications for Payment Systems, Book C-2, Kernel 2 Specification, Version 2.7, April 2018 (emphasis added)

112. Mastercard Transaction Instruments (e.g., smartcards provided in contactless Mastercard Cards and in connection with mobile wallets) query an onboard payment system directory in response to a command from the POS terminal.

The basic functions of the POS System include:

- communication with contactless cards
- application selection and kernel activation

5.8.2 Application Selection and Kernel Activation

The selection mechanism is designed around the use of a PPSE. For multi-brand acceptance, this allows Entry Point to obtain all the available brands and applications with a single command and to make an immediate choice based on priority and kernel availability.

A PPSE response returned by a card contains one or more File Control Information (FCI) data elements forming a list of products supported by the card, the kernel they will run with, and their priority relative to one another.

Entry Point compares the ADF Names and Kernel Identifiers with the transaction type specific set of Combinations of AIDs and kernels that it supports for the given transaction type. The result is a list of Combinations, prioritised according to priority value or (for equal priority matches) by their order in the FCI list. AIDs and ADF Names can be obtained from the relevant payment system.

In the final selection, Entry Point picks the Combination with the highest priority, sends the SELECT AID command with the AID of this Combination, and hands over processing to the selected kernel. The Entry Point Pre-Processing Indicators for the relevant Combination are made available to the selected kernel.

Proximity Payment System Environment (PPSE)	A list of all Combinations supported by the contactless card. PPSE is used in the Entry Point Combination Selection process.
--	--

EMV® Contactless Specifications for Payment Systems, Book A,

Architecture and General Requirements, Version 2.6, March 2016

113. A Mastercard transaction device (e.g., contactless card or mobile wallet, via the smartcard) will transmit an identification of each supported payment system (e.g., application) in response to a command from the POS terminal. The identification is usable by the POS terminal.

114. As shown below, each transaction device may support one or more applications (payment systems), where each payment system is associated with an Application Identifier (AID).

2.2.1 Visa U.S. Common Debit AID and Customized Application Selection

All transactions initiated with a Visa owned Application Identifier (AID) other than the Visa U.S. Common Debit AID must be routed to VisaNet and be processed according to Visa or Visa Interlink (as applicable) network operating rules and technical standards. Some products may be personalized with more than one AID, where one or more AIDs may represent products with their own routing option(s), for instance the Visa U.S. Common Debit AID. To initiate a transaction using such an AID, certain terminal logic may need to be executed as part of the outlined VSDC transaction flow. This logic is described in Section 4.4.3.

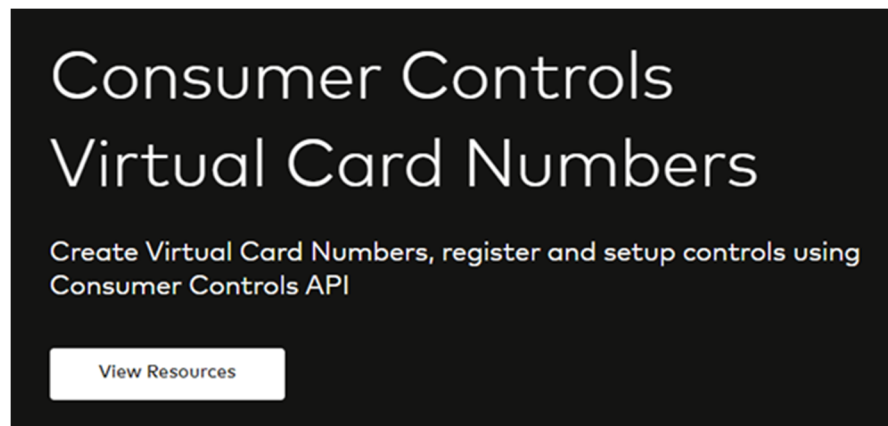
<https://www.visa.com/chip/merchants/grow-your-business/payment-technologies/credit-card-chip/docs/visa-emv-merchant-aig.pdf>

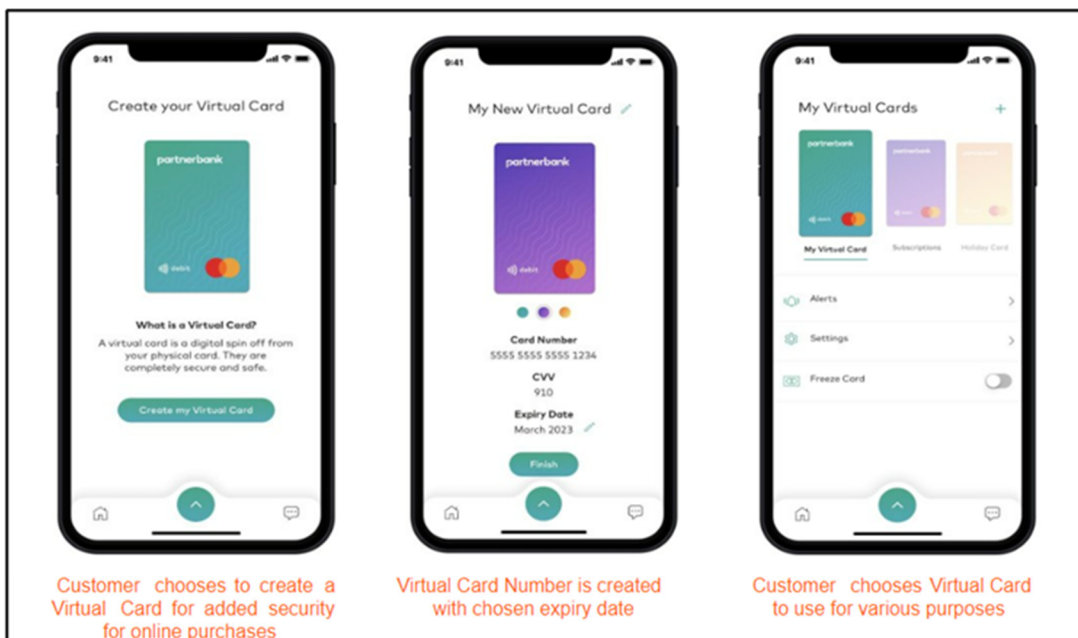
115. The Accused Instrumentalities of Defendants directly and/or indirectly infringe at least the claims of the '938 patent, which provide systems and methods that prevent card payment account numbers from being compromised, while also maximizing administrative efficiency. To do so, the '938 patent provides a mechanism to alter the card payment account number over the course of multiple transactions. Each new altered account number utilizes a different increment to make it difficult for a thief to predict what the new number will be, even if a prior account number was discovered. The account issuer also has the incremental values available in order to know what the current account number should be and associate the current account number with the particular cardholder. In one exemplary embodiment of the '938 patent, a computer-based system may replace a first portion of a first account code with data to create a second account code. A second portion of the second account code is associated with a second portion of the first account code. The second account may be used for a transaction. Such methods and systems of the '938 patent improve transaction security.

116. Claim 14 provides an example of how the methods and systems of the '938 patent provide technological innovations that can be used to enhance transaction security. Claim 14 of the '938 patent is directed to a computer-based solution for protecting a first account code by using the first account code to create a second account code that can be used for a transaction. *See* '938, 18:1-8, cl. 14. With conventional technology, the account number associated with a card is fixed when a

card is issued and does not change, although an existing card may be inactivated and replaced with another card, for example, if the card is lost or stolen. *See id.* at 18:9-20. These types of reactive measures, which address a threat after it is detected, may leave much to be desired in terms of transaction security. Advantageously, the invention of claim 14 facilitates more secure and proactive measures for protecting a card, for example, by enabling an account number to be changed from time to time during the life of the card, even after every transaction if so desired, while maintaining desired functionality of the card as a transaction device. *See id.* at 18:20-25.

117. As shown below, Defendants infringe the '938 patent by creating virtual account numbers, i.e., tokens, for accounts for Mastercard Cards and/or directing and controlling the actions of third parties (e.g., issuers of Mastercard Cards) in connection with the creation of these virtual account numbers.





<https://developer.mastercard.com/product/consumer-controls-virtual-card-numbers/>

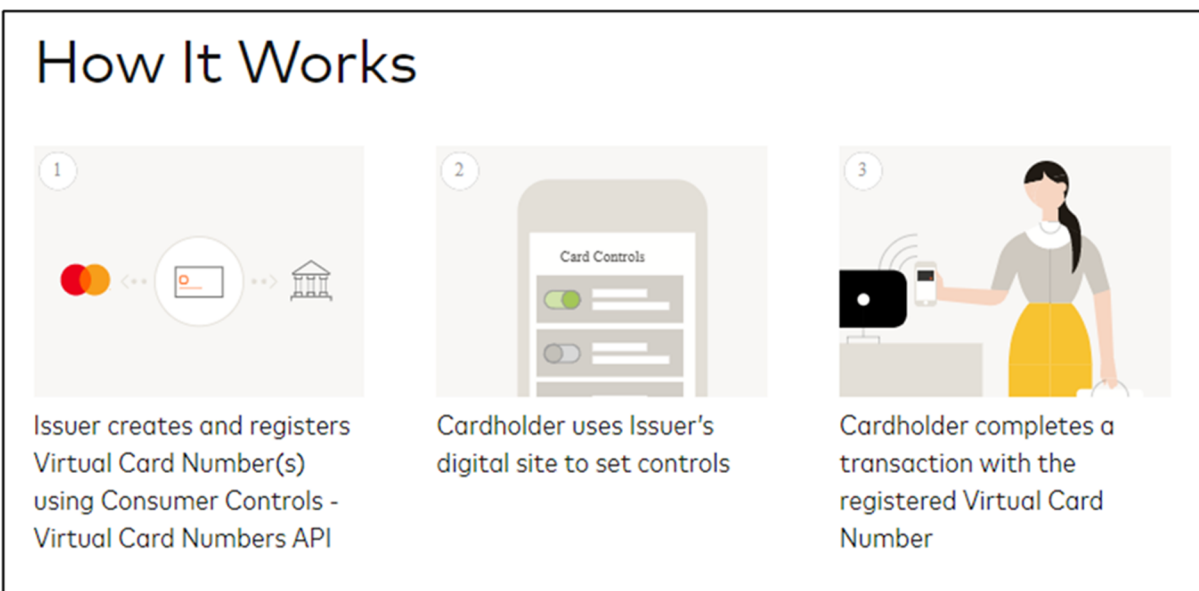
Issuer Identification Number (IIN)	The number that identifies the major industry and the card issuer and that forms the first part of the Primary Account Number (PAN)	ICC	n 6	'BF0C' or '73'	'42'	3
------------------------------------	---	-----	-----	----------------	------	---

https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_3_Application_Specification_20120607062110791.pdf

118. The virtual account numbers, created and utilized by Defendants’ Token Service, must begin with the same Issuer Identification Number (e.g., “second portion of the second account code”) as the primary account number (PAN) (i.e., the payment card number). The IIN identifies the card issuer and informs merchant systems to which payment network (i.e., Mastercard) to route transaction information.

119. Defendants provide these virtual account numbers to token requestors, including merchants and acquirers, who directly or indirectly “hold [the tokens] on file to initiate

transactions.” As illustrated by the example below, Mastercard virtual account numbers are used for transactions.



<https://developer.mastercard.com/product/consumer-controls-virtual-card-numbers/>

120. The Accused Instrumentalities of Defendants infringe one or more claims of the '207 patent, which provide technological solutions and improvements for processing a commercial transaction involving an authorization request from a merchant in response to a card payment request.

121. Conventional methods for payment transactions aimed at card transaction fraud were unsatisfactory, especially for online commerce (e.g., e-commerce). The increased risk of fraud with online and “card not present” transactions means that payment processors or providers historically may charge significantly higher rates for merchants engaging in online commerce, in some cases almost twice as much as the rates charged to “brick and mortar” merchants. Advantageously, the '207 patent provides systems and methods that can be used to authenticate the identity of a customer as the true cardholder, even when a card is not presented for payment. Among other benefits, to cardholders, merchants, and payment processors, this can reduce the risk of a card being used improperly. As described in exemplary embodiments of the '207 patent, a card payment

request is submitted to a merchant. A communication is initiated between a cardholder submitting the card payment request and an authorization computer of an issuer. An authorization request is received from the merchant in response to said card payment request, and an identity of the cardholder is authenticated using information received from the cardholder. The authentication includes matching the information received from the cardholder with a corresponding predetermined stored value and generating an authentication score representing a relative reliability of the identity of the cardholder based on the information from the cardholder. The authorization request is matched to the cardholder, the authorization request is authorized and, if the authorization request is approved, a private payment number is generated. Upon authorizing the authorization request, an authorization confirmation including the authorization score and the private payment number is issued to the merchant. Systems and methods of the '207 patent, such as these, advantageously address inadequacies found in conventional methods for securing e-commerce transactions.

122. Defendants infringe one or more claims of the '207 patent via Mastercard's offering 3-D Secure provider services, which practice a method for processing a commercial transaction that implements the EMV 3-D Secure specification.

What is EMV 3DS?

EMV 3DS is an e-commerce fraud prevention protocol that enables consumer authentication for CNP purchases, without adding unnecessary friction to the checkout process.

EMV® 3-D Secure, EMVCo, <https://www.emvco.com/emv-technologies/3-d-secure/> (last visited Oct. 18, 2023).

123. Mastercard Identity Check is a method for processing a commercial transaction that implements the EMV 3-D Secure specification.



<https://www.mastercard.us/en-us/business/overview/safety-and-security/identity-check.html>

Introduction to Identity Check and EMV 3-D Secure

Mastercard Identity Check is a global authentication program that utilizes the Mastercard authentication network in conjunction with the EMV 3-D Secure® protocol. It is designed to help provide additional security for digital transactions and to help facilitate higher approval rates, by improving the authentication experience for merchants, issuers, and cardholders.

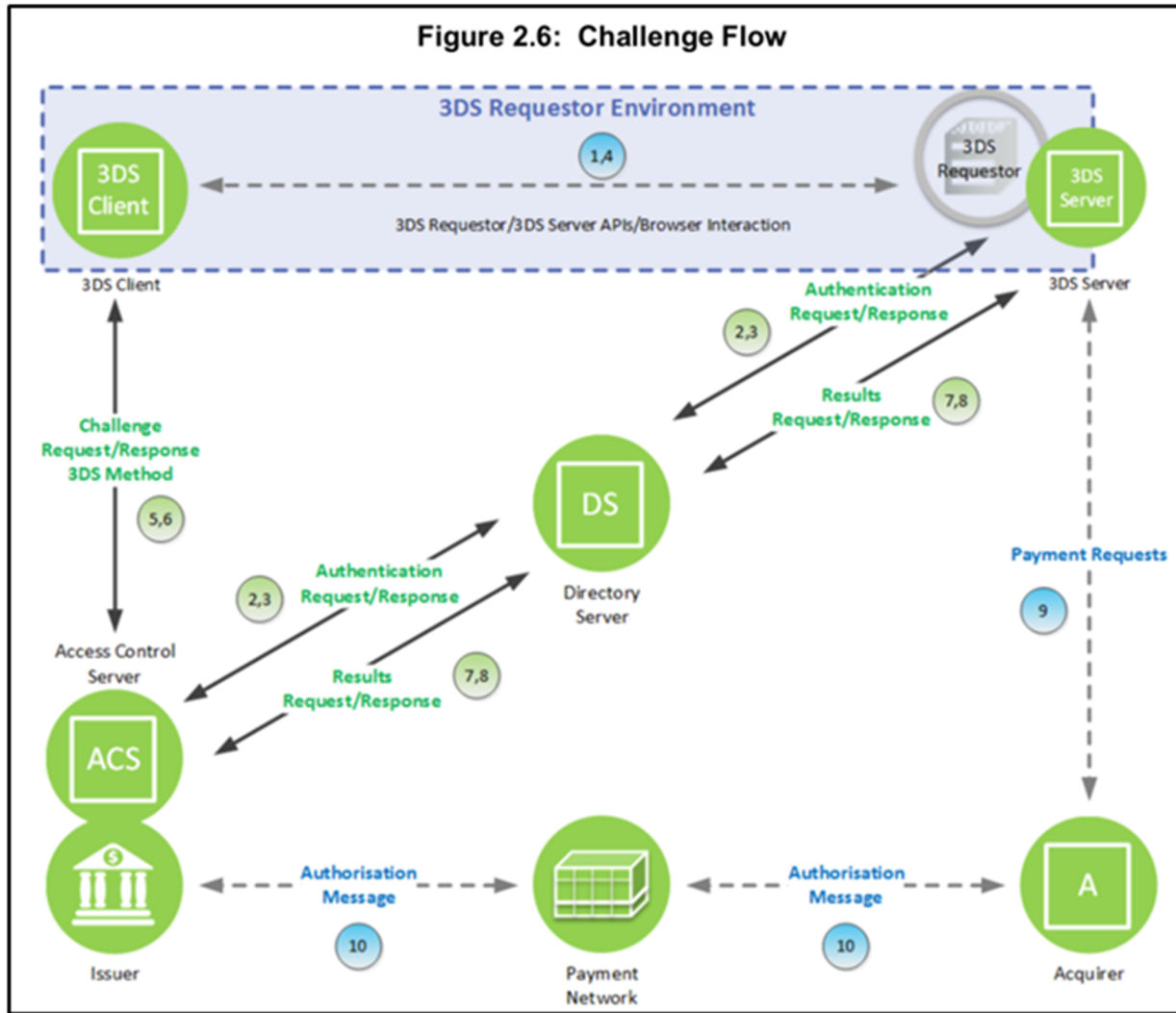
The purpose of this guide is to assist 3-D Secure Service Providers, Acquirers, and Merchants through the onboarding processes of program registration, testing, and production readiness. For more specifics regarding the Mastercard Identity Check program, please refer to *Mastercard Identity Check Program Guide* available on Mastercard Connect publication library.

<https://static.developer.mastercard.com/content/identity-check/uploads/files/mipts-manual.pdf>

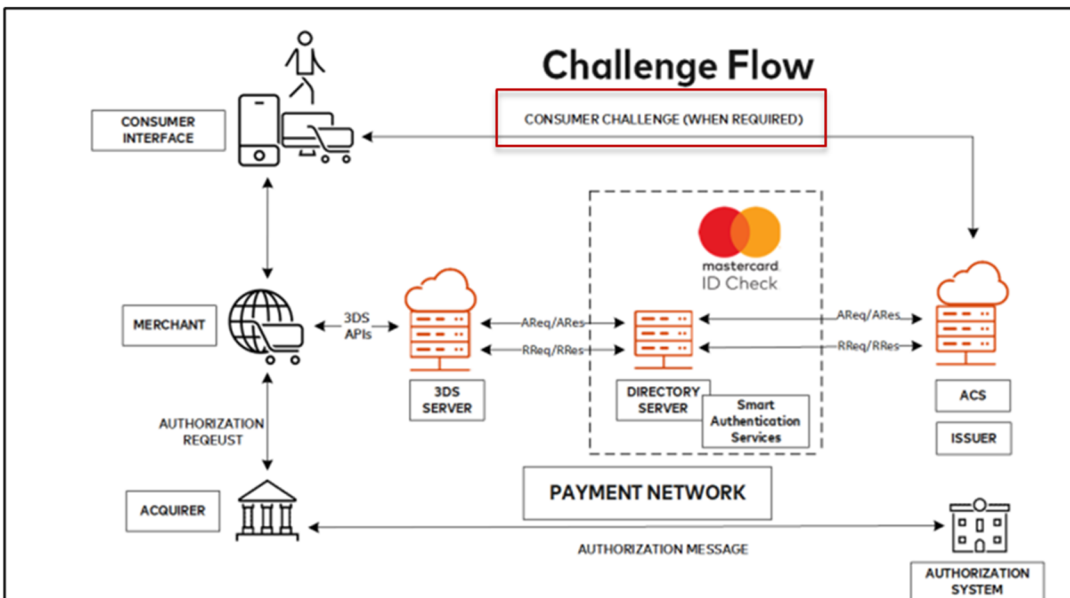
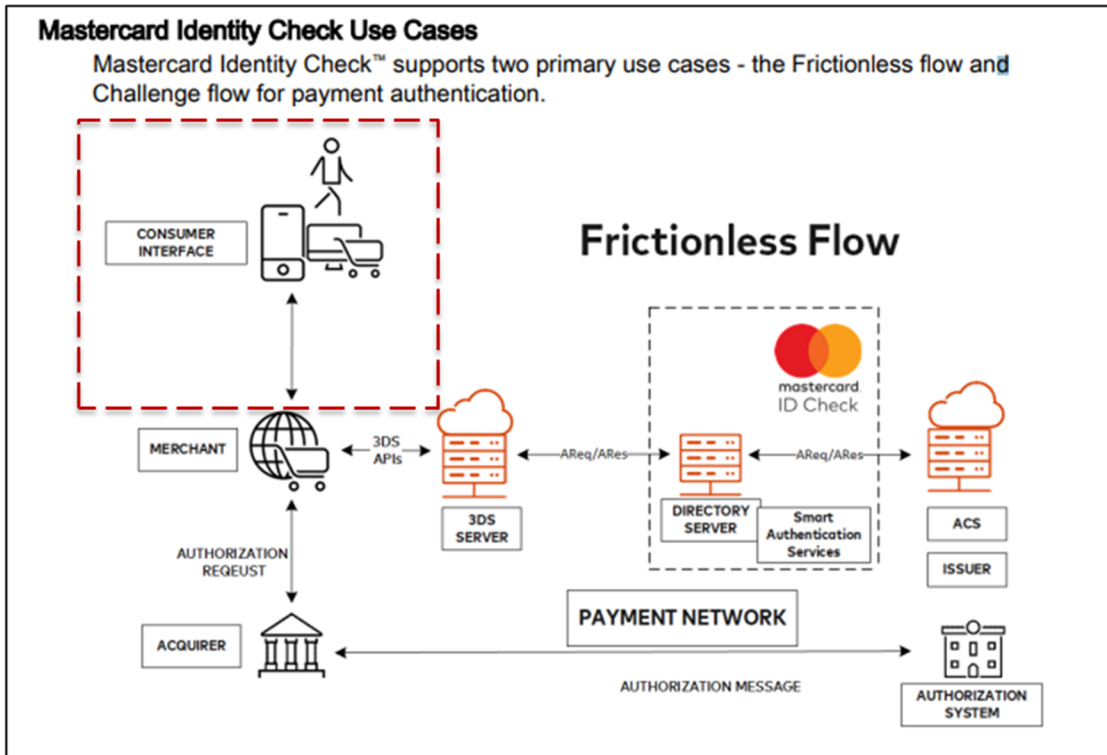
124. Mastercard also acts as the gateway and payment processor for its merchant customers.

125. As the merchant gateway, Mastercard receives a card payment request at the user's browser. For example, Mastercard's Identity Check Merchant Plug-in receives a card payment request at the user's browser, for submission to the merchant.

3DS Requestor	The initiator of the EMV 3-D Secure Authentication Request. For example, this may be a merchant or a digital wallet requesting authentication within a purchase flow.
---------------	---



EMV 3-D Secure: Protocol and Core Functions Specification, Version 2.1.0, October 2017



A Challenge/Step-up authentication flow demonstrates that the cardholder must perform additional steps such as entering a one-time pass code to successfully authenticate the transaction. Challenge flow is the same as a frictionless flow except that once the ACS issuer responds with the ARes message; it indicates that further interaction is required with the cardholder. This initiates a new set of messages, CReq and CRes between the 3-D Secure requestor and ACS/issuer where the challenge is performed. Then the ACS sends a RReq message to the 3-D Secure server through the DS, which responds with a RRes message to complete the transaction. Merchant and issuer then work together to complete the business as usual authorization flow.

<https://static.developer.mastercard.com/content/identity-check/uploads/files/mastercardidentitycheckprogram.pdf>

126. If 3DS authentication is selected for the transaction, Mastercard (e.g., via Mastercard Identity Check) initiates a communication between the cardholder and an ACS server of the issuing bank (e.g., via Mastercard's Directory Server).

127. Mastercard receives a transaction authorization request from the merchant. Mastercard (e.g., via the ACS Server) authenticates the identity of the cardholder by matching the information (e.g., a biometric) received from the cardholder or a response to another two-factor identification challenge, with stored information (e.g., a stored biometric or two-factor authentication code). The information may depend on a chosen authentication method.

IDENTITY CHECK MOBILE

Low-friction authentication when you really need it

- Two-factor authentication doesn't need to mean twice the work. Give your customers an intuitive and consistent experience to easily validate their identity without getting in the way.
- Get access to an all-in-one biometric solution that works across channels via facial, fingerprint, or voice recognition.
- We're always innovating for whatever comes next including additional authenticators, new protocols, and a changing digital landscape.
- APIs designed for flexibility in the environment that you need.

Before the payment: behavioral biometrics powered by NuDetect

- Funnels out automated attacks related to screen scraping, credit and gift card cycling and account cycling
- Analyzes behavioral data such as keystroke analysis, typing speed, deviations and pressure points to identify bad actors
- Leverage billions of data points to analyze in real time through machine learning

<https://www.mastercard.us/en-us/business/overview/safety-and-security/authentication-services/biometrics.html>
<https://www.mastercard.us/en-us/business/overview/safety-and-security/authentication-services/smart-interface.html>

- **Challenge Authentication** with one of the following approved challenge methods:
 - **Dynamic One-time Passcode** (by way of SMS, push notification, or mobile app)
 - **Biometric Fingerprint Match**
 - **Biometric Facial Recognition**

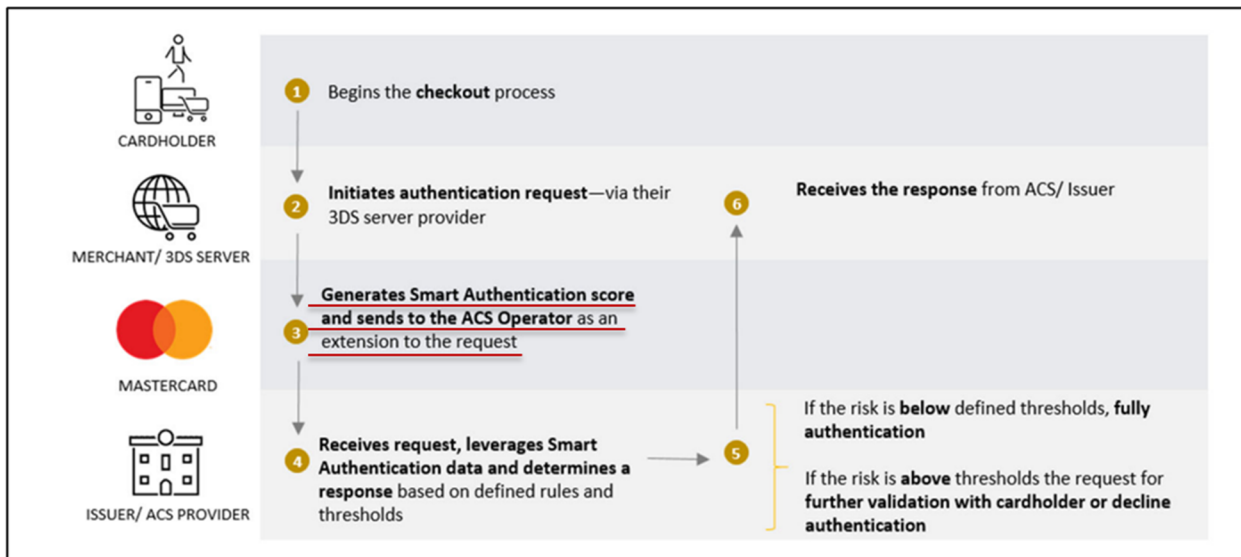
<https://static.developer.mastercard.com/content/identity-check/uploads/files/mastercardidentitycheckprogram.pdf>

128. The ACS Server matches the authorization request to the cardholder.

5. **3DS Client to ACS**—The 3DS Client initiates a CReq message based on information received in the ARes message. The manner in which this is done depends on the model:
 - **App-based**—A CReq message is formed by the 3DS SDK and is posted to the ACS URL received from the ARes message.
 - **Browser-based**—A CReq message is formed by the 3DS Server and is posted through the Cardholder's browser by the 3DS Requestor to the ACS URL received from the ARes message.
6. **ACS to 3DS Client**—The ACS receives the CReq message and interfaces with the 3DS Client to facilitate Cardholder interaction. The manner in which this is done depends on the model:
 - **App-based**—The ACS utilizes pairs of CReq and CRes messages to perform the challenge. In response to the CReq message, the CRes message requesting the Cardholder to enter the authentication data is formed by the ACS and sent to the 3DS SDK.
 - **Browser-based**—The ACS sends the authentication user interface to the Cardholder browser. The Cardholder enters the authentication data via the browser to be checked by the ACS. In response to the CReq message, the CRes message is formed by the ACS and sent to the 3DS Server to indicate the result of the authentication.

EMV 3-D Secure: Protocol and Core Functions Specification, Version 2.1.0, October 2017

129. Mastercard generates an authentication score that it places in the Transaction Status Reason message.



<https://static.developer.mastercard.com/content/identity-check/uploads/files/mastercardidentitycheckprogram.pdf>

Data Element/Field Name	Description	Source	Length/Format/Values	Device Channel	Message Category	Message Inclusion	Conditional Inclusion
Transaction Status Reason Field Name: transStatusReason	Provides information on why the Transaction Status field has the specified value.	ACS DS	Length: 2 characters JSON Data Type: String Values accepted: <ul style="list-style-type: none"> 01 = Card authentication failed 02 = Unknown Device 03 = Unsupported Device 04 = Exceeds authentication frequency limit 05 = Expired card 06 = Invalid card number 07 = Invalid transaction 08 = No Card record 09 = Security failure 10 = Stolen card 11 = Suspected fraud 12 = Transaction not permitted to cardholder 13 = Cardholder not enrolled in service 14 = Transaction timed out at the ACS 15 = Low confidence 16 = Medium confidence 17 = High confidence 18 = Very High confidence 19 = Exceeds ACS maximum challenges 	01-APP 02-BRW 03-3RI	01-PA 02-NPA	ARes = C RReq = C	For 01-PA, required if the Transaction Status field = N, U, or R. For 02-NPA, Conditional as defined by the DS.

EMV 3-D Secure: Protocol and Core Functions Specification, EMVCo, Version 2.1.0,

https://docs.3dsecure.io/3dsv2/_downloads/0b80f2e0693052852012f1151cde4f01/EMVCo_3DS_spec_v210.pdf (October 2017) (emphasis added).

130. MasterCard requires that online transactions be authorized by the Issuer. The authorization response must be accompanied by a transaction specific Authorization code.

5.1 Electronic Commerce Transactions

An electronic commerce ("e-commerce") Transaction must be authorized by the Issuer, in accordance with the authorization requirements described in Chapter 2. An e-commerce Transaction must not be effected using contactless payment functionality or as a purchase with cash back Transaction.

<https://www.mastercard.us/content/dam/mccom/en-us/documents/TPR-manual-June2015.pdf>

Authorization code

A six-digit alphanumeric code assigned by the issuer to identify the approval for a specific authorization request. Also referred to as "issuer's response code," "authorization approval code" or "authorization response code."

<https://www.mastercard.us/en-us/merchants/get-support/merchant-learning-center/glossary.html>

Merchant and Acquirer—The Merchant proceeds with authorisation exchange with its Acquirer. If appropriate, the Merchant, Acquirer, or Payment Processor can submit a standard authorisation request.

Payment Authorisation—The Acquirer can process an authorisation with the Issuer through the Payment System and return the authorisation results to the Merchant.

EMV 3-D Secure: Protocol and Core Functions Specification, Version 2.1.0, October 2017

131. If the authentication is successful and the Issuer does not otherwise decline the transaction, the issuer authorizes the transaction and sends an RReq message, containing the authorization score, to the merchant (3DS Server), as well as an Authorization code.

Data Element/Field Name	Description	Source	Length/Format/Values	Device Channel	Message Category	Message Inclusion	Conditional Inclusion
Transaction Status Reason Field Name: transStatusReason	Provides information on why the Transaction Status field has the specified value.	ACS DS	Length: 2 characters JSON Data Type: String Values accepted: <ul style="list-style-type: none"> 01 = Card authentication failed 02 = Unknown Device 03 = Unsupported Device 	01-APP 02-BRW 03-3RI	01-PA 02-NPA	ARes = C RReq = C	For 01-PA, required if the Transaction Status field = N, U, or R. For 02-NPA, Conditional as defined by the DS.

7. ACS through DS to 3DS Server—The ACS sends an RReq message that can include the Authentication Value (AV) to the DS, which then routes the message to the appropriate 3DS Server using the 3DS Server URL received from the AReq message.

EMV 3-D Secure: Protocol and Core Functions Specification, EMVCo, Version 2.1.0,

https://docs.3dsecure.io/3dsv2/_downloads/0b80f2e0693052852012f1151cde4f01/EMVCo_3DS_spec_v210.pdf (October 2017) (emphasis added).

Authorization response

An answer to an authorization request, which is typically a code that advises the acquirer or merchant on how to proceed with the transaction.

Authorization code

A six-digit alphanumeric code assigned by the issuer to identify the approval for a specific authorization request. Also referred to as "issuer's response code," "authorization approval code" or "authorization response code."

<https://www.mastercard.us/en-us/merchants/get-support/merchant-learning-center/glossary.html>

132. The Accused Instrumentalities of Defendants infringe at least the claims of the '101 patent, which provide methods and systems providing a privacy service for facilitating the auditing and control of privacy data. In the '101 patent, users provide their personal information (e.g., privacy data such as name, address, etc.) to a privacy service system. The user's privacy data is stored in a database associated with the privacy service. Users are allowed to audit the user's respective privacy data that is stored on the database. As part of a self-audit of the user's data, the user may be allowed to change the user's privacy data. The inventions disclosed in the '101 patent may be used for the early detection of various types of identity fraud. Users may utilize the disclosed privacy service systems to take appropriate actions, including notifying

various financial institutions of any identity fraud. Such appropriate actions in response to the detection of identity fraud may also be taken automatically by the privacy service system.

133. Defendants infringe the '101 patent by facilitating the self-auditing of first privacy data associated with a first user and second privacy data associated with as second user.

Profile	
First User	
Username	mincsulleysullivan Change Email Change Password
Email Address	mincsulleysullivan@gmail.com
First Privacy Data	
Name	Sulley Sullivan Change Profile Details
Company Name	MINC
Country of residence	UNITED STATES
Address	200 Crescent Court, Dallas,
Phone Number	2141234567
Notifications	You are not subscribed to receive emails about product updates and events Subscribe

Profile	
Second User	
Username	mincelliamae Change Email Change Password
Email Address	mincelliamae@gmail.com
Second Privacy Data	
Name	Celia Mae Change Profile Details
Company Name	MINC
Country of residence	UNITED STATES
Address	200 Crescent Court, Dallas,
Phone Number	2141234567
Notifications	You are not subscribed to receive emails about product updates and events Subscribe

<https://developer.mastercard.com/account/profile>

134. When a first user signs up for a MasterCard developer account, they're prompted to enter first privacy data in the form of an email address, which is subsequently collected by MasterCard.

135. First privacy data, such as the first user's email address, can be subsequently viewed on the "My Account" section of MasterCard's developer website. On information and belief, MasterCard stores privacy data in a central database.

136. When a second user signs up for a MasterCard developer account, they're prompted to enter second privacy data in the form of an email address, which is subsequently collected by MasterCard.

137. Second privacy data, such as the second user's email address, can be subsequently viewed on the "My Account" section of MasterCard's developer website. On information and belief, MasterCard stores privacy data in a central database.

138. A first user must log in to self audit their privacy data. When a first user logs in, the first user is only given access to information specific to their own account, and as such, are restricted from auditing the second privacy data.

139. When a first user navigates to the "My Account" section, audit information for the first privacy data that is retrieved and presented for review. For example, the email address the first user added to the account is displayed.

140. In the "My Account" section, the first user can change the first privacy data associated with the first user by selecting the "Change Email" option and entering a new email address. Further, a first privacy policy may be changed by selecting the "(Un)Subscribe" option to either subscribe or unsubscribe to receiving emails about product updates and events.

Profile

First User

Username mincsulleysullivan Change Email Change Password

Email Address mincsulleysullivan@gmail.com

First Privacy Data

Name Sulley Sullivan Change Profile Details

Company Name MINC

Country of residence UNITED STATES

Address 200 Crescent Court, Dallas,

Phone Number 2141234567

First Privacy Policy

Notifications You are not subscribed to receive emails about product updates and events Subscribe

Profile

First User

Username mincsulleysullivan Change Email Change Password

Email Address mincmikewazowski@gmail.com

Changed First Privacy Data

Name Sulley Sullivan Change Profile Details

Company Name MINC

Country of residence UNITED STATES

Address 200 Crescent Court, Dallas,

Phone Number 2141234567

Changed First Privacy Policy

Notifications You have opted in to receive emails about product updates and events Unsubscribe

<https://developer.mastercard.com/account/profile>

141. A second user must log in to self audit their privacy data. When a second user logs in, the second user is only given access to information specific to their own account, and as such, are restricted from auditing the first privacy data.

142. When a second user navigates to the “My Account” section, audit information for the second privacy data is retrieved and presented for review. For example, the email address the second user added to the account is displayed.

143. In the “My Account” section, the second user can change the second privacy data associated with the second user by selecting the “Change Email” option and entering a new email address. Further, a second privacy policy may be changed by selecting the “(Un)Subscribe” option to either subscribe or unsubscribe to receiving emails about product updates and events.

144. By performing the patented methods for transaction processing, the Accused Instrumentalities include products, methods, and/or services for offering, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from commercial transactions via Mastercard developer accounts, Mastercard Transaction Instruments (e.g., Mastercard Cards) and associated accounts that are covered by the Asserted Patents.

145. By utilizing EMV standards and performing the patented methods for transaction processing, the Accused Instrumentalities include Defendants’ products, methods, and/or services for offering, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from commercial transactions via Mastercard developer accounts, Mastercard Transaction Instruments (e.g., Mastercard Cards) and other associated accounts that are covered by the Asserted Patents. Furthermore, the Accused Instrumentalities include products, methods, and/or services for initiating secure communications between users of Defendants’ websites and Defendants’ web servers and for providing self-auditing features of users’ privacy data that are also covered by the Asserted Patents. Along with the above technology discussion, each respective Count below describes how the Accused Instrumentalities infringe on specific claims of the Asserted Patents.

COUNT I

(INFRINGEMENT OF U.S. PATENT NO. 8,851,369)

146. Plaintiff incorporates paragraphs 1 through 146 herein by reference.

147. Plaintiff is the assignee of the '369 patent, entitled "Systems and Methods for Transaction Processing Using a Smartcard," with ownership of all substantial rights in the '369 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

148. The '369 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '369 patent issued from U.S. Patent Application No. 12/505,164.

149. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '369 patent in this District and elsewhere in Florida and the United States.

150. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '369 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., Mastercard Transaction Instruments and/or Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

151. Defendants directly infringe, individually and/or jointly with at least one other entity, the '369 patent via 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '369 patent for and/or to, for example, its alter egos, agents, intermediaries, licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients. Defendants' infringement involves Defendants' own action and/or direction and control of third parties' actions.

152. Defendant MINC directly infringes the '369 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant MINT, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, developers, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '369 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, MINT, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

153. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners,

developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and/or consumers to perform one or more steps of the claimed methods of the '369 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) (“[A]n actor is liable for infringement under § 271(a) if it acts through an agent ... or contracts with another to perform one or more steps of a claimed method.”). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants’ cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants’ agreements with such third parties to provide access to Defendants’ products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants’ products, systems, methods, and/or services, for example, Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for contactless and mobile payments, as a condition of each third party’s access to, use of, and/or participation in such products, systems, methods, and/or services. *See id.* (“[L]iability under § 271(a) can also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance.”). The activities of each third party (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) in providing services to holders of Defendants’ Mastercard Transaction Instruments, cardholders of

Defendants' Mastercard Cards, and users of other products, systems, methods, and/or services are thus attributed to the Defendants such that Defendants become the "single actor" chargeable with the direct infringement.

154. In addition to the liability arising from the Defendants' relationship with third parties, Defendants also directly infringe, individually and/or jointly, the '369 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Mastercard Transaction Instruments and/or Mastercard Cards. On information and belief, Defendants design and develop payment applications for accounts used in connection with Mastercard Transaction Instruments and/or Mastercard Cards, which are used with physical Mastercard Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Find a Card*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview/cards.html> (last visited Jan. 22, 2024) (showing Mastercard offers payment solutions, for example, contactless payments and digital payments, and various cards including debit, credit, ATM, prepaid and gift cards); *EMV Technology at Work*, MASTERCARD, <https://sea.mastercard.com/en-region-sea/business/issuers/products-and-solutions/payment-innovations/chip-emv.html> (last visited Jan. 22, 2024) ("For 15 years, Mastercard has played a leading role in the creation, management and continued development of the EMV standard. We [Mastercard] offer a unique set of EMV solutions to help issuers and merchants implement new payment solutions quickly.").

155. For example, Defendants infringe claim 1 of the '369 patent via their Accused Instrumentalities that implement EMV standards to provide processing, authorization, clearing, and/or settlement services to Defendants' card issuer customers; and/or for mobile and/or

contactless payments, including Mastercard's contactless chip devices and technology provided to consumers via licenses with at least issuers, acquirers, chip vendors, and/or merchants. These services and devices and the technology utilized within them implement and perform methods pursuant to at least EMV standards, including without limitation standards that Mastercard utilizes and/or requires third parties to utilize. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Mastercard Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and/or use Mastercard's products, systems, devices and/or methods for the authorization and settlement of payment transactions. Defendants' mobile payments can be facilitated by Mastercard provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Mastercard Transaction Instruments and/or Mastercard Cards. Or such contactless payments can be facilitated by using contactless chips embedded on physical Mastercard Cards, for example, those provided, provisioned and/or issued by Mastercard. Defendants perform and/or direct and control infringement of the infringing products, systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, developers, merchants, customers, consumers, and/or clients, for the authorization of and settlement of these mobile or contactless payments conducted using Mastercard Cards.

156. The Accused Instrumentalities implement the method of claim 1 of the '369 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff's allegations that each of those limitations is met. For example, the Accused Instrumentalities include a method implementing the steps: receiving, at a smartcard, a payment request for a transaction; determining, by the smartcard, a first payment system for processing at

least a portion of the transaction, wherein said determining includes the smartcard querying payment directory information stored on the smartcard; and transmitting, by the smartcard, an identification of the first payment system to a point of service (POS) device, wherein the identification is usable by the POS device to transmit a first authorization request related to at least a portion of the transaction to the first payment system.

157. At a minimum, Defendants have known of the '369 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '369 patent on numerous occasions. For example, Defendants have known about the patent portfolio including the '369 patent, since at least March 15, 2018, when, via email, Colm J. Dobbyn (General Counsel, Intellectual Property, Mastercard) responded to email correspondence from a representative of Plaintiff affiliate Dominion Harbor Group, LLC ("DHG") that informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in acquisition discussions relating to Plaintiff's patent portfolio, and offered a phone call and email address to discuss the acquisition opportunity. At least as early as on or around October 11, 2018, Defendants were provided with access to a presentation and data room containing information related to the American Express patent portfolio and the '369 patent. On October 3, 2022, via email, DHG again requested a call to discuss an acquisition opportunity (e.g., licensing opportunity) for the American Express patent portfolio on behalf of Plaintiff and again provided access to a data room containing information related to the American Express patent portfolio and the '369 patent. The data rooms included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '369 patent.

158. On information and belief, since at least each of the above-mentioned dates when Defendants were on notice of their infringement, Defendants have actively induced, under U.S.C. § 271(b), intermediaries, distributors, suppliers, partners, developers, issuers, acquirers, merchants, customers, clients, consumers, and/or payment platforms (e.g., Samsung and Google mobile wallets) that distribute, make, purchase, offer to sell, sale, use, and/or service the Accused Instrumentalities to directly infringe one or more claims of the '369 patent by distributing, making, using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date and/or dates, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '369 patent. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, developers, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Mastercard Transaction Instruments and/or Mastercard Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction instruments with the payment applications, generating and installing cryptographic keys, and processing transactions; creating and/or maintaining established distribution channels for

the Accused Instrumentalities into and within the United States; manufacturing and designing, including without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing and/or inducing third parties to test Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., [mastercard.us](https://www.mastercard.us) and developer.mastercard.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, in the United States. *See, e.g., Find a credit card*, MASTERCARD, <https://www.mastercard.us/en-us/personal/find-card-products/index.php> (last visited Jan. 22, 2024) (advertising Mastercard's "most popular features and benefits," including rewards, cash back, travel / airline, 0% APR, low interest, and balance transfers, and stating "[f]ind a Mastercard from your favorite financial institution."); *Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024); *Contactless Toolkit for Issuers*, MASTERCARD, https://www.mastercard.com/contactless/doc/MC_Contactless_Toolkit_Issuers.pdf (last visited Jan. 19, 2024); *More than 50 years of payments experience combined with innovative technology*, MASTERCARD, <https://www.mastercard.us/en-us/business/issuers.html> (last visited Jan. 22, 2024) (advertising that Mastercard "work[s] with issuers of all sizes to create more efficient and secure ways to pay"); *Access to Capital*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview.html> (last visited Jan. 22, 2024) (indicating "[Mastercard] can help you access sources of capital so you can have more freedom and flexibility when it comes to building,

managing or growing your business,” and “Mastercard connects you to capital, technology, financial tools, partnerships and more to help grow and protect your business every step of the way.”).

159. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients to directly infringe via Mastercard’s developer resources and website (e.g., developer.mastercard.com), which includes APIs and invites developers to “[c]heck out our full product catalog.” *See developers, MASTERCARD, https://developer.mastercard.com/* (last visited Jan. 22, 2024).

160. On information and belief, despite having knowledge of the ‘369 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ‘369 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Defendants’ infringing activities relative to the ‘369 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

161. Plaintiff LPV has been damaged as a result of Defendants’ infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to LPV in an amount that adequately compensates LPV for Defendants’ infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT II

(INFRINGEMENT OF U.S. PATENT NO. 8,814,039)

162. Plaintiff incorporates paragraphs 1 through 162 herein by reference.

163. Plaintiff is the assignee of the '039 patent, entitled "Methods for Processing a Payment Authorization Request Utilizing a Network of Point-of-Sale Devices," with ownership of all substantial rights in the '039 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

164. The '039 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '039 patent issued from U.S. Patent Application No. 12/353,081.

165. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '039 patent in this District and elsewhere in Florida and the United States.

166. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '039 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., Mastercard Transaction Instruments and/or Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

167. Defendants directly infringe, individually and/or jointly with at least one other entity, the '039 patent via 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '039 patent for and/or to, for example, its alter egos, agents, intermediaries, licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients. Defendants' infringement involves Defendants' own action and/or direction and control of third parties' actions.

168. Defendant MINC directly infringes the '039 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant MINT, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, developers, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '039 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, MINT, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

169. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners,

developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and/or consumers to perform one or more steps of the claimed methods of the '039 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) (“[A]n actor is liable for infringement under § 271(a) if it acts through an agent ... or contracts with another to perform one or more steps of a claimed method.”). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants’ cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants’ agreements with such third parties to provide access to Defendants’ products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants’ products, systems, methods, and/or services, for example, Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for contactless and mobile payments, as a condition of each third party’s access to, use of, and/or participation in such products, systems, methods, and/or services. *See id.* (“[L]iability under § 271(a) can also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance.”). The activities of each third party (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) in providing services to holders of Defendants’ Mastercard Transaction Instruments, cardholders of

Defendants' Mastercard Cards, and users of other products, systems, methods, and/or services are thus attributed to the Defendants such that Defendants become the "single actor" chargeable with the direct infringement.

170. In addition to the liability arising from the Defendants' relationship with third parties, Defendants also directly infringe, individually and/or jointly, the '039 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Mastercard Transaction Instruments and/or Mastercard Cards. On information and belief, Defendants design and develop payment applications for accounts used in connection with Mastercard Transaction Instruments and/or Mastercard Cards, which are used with physical Mastercard Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Find a Card*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview/cards.html> (last visited Jan. 22, 2024) (showing Mastercard offers payment solutions, for example, contactless payments and digital payments, and various cards including debit, credit, ATM, prepaid and gift cards); *EMV Technology at Work*, MASTERCARD, <https://sea.mastercard.com/en-region-sea/business/issuers/products-and-solutions/payment-innovations/chip-emv.html> (last visited Jan. 22, 2024) ("For 15 years, Mastercard has played a leading role in the creation, management and continued development of the EMV standard. We [Mastercard] offer a unique set of EMV solutions to help issuers and merchants implement new payment solutions quickly.")

171. For example, Defendants infringe claim 1 of the '039 patent via their Accused Instrumentalities that implement EMV standards to provide tokenization, processing, authorization, clearing, and/or settlement services to Defendants' card issuer customers; and/or for mobile and/or

contactless payments, including Mastercard's contactless chip devices and technology provided to consumers via licenses with at least issuers, acquirers, chip vendors, and/or merchants. These services and devices and the technology utilized within them implement and perform methods pursuant to at least EMV standards, including without limitation standards that Mastercard utilizes and/or requires third parties to utilize. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Mastercard Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and/or use Mastercard's products, systems, devices and/or methods for the authorization and settlement of payment transactions. Defendants' mobile payments can be facilitated by Mastercard provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Mastercard Transaction Instruments and/or Mastercard Cards. Or such contactless payments can be facilitated by using contactless chips embedded on physical Mastercard Cards, for example, those provided, provisioned and/or issued by Mastercard. Defendants perform and/or direct and control infringement of the infringing products, systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, developers, merchants, customers, consumers, and/or clients, for the authorization of and settlement of these mobile or contactless payments conducted using Mastercard Cards.

172. The Accused Instrumentalities implement the method of claim 1 of the '039 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff's allegations that each of those limitations is met. For example, the Accused Instrumentalities include a method for facilitating a transaction at a first point of sale (POS) device, said method implementing the steps: sending a query from a computer based system to a payment

system directory, wherein the query includes a request to locate a candidate payment system that is configured to process at least a portion of said transaction, wherein said candidate payment system is configured to receive payment information related to said transaction at said first POS device; causing, by said computer based system, a payment authorization request related to said transaction to be transmitted from said first POS device to said candidate payment system; receiving, by said computer based system, payment authorization from said candidate payment system; and sending, by said computer based system, said payment authorization to said first POS device.

173. At a minimum, Defendants have known of the '039 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '039 patent on numerous occasions. For example, Defendants have known about the patent portfolio including the '039 patent, since at least March 15, 2018, when, via email, Colm J. Dobbyn (General Counsel, Intellectual Property, Mastercard) responded to email correspondence from a representative of Plaintiff affiliate Dominion Harbor Group, LLC ("DHG") that informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in acquisition discussions relating to Plaintiff's patent portfolio, and offered a phone call and email address to discuss the acquisition opportunity. At least as early as on or around October 11, 2018, Defendants were provided with access to a presentation and data room containing information related to the American Express patent portfolio and the '039 patent. On October 3, 2022, via email, DHG again requested a call to discuss an acquisition opportunity (e.g., licensing opportunity) for the American Express patent portfolio on behalf of Plaintiff and again provided access to a data room containing information related to the American Express patent portfolio and the '039 patent. The data rooms

included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '039 patent.

174. On information and belief, since at least each of the above-mentioned dates when Defendants were on notice of their infringement, Defendants have actively induced, under U.S.C. § 271(b), intermediaries, distributors, suppliers, partners, developers, issuers, acquirers, merchants, customers, clients, consumers, and/or payment platforms (e.g., Samsung and Google mobile wallets) that distribute, make, purchase, offer to sell, sale, use, and/or service the Accused Instrumentalities to directly infringe one or more claims of the '039 patent by distributing, making, using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date and/or dates, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '039 patent.

175. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, developers, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Mastercard Transaction Instruments and/or Mastercard Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing

transaction instruments with the payment applications, generating and installing cryptographic keys, and processing transactions; creating and/or maintaining established distribution channels for the Accused Instrumentalities into and within the United States; manufacturing and designing, including without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing and/or inducing third parties to test Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., [mastercard.us](https://www.mastercard.us) and developer.mastercard.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, in the United States. *See, e.g., Find a credit card*, MASTERCARD, <https://www.mastercard.us/en-us/personal/find-card-products/index.php> (last visited Jan. 22, 2024) (advertising Mastercard's "most popular features and benefits," including rewards, cash back, travel / airline, 0% APR, low interest, and balance transfers, and stating "[f]ind a Mastercard from your favorite financial institution."); *Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024); *Contactless Toolkit for Issuers*, MASTERCARD, https://www.mastercard.com/contactless/doc/MC_Contactless_Toolkit_Issuers.pdf (last visited Jan. 19, 2024); *More than 50 years of payments experience combined with innovative technology*, MASTERCARD, <https://www.mastercard.us/en-us/business/issuers.html> (last visited Jan. 22, 2024) (advertising that Mastercard "work[s] with issuers of all sizes to create more efficient and secure ways to pay"); *Access to Capital*, MASTERCARD, [**PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT** – Page 113](https://www.mastercard.us/en-</p></div><div data-bbox=)

us/business/overview.html (last visited Jan. 22, 2024) (indicating “[Mastercard] can help you access sources of capital so you can have more freedom and flexibility when it comes to building, managing or growing your business,” and “Mastercard connects you to capital, technology, financial tools, partnerships and more to help grow and protect your business every step of the way.”).

176. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients to directly infringe via Mastercard’s developer resources and website (e.g., developer.mastercard.com), which includes APIs and invites developers to “[c]heck out our full product catalog.” *See developers, MASTERCARD, https://developer.mastercard.com/* (last visited Jan. 22, 2024).

177. On information and belief, despite having knowledge of the ‘039 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ‘039 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Defendants’ infringing activities relative to the ‘039 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

178. Plaintiff LPV has been damaged as a result of Defendants’ infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to LPV in an amount that adequately compensates LPV for Defendants’ infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT III

(INFRINGEMENT OF U.S. PATENT NO. 8,794,509)

179. Plaintiff incorporates paragraphs 1 through 179 herein by reference.

180. Plaintiff is the assignee of the ‘509 patent, entitled “Systems and Methods for Processing a Payment Authorization Request Over Disparate Payment Networks,” with ownership of all substantial rights in the ‘509 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

181. The ‘509 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The ‘509 patent issued from U.S. Patent Application No. 12/353,109.

182. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the ‘509 patent in this District and elsewhere in Florida and the United States.

183. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the ‘509 patent, which includes Defendants’ offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., Mastercard Transaction Instruments and/or Mastercard Cards) and related products, methods, and/or services for Defendants’ licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, including Defendants’ issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants’ payment processing, authentication, authorization,

validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

184. Defendants directly infringe, individually and/or jointly with at least one other entity, the '509 patent via 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '509 patent for and/or to, for example, its alter egos, agents, intermediaries, licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients. Defendants' infringement involves Defendants' own action and/or direction and control of third parties' actions.

185. Defendant MINC directly infringes the '509 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant MINT, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, developers, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '509 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, MINT, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud

detection related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

186. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and/or consumers to perform one or more steps of the claimed methods of the '509 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) (“[A]n actor is liable for infringement under § 271(a) if it acts through an agent ... or contracts with another to perform one or more steps of a claimed method.”). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants' agreements with such third parties to provide access to Defendants' products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants' products, systems, methods, and/or services, for example, Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for contactless and mobile payments, as a condition of each third party's access to, use of, and/or participation in such products, systems, methods, and/or services. *See id.* (“[L]iability under § 271(a) can also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and

establishes the manner or timing of that performance.”). The activities of each third party (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) in providing services to holders of Defendants’ Mastercard Transaction Instruments, cardholders of Defendants’ Mastercard Cards, and users of other products, systems, methods, and/or services are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

187. In addition to the liability arising from the Defendants’ relationship with third parties, Defendants also directly infringe, individually and/or jointly, the ‘509 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Mastercard Transaction Instruments and/or Mastercard Cards. On information and belief, Defendants design and develop payment applications for accounts used in connection with Mastercard Transaction Instruments and/or Mastercard Cards, which are used with physical Mastercard Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Find a Card*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview/cards.html> (last visited Jan. 22, 2024) (showing Mastercard offers payment solutions, for example, contactless payments and digital payments, and various cards including debit, credit, ATM, prepaid and gift cards); *EMV Technology at Work*, MASTERCARD, <https://sea.mastercard.com/en-region-sea/business/issuers/products-and-solutions/payment-innovations/chip-emv.html> (last visited Jan. 22, 2024) (“For 15 years, Mastercard has played a leading role in the creation, management and

continued development of the EMV standard. We [Mastercard] offer a unique set of EMV solutions to help issuers and merchants implement new payment solutions quickly.”)

188. For example, Defendants infringe claim 1 of the ‘509 patent via their Accused Instrumentalities that implement EMV standards to provide tokenization, processing, authorization, clearing, and/or settlement services to Defendants’ card issuer customers; and/or for mobile and/or contactless payments, including Mastercard’s contactless chip devices and technology provided to consumers via licenses with at least issuers, acquirers, chip vendors, and/or merchants. These services and devices and the technology utilized within them implement and perform methods pursuant to at least EMV standards, including without limitation standards that Mastercard utilizes and/or requires third parties to utilize. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Mastercard Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and/or use Mastercard’s products, systems, devices and/or methods for the authorization and settlement of payment transactions. Defendants’ mobile payments can be facilitated by Mastercard provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Mastercard Transaction Instruments and/or Mastercard Cards. Defendants perform and/or direct and control infringement of the infringing products, systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, developers, merchants, customers, consumers, and/or clients, for the authorization of and settlement of these mobile or contactless payments conducted using Mastercard Cards.

189. The Accused Instrumentalities implement the method of claim 1 of the ‘509 patent. The technology discussion above and the example Accused Instrumentalities provide context for

Plaintiff's allegations that each of those limitations is met. For example, the Accused Instrumentalities include a method implementing the steps: querying, by a computer-based system configured to facilitate a transaction, a payment system directory, wherein said payment system directory communicates with said computer-based system, and wherein said payment system directory comprises information regarding a plurality of candidate payment systems, and wherein said payment system directory locates a candidate payment system for processing at least a portion of said transaction, wherein said candidate payment system receives payment information related to said transaction for developing a payment authorization, and wherein said payment information includes a proxy account number; transmitting, by said computer-based system, a payment authorization request related to said transaction to said candidate payment system; and receiving, by said computer-based system, said payment authorization from said candidate payment system.

190. At a minimum, Defendants have known of the '509 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '509 patent on numerous occasions. For example, Defendants have known about the patent portfolio including the '509 patent, since at least March 15, 2018, when, via email, Colm J. Dobbyn (General Counsel, Intellectual Property, Mastercard) responded to email correspondence from a representative of Plaintiff affiliate Dominion Harbor Group, LLC ("DHG") that informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in acquisition discussions relating to Plaintiff's patent portfolio, and offered a phone call and email address to discuss the acquisition opportunity. At least as early as on or around October 11, 2018, Defendants were provided with access to a presentation and data room containing information related to the American Express patent portfolio and the '509 patent. On October 3, 2022, via email, DHG again

requested a call to discuss an acquisition opportunity (e.g., licensing opportunity) for the American Express patent portfolio on behalf of Plaintiff and again provided access to a data room containing information related to the American Express patent portfolio and the '509 patent. The data rooms included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '509 patent.

191. On information and belief, since at least each of the above-mentioned dates when Defendants were on notice of their infringement, Defendants have actively induced, under U.S.C. § 271(b), intermediaries, distributors, suppliers, partners, developers, issuers, acquirers, merchants, customers, clients, consumers, and/or payment platforms (e.g., Samsung and Google mobile wallets) that distribute, make, purchase, offer to sell, sale, use, and/or service the Accused Instrumentalities to directly infringe one or more claims of the '509 patent by distributing, making, using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date and/or dates, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '509 patent.

192. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, developers, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Mastercard Transaction Instruments and/or Mastercard Cards, providing EMV payment applications, related tokens, and

virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction instruments with the payment applications, generating and installing cryptographic keys, and processing transactions; creating and/or maintaining established distribution channels for the Accused Instrumentalities into and within the United States; manufacturing and designing, including without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing and/or inducing third parties to test Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., [mastercard.us](https://www.mastercard.us) and developer.mastercard.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, in the United States. *See, e.g., Find a credit card*, MASTERCARD, <https://www.mastercard.us/en-us/personal/find-card-products/index.php> (last visited Jan. 22, 2024) (advertising Mastercard's "most popular features and benefits," including rewards, cash back, travel / airline, 0% APR, low interest, and balance transfers, and stating "[f]ind a Mastercard from your favorite financial institution."); *Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024); *Contactless Toolkit for Issuers*, MASTERCARD, https://www.mastercard.com/contactless/doc/MC_Contactless_Toolkit_Issuers.pdf (last visited Jan. 19, 2024); *More than 50 years of payments experience combined with innovative technology*,

MASTERCARD, <https://www.mastercard.us/en-us/business/issuers.html> (last visited Jan. 22, 2024) (advertising that Mastercard “work[s] with issuers of all sizes to create more efficient and secure ways to pay”); *Access to Capital*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview.html> (last visited Jan. 22, 2024) (indicating “[Mastercard] can help you access sources of capital so you can have more freedom and flexibility when it comes to building, managing or growing your business,” and “Mastercard connects you to capital, technology, financial tools, partnerships and more to help grow and protect your business every step of the way.”).

193. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients to directly infringe via Mastercard’s developer resources and website (e.g., developer.mastercard.com), which includes APIs and invites developers to “[c]heck out our full product catalog.” *See developers*, MASTERCARD, <https://developer.mastercard.com/> (last visited Jan. 22, 2024).

194. On information and belief, despite having knowledge of the ‘509 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ‘509 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Defendants’ infringing activities relative to the ‘509 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

195. Plaintiff LPV has been damaged as a result of Defendants’ infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to LPV in an amount

that adequately compensates LPV for Defendants' infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT IV

(INFRINGEMENT OF U.S. PATENT NO. 7,953,671)

196. Plaintiff incorporates paragraphs 1 through 196 herein by reference.

197. Plaintiff is the assignee of the '671 patent, entitled "Methods and Apparatus for Conducting Electronic Transactions," with ownership of all substantial rights in the '671 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

198. The '671 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '671 patent issued from U.S. Patent Application No. 12/275,924.

199. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '671 patent in this District and elsewhere in Florida and the United States.

200. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '671 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., Mastercard Transaction Instruments and/or Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, including

Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

201. Defendants directly infringe, individually and/or jointly with at least one other entity, the '671 patent via 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '671 patent for and/or to, for example, its alter egos, agents, intermediaries, licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients. Defendants' infringement involves Defendants' own action and/or direction and control of third parties' actions.

202. Defendant MINC directly infringes the '671 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant MINT, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, developers, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '671 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, MINT provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing,

issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

203. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and/or consumers to perform one or more steps of the claimed methods of the '671 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) (“[A]n actor is liable for infringement under § 271(a) if it acts through an agent ... or contracts with another to perform one or more steps of a claimed method.”). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants' agreements with such third parties to provide access to Defendants' products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants' products, systems, methods, and/or services, for example, Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for contactless and mobile payments, as a condition of each third party's access to, use of, and/or participation in such products, systems, methods, and/or services. *See id.* (“[L]iability under § 271(a) can also be found when an alleged infringer conditions participation in

an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance.”). The activities of each third party (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) in providing services to holders of Defendants’ Mastercard Transaction Instruments, cardholders of Defendants’ Mastercard Cards, and users of other products, systems, methods, and/or services are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

204. In addition to the liability arising from the Defendants’ relationship with third parties, Defendants also directly infringe, individually and/or jointly, the ‘671 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Mastercard Transaction Instruments and/or Mastercard Cards. On information and belief, Defendants design and develop payment applications for accounts used in connection with Mastercard Transaction Instruments and/or Mastercard Cards, which are used with physical Mastercard Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Find a Card*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview/cards.html> (last visited Jan. 22, 2024) (showing Mastercard offers payment solutions, for example, contactless payments and digital payments, and various cards including debit, credit, ATM, prepaid and gift cards); *EMV Technology at Work*, MASTERCARD, <https://sea.mastercard.com/en-region-sea/business/issuers/products-and-solutions/payment-innovations/chip-emv.html> (last visited Jan. 22, 2024) (“For 15 years, Mastercard has played a leading role in the creation, management and

continued development of the EMV standard. We [Mastercard] offer a unique set of EMV solutions to help issuers and merchants implement new payment solutions quickly.”)

205. For example, Defendants infringe claim 1 of the ‘671 patent via their Accused Instrumentalities that implement EMV standards to provide tokenization, processing, authorization, clearing, and/or settlement services to Defendants’ card issuer customers; and/or for mobile and/or contactless payments, including Mastercard’s contactless chip devices and technology provided to consumers via licenses with at least issuers, acquirers, chip vendors, and/or merchants. These services and devices and the technology utilized within them implement and perform methods pursuant to at least EMV standards, including without limitation standards that Mastercard utilizes and/or requires third parties to utilize. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Mastercard Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and/or use Mastercard’s products, systems, devices and/or methods for the authorization and settlement of payment transactions. Defendants’ mobile payments can be facilitated by Mastercard provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Mastercard Transaction Instruments and/or Mastercard Cards. Defendants perform and/or direct and control infringement of the infringing products, systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, developers, merchants, customers, consumers, and/or clients, for the authorization of and settlement of these mobile or contactless payments conducted using Mastercard Cards.

206. The Accused Instrumentalities implement the method of claim 1 of the ‘671 patent. The technology discussion above and the example Accused Instrumentalities provide context for

Plaintiff's allegations that each of those limitations is met. For example, the Accused Instrumentalities include a method implementing the steps: forwarding, by a computer-based system for conducting a transaction, a challenge to an intelligent token of a client, wherein said intelligent token generates a challenge response, and wherein said computer-based system comprises a processor and a non-transitory memory; receiving, by said computer-based system, said challenge response; assembling, by said computer-based system, credentials for a transaction in response to verifying said challenge response, wherein said assembled credentials include a key; receiving, by said computer-based system, a request from said client, wherein said request includes at least a portion of said assembled credentials provided to said client; validating, by said computer-based system, said portion of said assembled credentials with said key of said assembled credentials; and, providing, by said computer-based system, access to a transaction service in response to said validating.

207. At a minimum, Defendants have known of the '671 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '671 patent on numerous occasions. For example, Defendants have known about the patent portfolio including the '671 patent, since at least March 15, 2018, when, via email, Colm J. Dobbyn (General Counsel, Intellectual Property, Mastercard) responded to email correspondence from a representative of Plaintiff affiliate Dominion Harbor Group, LLC ("DHG") that informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in acquisition discussions relating to Plaintiff's patent portfolio, and offered a phone call and email address to discuss the acquisition opportunity. At least as early as on or around October 11, 2018, Defendants were provided with access to a presentation and data room containing information related to the

American Express patent portfolio and the '671 patent. On October 3, 2022, via email, DHG again requested a call to discuss an acquisition opportunity (e.g., licensing opportunity) for the American Express patent portfolio on behalf of Plaintiff and again provided access to a data room containing information related to the American Express patent portfolio and the '671 patent. The data rooms included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '671 patent.

208. On information and belief, since at least each of the above-mentioned dates when Defendants were on notice of their infringement, Defendants have actively induced, under U.S.C. § 271(b), intermediaries, distributors, suppliers, partners, developers, issuers, acquirers, merchants, customers, clients, consumers, and/or payment platforms (e.g., Samsung and Google mobile wallets) that distribute, make, purchase, offer to sell, sale, use, and/or service the Accused Instrumentalities to directly infringe one or more claims of the '671 patent by distributing, making, using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date and/or dates, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '671 patent.

209. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, developers, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Mastercard Transaction

Instruments and/or Mastercard Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction instruments with the payment applications, generating and installing cryptographic keys, and processing transactions; creating and/or maintaining established distribution channels for the Accused Instrumentalities into and within the United States; manufacturing and designing, including without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing and/or inducing third parties to test Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., [mastercard.us](https://www.mastercard.us) and developer.mastercard.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, in the United States. *See, e.g., Find a credit card*, MASTERCARD, <https://www.mastercard.us/en-us/personal/find-card-products/index.php> (last visited Jan. 22, 2024) (advertising Mastercard's "most popular features and benefits," including rewards, cash back, travel / airline, 0% APR, low interest, and balance transfers, and stating "[f]ind a Mastercard from your favorite financial institution."); *Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024); *Contactless Toolkit for Issuers*, MASTERCARD, https://www.mastercard.com/contactless/doc/MC_Contactless_Toolkit_Issuers.pdf (last visited

Jan. 19, 2024); *More than 50 years of payments experience combined with innovative technology*, MASTERCARD, <https://www.mastercard.us/en-us/business/issuers.html> (last visited Jan. 22, 2024) (advertising that Mastercard “work[s] with issuers of all sizes to create more efficient and secure ways to pay”); *Access to Capital*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview.html> (last visited Jan. 22, 2024) (indicating “[Mastercard] can help you access sources of capital so you can have more freedom and flexibility when it comes to building, managing or growing your business,” and “Mastercard connects you to capital, technology, financial tools, partnerships and more to help grow and protect your business every step of the way.”).

210. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients to directly infringe via Mastercard’s developer resources and website (e.g., developer.mastercard.com), which includes APIs and invites developers to “[c]heck out our full product catalog.” *See developers*, MASTERCARD, <https://developer.mastercard.com/> (last visited Jan. 22, 2024).

211. On information and belief, despite having knowledge of the ‘671 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ‘671 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Defendants’ infringing activities relative to the ‘671 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

212. Plaintiff LPV has been damaged as a result of Defendants' infringing conduct described in this Count. Each Defendant is thus, jointly, and severally, liable to LPV in an amount that adequately compensates LPV for Defendants' infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT V

(INFRINGEMENT OF U.S. PATENT NO. 9,195,985)

213. Plaintiff incorporates paragraphs 1 through 213 herein by reference.

214. Plaintiff is the assignee of the '985 patent, entitled "Method, System, and Computer Program Product for Customer-Level Data Verification," with ownership of all substantial rights in the '985 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

215. The '985 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '985 patent issued from U.S. Patent Application No. US 11/448/767.

216. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '985 patent in this District and elsewhere in Florida and the United States.

217. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '985 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., Mastercard Transaction Instruments and/or

Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

218. Defendants directly infringe, individually and/or jointly with at least one other entity, the '985 patent via 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '985 patent for and/or to, for example, its alter egos, agents, intermediaries, licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients. Defendants' infringement involves Defendants' own action and/or direction and control of third parties' actions.

219. Defendant MINC directly infringes the '985 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant MINT, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, developers, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '985 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, MINT, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees,

issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

220. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and/or consumers to perform one or more steps of the claimed methods of the '985 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) (“[A]n actor is liable for infringement under § 271(a) if it acts through an agent ... or contracts with another to perform one or more steps of a claimed method.”). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants' agreements with such third parties to provide access to Defendants' products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants' products, systems, methods, and/or services, for example, Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for contactless and mobile payments, as a condition of each third party's

access to, use of, and/or participation in such products, systems, methods, and/or services. *See id.* (“[L]iability under § 271(a) can also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance.”). The activities of each third party (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) in providing services to holders of Defendants’ Mastercard Transaction Instruments, cardholders of Defendants’ Mastercard Cards, and users of other products, systems, methods, and/or services are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

221. In addition to the liability arising from the Defendants’ relationship with third parties, Defendants also directly infringe, individually and/or jointly, the ‘985 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Mastercard Transaction Instruments and/or Mastercard Cards. On information and belief, Defendants design and develop payment applications for accounts used in connection with Mastercard Transaction Instruments and/or Mastercard Cards used with digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Find a Card*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview/cards.html> (last visited Jan. 22, 2024) (showing Mastercard offers payment solutions, for example, contactless payments and digital payments, and various cards including debit, credit, ATM, prepaid and gift cards); *EMV Technology at Work*, MASTERCARD, <https://sea.mastercard.com/en-region-sea/business/issuers/products-and->

solutions/payment-innovations/chip-emv.html (last visited Jan. 22, 2024) (“For 15 years, Mastercard has played a leading role in the creation, management and continued development of the EMV standard. We [Mastercard] offer a unique set of EMV solutions to help issuers and merchants implement new payment solutions quickly.”)

222. For example, Defendants infringe claim 1 of the ‘985 patent via their Accused Instrumentalities that implement EMV standards to provide tokenization, processing, authorization, clearing, and/or settlement services to Defendants’ card issuer customers; and/or for mobile and/or contactless payments, including Mastercard’s contactless chip devices and technology provided to consumers via licenses with at least issuers, acquirers, chip vendors, and/or merchants. These services and devices and the technology utilized within them implement and perform methods pursuant to at least EMV standards, including without limitation standards that Mastercard utilizes and/or requires third parties to utilize. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers services for mobile or contactless payments that conform to the EMV standards and/or use Mastercard’s products, systems, devices and/or methods for the authorization and settlement of payment transactions. Defendants’ mobile payments can be facilitated by Mastercard provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Mastercard Transaction Instruments and/or Mastercard Cards. Defendants perform and/or direct and control infringement of the infringing products, systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, developers, merchants, customers, consumers, and/or clients, for the authorization of and settlement of these mobile or contactless payments conducted using Mastercard Cards.

223. The Accused Instrumentalities implement the method of claim 1 of the '985 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Instrumentalities include a method implementing the steps: receiving, by a computer system, an authorization request from a merchant for a transaction, wherein the authorization request indicates that the transaction has been initiated using a first transaction instrument corresponding to a user; based on the authorization request, the computer system determining a second transaction instrument corresponding to the user; the computer system analyzing transaction data for the transaction, wherein the analyzing includes determining whether the transaction data at least partially corresponds to particular transaction data associated with the second transaction instrument; and based on said analyzing, the computer system transmitting a response to the authorization request to the merchant, wherein the response indicates whether the transaction is authorized.

224. At a minimum, Defendants have known of the '985 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '985 patent on numerous occasions. For example, Defendants have known about the patent portfolio including the '985 patent, since at least March 15, 2018, when, via email, Colm J. Dobbyn (General Counsel, Intellectual Property, Mastercard) responded to email correspondence from a representative of Plaintiff affiliate Dominion Harbor Group, LLC ("DHG") that informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in acquisition discussions relating to Plaintiff's patent portfolio, and offered a phone call and email address to discuss the acquisition opportunity. At least as early as on or around October 11, 2018, Defendants

were provided with access to a presentation and data room containing information related to the American Express patent portfolio and the '985 patent. On October 3, 2022, via email, DHG again requested a call to discuss an acquisition opportunity (e.g., licensing opportunity) for the American Express patent portfolio on behalf of Plaintiff and again provided access to a data room containing information related to the American Express patent portfolio. The data rooms included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one example of a claim of the '985 patent.

225. On information and belief, since at least each of the above-mentioned dates when Defendants were on notice of their infringement, Defendants have actively induced, under U.S.C. § 271(b), intermediaries, distributors, suppliers, partners, developers, issuers, acquirers, merchants, customers, clients, consumers, and/or payment platforms (e.g., Samsung and Google mobile wallets) that distribute, make, purchase, offer to sell, sale, use, and/or service the Accused Instrumentalities to directly infringe one or more claims of the '985 patent by distributing, making, using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date and/or dates, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '985 patent.

226. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, developers, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications;

as provider of products, systems, methods, and services associated with Mastercard Transaction Instruments and/or Mastercard Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction instruments with the payment applications, generating and installing cryptographic keys, and processing transactions; creating and/or maintaining established distribution channels for the Accused Instrumentalities into and within the United States; manufacturing and designing, including without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing and/or inducing third parties to test Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., [mastercard.us](https://www.mastercard.us) and developer.mastercard.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, in the United States. *See, e.g., Find a credit card*, MASTERCARD, <https://www.mastercard.us/en-us/personal/find-card-products/index.php> (last visited Jan. 22, 2024) (advertising Mastercard's "most popular features and benefits," including rewards, cash back, travel / airline, 0% APR, low interest, and balance transfers, and stating "[f]ind a Mastercard from your favorite financial institution."); *Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024); *Contactless Toolkit for Issuers*, MASTERCARD,

https://www.mastercard.com/contactless/doc/MC_Contactless_Toolkit_Issuers.pdf (last visited Jan. 19, 2024); *More than 50 years of payments experience combined with innovative technology*, MASTERCARD, <https://www.mastercard.us/en-us/business/issuers.html> (last visited Jan. 22, 2024) (advertising that Mastercard “work[s] with issuers of all sizes to create more efficient and secure ways to pay”); *Access to Capital*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview.html> (last visited Jan. 22, 2024) (indicating “[Mastercard] can help you access sources of capital so you can have more freedom and flexibility when it comes to building, managing or growing your business,” and “Mastercard connects you to capital, technology, financial tools, partnerships and more to help grow and protect your business every step of the way.”).

227. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients to directly infringe via Mastercard’s developer resources and website (e.g., developer.mastercard.com), which includes APIs and invites developers to “[c]heck out our full product catalog.” *See developers*, MASTERCARD, <https://developer.mastercard.com/> (last visited Jan. 22, 2024).

228. On information and belief, despite having knowledge of the ‘985 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ‘985 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Defendants’ infringing activities relative to the ‘985 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

229. Plaintiff LPV has been damaged as a result of Defendants' infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to LPV in an amount that adequately compensates LPV for Defendants' infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT VI

(INFRINGEMENT OF U.S. PATENT NO. 7,587,756)

230. Plaintiff incorporates paragraphs 1 through 230 herein by reference.

231. Plaintiff is the assignee of the '756 patent, entitled "Methods and Apparatus for a Secure Proximity Integrated Circuit Card Transactions," with ownership of all substantial rights in the '756 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

232. The '756 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '756 patent issued from U.S. Patent Application No. 10/710,611.

233. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '756 patent in this District and elsewhere in Florida and the United States.

234. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '756 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., Mastercard Transaction Instruments and/or

Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, point of sale, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

235. Defendants directly infringe, individually and/or jointly with at least one other entity, the '756 patent via 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '756 patent for and/or to, for example, its alter egos, agents, intermediaries, licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients. Defendants' infringement involves Defendants' own action and/or direction and control of third parties' actions.

236. Defendant MINC directly infringes the '756 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant MINT, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, developers, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '756 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, MINT, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees,

issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants' point of sale products (e.g., products and services for POS terminals), as used with contactless chips, mobile payments, and digital wallets.

237. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and/or consumers to perform one or more steps of the claimed methods of the '756 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) (“[A]n actor is liable for infringement under § 271(a) if it acts through an agent ... or contracts with another to perform one or more steps of a claimed method.”). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, payment acceptance, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants' agreements with such third parties to provide access to Defendants' products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants' products, systems, methods, and/or services, for example, Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for contactless and mobile payments, as a condition

of each third party's access to, use of, and/or participation in such products, systems, methods, and/or services. *See id.* (“[L]iability under § 271(a) can also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance.”). The activities of each third party (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) in providing services to holders of Defendants’ Mastercard Transaction Instruments, cardholders of Defendants’ Mastercard Cards, and users of other products, systems, methods, and/or services are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

238. In addition to the liability arising from the Defendants’ relationship with third parties, Defendants also directly infringe, individually and/or jointly, the ‘756 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Mastercard Transaction Instruments, Mastercard Cards, and/or point-of-sale terminals. On information and belief, Defendants design and develop payment applications for accounts used in connection with Mastercard Transaction Instruments and/or Mastercard Cards, which are used with physical Mastercard Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Find a Card*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview/cards.html> (last visited Jan. 22, 2024) (showing Mastercard offers payment solutions, for example, contactless payments and digital payments, and various cards including debit, credit, ATM, prepaid and gift cards); *EMV Technology at Work*, MASTERCARD,

<https://sea.mastercard.com/en-region-sea/business/issuers/products-and-solutions/payment-innovations/chip-emv.html> (last visited Jan. 22, 2024) (“For 15 years, Mastercard has played a leading role in the creation, management and continued development of the EMV standard. We [Mastercard] offer a unique set of EMV solutions to help issuers and merchants implement new payment solutions quickly.”)

239. For example, Defendants infringe claim 1 of the ‘756 patent via their Accused Instrumentalities that implement EMV standards to provide EMV compliant products and services that perform a method of securing a transaction utilizing a proximity integrated circuit transaction device.

240. The Accused Instrumentalities implement the method of claim 1 of the ‘756 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff’s allegations that each of those limitations is met. For example, the Accused Instrumentalities include a method for securing a transaction utilizing a proximity integrated circuit (PIC) transaction device and a merchant system. The method implements the steps: determining a first merchant action analysis result, at the merchant system, based at least in part on one of an authentication of the PIC transaction device using Offline Data Authentication (ODA), a transaction process restriction, and a merchant risk management factor, the first merchant action analysis result indicating at least one of approving the transaction offline, approving the transaction online, and denying the transaction; requesting, by the merchant system, an application cryptogram from the PIC transaction device, the application cryptogram being one of a cryptogram for approving the transaction offline, a cryptogram for approving the transaction online, and a cryptogram for denying the transaction based on the first merchant action analysis result; determining a first card action analysis result, at the PIC transaction device, the first card action analysis result indicating at least

one of approving the transaction offline, approving the transaction online, and denying the transaction; transmitting, by the PIC transaction device, the first card action analysis result to the merchant system, wherein the first card action analysis result includes the requested application cryptogram; requesting, by the merchant system, based on at least one of the first merchant action analysis result and the first card action analysis result, an authorization response from a PIC issuer system; and if the merchant system receives the authorization response from the PIC issuer system, determining, at the merchant system, based at least in part on a predetermined rule and at least one of the first merchant action analysis result and the first card action analysis result, whether to approve the transaction offline or deny the transaction offline.

241. At a minimum, Defendants have known of the ‘756 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff’s American Express patent portfolio and the ‘756 patent on numerous occasions. For example, Defendants have known about the patent portfolio including the ‘756 patent, since at least March 15, 2018, when, via email, Colm J. Dobbyn (General Counsel, Intellectual Property, Mastercard) responded to email correspondence from a representative of Plaintiff affiliate Dominion Harbor Group, LLC (“DHG”) that informed Defendants of Plaintiff’s acquisition of the American Express patent portfolio, invited Defendants to engage in acquisition discussions relating to Plaintiff’s patent portfolio, and offered a phone call and email address to discuss the acquisition opportunity. At least as early as on or around October 11, 2018, Defendants were provided with access to a presentation and data room containing information related to the American Express patent portfolio and the ‘756 patent. On October 3, 2022, via email, DHG again requested a call to discuss an acquisition opportunity (e.g., licensing opportunity) for the American Express patent portfolio on behalf of Plaintiff and again provided access to a data room containing

information related to the American Express patent portfolio and the '756 patent. The data rooms included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '756 patent.

242. On information and belief, since at least each of the above-mentioned dates when Defendants were on notice of their infringement, Defendants have actively induced, under U.S.C. § 271(b), intermediaries, distributors, suppliers, partners, developers, issuers, acquirers, merchants, customers, clients, consumers, and/or payment platforms (e.g., Samsung and Google mobile wallets) that distribute, make, purchase, offer to sell, sale, use, and/or service the Accused Instrumentalities to directly infringe one or more claims of the '756 patent by distributing, making, using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date and/or dates, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '756 patent.

243. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, developers, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Mastercard Transaction Instruments and/or Mastercard Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants'

Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction instruments with the payment applications, generating and installing cryptographic keys, and processing transactions; creating and/or maintaining established distribution channels for the Accused Instrumentalities into and within the United States; manufacturing and designing, including without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing and/or inducing third parties to test Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., [mastercard.us](https://www.mastercard.us) and developer.mastercard.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, in the United States. *See, e.g., Find a credit card*, MASTERCARD, <https://www.mastercard.us/en-us/personal/find-card-products/index.php> (last visited Jan. 22, 2024) (advertising Mastercard's "most popular features and benefits," including rewards, cash back, travel / airline, 0% APR, low interest, and balance transfers, and stating "[f]ind a Mastercard from your favorite financial institution."); *Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024); *Contactless Toolkit for Issuers*, MASTERCARD, https://www.mastercard.com/contactless/doc/MC_Contactless_Toolkit_Issuers.pdf (last visited Jan. 19, 2024); *More than 50 years of payments experience combined with innovative technology*, MASTERCARD, <https://www.mastercard.us/en-us/business/issuers.html> (last visited Jan. 22, 2024) (advertising that Mastercard "work[s] with issuers of all sizes to create more efficient and secure

ways to pay”); *Access to Capital*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview.html> (last visited Jan. 22, 2024) (indicating “[Mastercard] can help you access sources of capital so you can have more freedom and flexibility when it comes to building, managing or growing your business,” and “Mastercard connects you to capital, technology, financial tools, partnerships and more to help grow and protect your business every step of the way.”).

244. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients to directly infringe via Mastercard’s developer resources and website (e.g., developer.mastercard.com), which includes APIs and invites developers to “[c]heck out our full product catalog.” *See developers*, MASTERCARD, <https://developer.mastercard.com/> (last visited Jan. 22, 2024).

245. On information and belief, despite having knowledge of the ‘756 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ‘756 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Defendants’ infringing activities relative to the ‘756 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

246. Plaintiff LPV has been damaged as a result of Defendants’ infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to LPV in an amount that adequately compensates LPV for Defendants’ infringements, which, by law, cannot be less

than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT VII

(INFRINGEMENT OF U.S. PATENT NO. 7,668,750)

247. Plaintiff incorporates paragraphs 1 through 247 herein by reference.

248. Plaintiff is the assignee of the ‘750 patent, entitled “Securing RF Transactions Using a Transactions Counter,” with ownership of all substantial rights in the ‘750 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

249. The ‘750 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The ‘750 patent issued from U.S. Patent Application No. 10/708,545.

250. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the ‘750 patent in this District and elsewhere in Florida and the United States.

251. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the ‘750 patent, which includes Defendants’ offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., Mastercard Transaction Instruments and/or Mastercard Cards) and related products, methods, and/or services for Defendants’ licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, including Defendants’ issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants’ payment processing, authentication, authorization,

validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

252. Defendants directly infringe, individually and/or jointly with at least one other entity, the '750 patent via 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '750 patent for and/or to, for example, its alter egos, agents, intermediaries, licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients. Defendants' infringement involves Defendants' own action and/or direction and control of third parties' actions.

253. Defendant MINC directly infringes the '750 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant MINT, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, developers, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '750 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, MINT, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud

detection related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

254. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and/or consumers to perform one or more steps of the claimed methods of the '750 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) (“[A]n actor is liable for infringement under § 271(a) if it acts through an agent ... or contracts with another to perform one or more steps of a claimed method.”). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants' agreements with such third parties to provide access to Defendants' products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants' products, systems, methods, and/or services, for example, Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for contactless and mobile payments, as a condition of each third party's access to, use of, and/or participation in such products, systems, methods, and/or services. *See id.* (“[L]iability under § 271(a) can also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and

establishes the manner or timing of that performance.”). The activities of each third party (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) in providing services to holders of Defendants’ Mastercard Transaction Instruments, cardholders of Defendants’ Mastercard Cards, and users of other products, systems, methods, and/or services are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

255. In addition to the liability arising from the Defendants’ relationship with third parties, Defendants also directly infringe, individually and/or jointly, the ‘750 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Mastercard Transaction Instruments and/or Mastercard Cards. On information and belief, Defendants design and develop payment applications for accounts used in connection with Mastercard Transaction Instruments and/or Mastercard Cards, which are used with physical Mastercard Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Find a Card*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview/cards.html> (last visited Jan. 22, 2024) (showing Mastercard offers payment solutions, for example, contactless payments and digital payments, and various cards including debit, credit, ATM, prepaid and gift cards); *EMV Technology at Work*, MASTERCARD, <https://sea.mastercard.com/en-region-sea/business/issuers/products-and-solutions/payment-innovations/chip-emv.html> (last visited Jan. 22, 2024) (“For 15 years, Mastercard has played a leading role in the creation, management and

continued development of the EMV standard. We [Mastercard] offer a unique set of EMV solutions to help issuers and merchants implement new payment solutions quickly.”)

256. For example, Defendants infringe at least claim 1 and claim 12 of the ‘750 patent via their Accused Instrumentalities that implement EMV standards to provide EMV compliant products and services that effect RF payment transactions, for example, performing a method of securing a RFID transactions with mobile wallets (e.g., Google Pay and/or Samsung Pay) using host card emulation.

257. The Accused Instrumentalities implement the method of claim 1 of the ‘750 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff’s allegations that each of those limitations is met. For example, the Accused Instrumentalities include a method implementing the steps: receiving a financial transaction request from an RF transaction device at an RF reader of a merchant system, wherein said financial transaction request comprises a transactions counted value that indicates a number of financial transactions performed with said RF transaction device; transmitting said financial transaction request to a transaction processor; receiving a denial message from said transaction processor in response to said transactions counted value exceeding a maximum transactions value; and denying, by said merchant system, said financial transaction request in response to said transactions counted value exceeding said maximum transactions value.

258. The Accused Instrumentalities implement the method of claim 12 of the ‘750 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff’s allegations that each of those limitations is met. For example, the Accused Instrumentalities include a method implementing the steps: transmitting a financial transaction request from a Radio Frequency (RF) transaction device to an RFID reader, wherein said financial

transaction request comprises a transactions counted value that indicates a number of financial transactions performed with said RF transaction device, wherein said financial transaction request is transmitted to a transaction processor, wherein said RFID reader receives a denial message from said transaction processor in response to said transactions counted value exceeding a maximum transactions value, and wherein said financial transaction request is denied in response to said transactions counted value exceeding said maximum transactions value; and incrementing, at said RF transaction device, said transaction counted value.

259. At a minimum, Defendants have known of the '750 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '750 patent on numerous occasions. For example, Defendants have known about the patent portfolio including the '750 patent, since at least March 15, 2018, when, via email, Colm J. Dobbyn (General Counsel, Intellectual Property, Mastercard) responded to email correspondence from a representative of Plaintiff affiliate Dominion Harbor Group, LLC ("DHG") that informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in acquisition discussions relating to Plaintiff's patent portfolio, and offered a phone call and email address to discuss the acquisition opportunity. At least as early as on or around October 11, 2018, Defendants were provided with access to a presentation and data room containing information related to the American Express patent portfolio and the '750 patent. On October 3, 2022, via email, DHG again requested a call to discuss an acquisition opportunity (e.g., licensing opportunity) for the American Express patent portfolio on behalf of Plaintiff and again provided access to a data room containing information related to the American Express patent portfolio and the '750 patent. The data rooms

included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '750 patent.

260. On information and belief, since at least each of the above-mentioned dates when Defendants were on notice of their infringement, Defendants have actively induced, under U.S.C. § 271(b), intermediaries, distributors, suppliers, partners, developers, issuers, acquirers, merchants, customers, clients, consumers, and/or payment platforms (e.g., Samsung and Google mobile wallets) that distribute, make, purchase, offer to sell, sale, use, and/or service the Accused Instrumentalities to directly infringe one or more claims of the '750 patent by distributing, making, using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date and/or dates, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '750 patent.

261. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, developers, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Mastercard Transaction Instruments and/or Mastercard Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing

transaction instruments with the payment applications, generating and installing cryptographic keys, and processing transactions; creating and/or maintaining established distribution channels for the Accused Instrumentalities into and within the United States; manufacturing and designing, including without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing and/or inducing third parties to test Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., [mastercard.us](https://www.mastercard.us) and developer.mastercard.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, in the United States. *See, e.g., Find a credit card*, MASTERCARD, <https://www.mastercard.us/en-us/personal/find-card-products/index.php> (last visited Jan. 22, 2024) (advertising Mastercard's "most popular features and benefits," including rewards, cash back, travel / airline, 0% APR, low interest, and balance transfers, and stating "[f]ind a Mastercard from your favorite financial institution."); *Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024); *Contactless Toolkit for Issuers*, MASTERCARD, https://www.mastercard.com/contactless/doc/MC_Contactless_Toolkit_Issuers.pdf (last visited Jan. 19, 2024); *More than 50 years of payments experience combined with innovative technology*, MASTERCARD, <https://www.mastercard.us/en-us/business/issuers.html> (last visited Jan. 22, 2024) (advertising that Mastercard "work[s] with issuers of all sizes to create more efficient and secure ways to pay"); *Access to Capital*, MASTERCARD, [**PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT** – Page 158](https://www.mastercard.us/en-</p></div><div data-bbox=)

us/business/overview.html (last visited Jan. 22, 2024) (indicating “[Mastercard] can help you access sources of capital so you can have more freedom and flexibility when it comes to building, managing or growing your business,” and “Mastercard connects you to capital, technology, financial tools, partnerships and more to help grow and protect your business every step of the way.”).

262. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients to directly infringe via Mastercard’s developer resources and website (e.g., developer.mastercard.com), which includes APIs and invites developers to “[c]heck out our full product catalog.” *See developers, MASTERCARD, https://developer.mastercard.com/* (last visited Jan. 22, 2024).

263. On information and belief, despite having knowledge of the ‘750 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ‘750 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Defendants’ infringing activities relative to the ‘750 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

264. Plaintiff LPV has been damaged as a result of Defendants’ infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to LPV in an amount that adequately compensates LPV for Defendants’ infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT VIII

(INFRINGEMENT OF U.S. PATENT NO. 8,584,938)

265. Plaintiff incorporates paragraphs 1 through 264 herein by reference.

266. Plaintiff is the assignee of the '938 patent, entitled "Wireless Transaction Medium Having Combined Magnetic Stripe and Radio Frequency Communications," with ownership of all substantial rights in the '938 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

267. The '938 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '938 patent issued from U.S. Patent Application No. 13/713,976.

268. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '938 patent in this District and elsewhere in Florida and the United States.

269. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '938 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., Mastercard Transaction Instruments and/or Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, authentication, authorization,

validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

270. Defendants directly infringe, individually and/or jointly with at least one other entity, the '938 patent via 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '938 patent for and/or to, for example, its alter egos, agents, intermediaries, licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients. Defendants' infringement involves Defendants' own action and/or direction and control of third parties' actions.

271. Defendant MINC directly infringes the '938 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant MINT, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, developers, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '938 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, MINT, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud

detection related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

272. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and/or consumers to perform one or more steps of the claimed methods of the '938 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) (“[A]n actor is liable for infringement under § 271(a) if it acts through an agent ... or contracts with another to perform one or more steps of a claimed method.”). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants' agreements with such third parties to provide access to Defendants' products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants' products, systems, methods, and/or services, for example, Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for contactless and mobile payments, as a condition of each third party's access to, use of, and/or participation in such products, systems, methods, and/or services. *See id.* (“[L]iability under § 271(a) can also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and

establishes the manner or timing of that performance.”). The activities of each third party (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) in providing services to holders of Defendants’ Mastercard Transaction Instruments, cardholders of Defendants’ Mastercard Cards, and users of other products, systems, methods, and/or services are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

273. In addition to the liability arising from the Defendants’ relationship with third parties, Defendants also directly infringe, individually and/or jointly, the ‘938 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Mastercard Transaction Instruments and/or Mastercard Cards. On information and belief, Defendants design and develop payment applications for accounts used in connection with Mastercard Transaction Instruments and/or Mastercard Cards, which are used with physical Mastercard Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Find a Card*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview/cards.html> (last visited Jan. 22, 2024) (showing Mastercard offers payment solutions, for example, contactless payments and digital payments, and various cards including debit, credit, ATM, prepaid and gift cards); *EMV Technology at Work*, MASTERCARD, <https://sea.mastercard.com/en-region-sea/business/issuers/products-and-solutions/payment-innovations/chip-emv.html> (last visited Jan. 22, 2024) (“For 15 years, Mastercard has played a leading role in the creation, management and

continued development of the EMV standard. We [Mastercard] offer a unique set of EMV solutions to help issuers and merchants implement new payment solutions quickly.”)

274. For example, Defendants infringe claim 14 of the '938 patent via their Accused Instrumentalities that implement EMV standards for mobile or contactless payments, including Mastercard Transaction Instruments and technology provided to consumers via licenses with at least issuers, acquirers, chip vendors, and merchants. These devices and the technology utilized within them implement and perform methods pursuant to at least EMV standards, which Mastercard utilizes and/or requires third parties to utilize. Moreover, these devices and technology enable the tokenization of consumers' primary account numbers (PANs) to facilitate secure financial transactions for Mastercard Cards, via Mastercard products and/or services. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Mastercard Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards. Defendants' mobile payments can be facilitated by Mastercard provisioning mobile wallets such as Google Pay and Samsung Pay contactless payment functions for financial accounts associated with Mastercard Cards. Or such contactless payments can be facilitated by using contactless chips embedded on the physical Mastercard Cards. Defendants perform and/or direct and control the infringing systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, developers, customers, consumers, and clients, for the authorization of and settlement of these mobile or contactless payments conducted using Mastercard Cards.

275. The Accused Instrumentalities implement the method of claim 14 of the '938 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused

Instrumentalities practice the following method steps: replacing, by a computer-based system for creating a second account code, a first portion of a first account code with data to create the second account code, wherein a second portion of the second account code is associated with a second portion of the first account code; and wherein the second account code may be used for a transaction.

276. At a minimum, Defendants have known of the '938 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '938 patent on numerous occasions. For example, Defendants have known about the patent portfolio including the '938 patent, since at least March 15, 2018, when, via email, Colm J. Dobbyn (General Counsel, Intellectual Property, Mastercard) responded to email correspondence from a representative of Plaintiff affiliate Dominion Harbor Group, LLC ("DHG") that informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in acquisition discussions relating to Plaintiff's patent portfolio, and offered a phone call and email address to discuss the acquisition opportunity. At least as early as on or around October 11, 2018, Defendants were provided with access to a presentation and data room containing information related to the American Express patent portfolio and the '938 patent. On October 3, 2022, via email, DHG again requested a call to discuss an acquisition opportunity (e.g., licensing opportunity) for the American Express patent portfolio on behalf of Plaintiff and again provided access to a data room containing information related to the American Express patent portfolio and the '938 patent. The data rooms included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '938 patent.

277. On information and belief, since at least each of the above-mentioned dates when Defendants were on notice of their infringement, Defendants have actively induced, under U.S.C. § 271(b), intermediaries, distributors, suppliers, partners, developers, issuers, acquirers, merchants, customers, clients, consumers, and/or payment platforms (e.g., Samsung and Google mobile wallets) that distribute, make, purchase, offer to sell, sale, use, and/or service the Accused Instrumentalities to directly infringe one or more claims of the '938 patent by distributing, making, using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date and/or dates, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '938 patent.

278. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, developers, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Mastercard Transaction Instruments and/or Mastercard Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction instruments with the payment applications, generating and installing cryptographic keys, and processing transactions; creating and/or maintaining established distribution channels for

the Accused Instrumentalities into and within the United States; manufacturing and designing, including without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing and/or inducing third parties to test Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., mastercard.us and developer.mastercard.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, in the United States. *See, e.g., Consumer Controls Virtual Card Numbers*, MASTERCARD, <https://developer.mastercard.com/product/consumer-controls-virtual-card-numbers/> (last visited Jan. 23, 2024) (“Create Virtual Card Numbers, register and setup controls using Consumer Controls API”); *MASTERCARD CARD ON FILE: Card on File – Card Tokenization*, MASTERCARD, <https://www.mastercard.us/en-us/checkout/card-on-file.html> (last visited Jan. 23, 2024) (“WHY MASTERCARD CARD ON FILE Convenience for your customers, peace of mind for you.”); *Find a credit card*, MASTERCARD, <https://www.mastercard.us/en-us/personal/find-card-products/index.php> (last visited Jan. 22, 2024) (advertising Mastercard’s “most popular features and benefits,” including rewards, cash back, travel / airline, 0% APR, low interest, and balance transfers, and stating “[f]ind a Mastercard from your favorite financial institution.”); *Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024); *Contactless Toolkit for Issuers*, MASTERCARD, https://www.mastercard.com/contactless/doc/MC_Contactless_Toolkit_Issuers.pdf (last visited

Jan. 19, 2024); *More than 50 years of payments experience combined with innovative technology*, MASTERCARD, <https://www.mastercard.us/en-us/business/issuers.html> (last visited Jan. 22, 2024) (advertising that Mastercard “work[s] with issuers of all sizes to create more efficient and secure ways to pay”); *Access to Capital*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview.html> (last visited Jan. 22, 2024) (indicating “[Mastercard] can help you access sources of capital so you can have more freedom and flexibility when it comes to building, managing or growing your business,” and “Mastercard connects you to capital, technology, financial tools, partnerships and more to help grow and protect your business every step of the way.”).

279. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients to directly infringe via Mastercard’s developer resources and website (e.g., developer.mastercard.com), which includes APIs and invites developers to “[c]heck out our full product catalog.” *See developers*, MASTERCARD, <https://developer.mastercard.com/> (last visited Jan. 22, 2024).

280. On information and belief, despite having knowledge of the ‘938 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ‘938 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Defendants’ infringing activities relative to the ‘938 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

281. Plaintiff LPV has been damaged as a result of Defendants' infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to LPV in an amount that adequately compensates LPV for Defendants' infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT IX

(INFRINGEMENT OF U.S. PATENT NO. 7,431,207)

282. Plaintiff incorporates paragraphs 1 through 281 herein by reference.

283. Plaintiff is the assignee of the '207 patent, entitled "System and Method for Two-Step Payment Transaction Authorizations," with ownership of all substantial rights in the '207 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

284. The '207 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '207 patent issued from U.S. Patent Application No. 11/031,111.

285. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '207 patent in this District and elsewhere in Florida and the United States.

286. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '207 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with card-not-present transactions (e.g., transactions implementing EMV 3D Secure)

and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Mastercard Cards), as used in card-not-present transactions.

287. Defendants directly infringe, individually and/or jointly with at least one other entity, the '207 patent via 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '207 patent for and/or to, for example, its alter egos, agents, intermediaries, licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients. Defendants' infringement involves Defendants' own action and/or direction and control of third parties' actions.

288. Defendant MINC directly infringes the '207 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant MINT, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, developers, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '207 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, MINT, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients including

without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants' card products (e.g., Mastercard Cards), as used in card-not-present transactions.

289. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and/or consumers to perform one or more steps of the claimed methods of the '207 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) (“[A]n actor is liable for infringement under § 271(a) if it acts through an agent ... or contracts with another to perform one or more steps of a claimed method.”). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants' agreements with such third parties to provide access to Defendants' products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants' products, systems, methods, and/or services, for example, Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for securing card-not-present transactions, as a condition of each third party's access to, use of, and/or participation in such products, systems, methods, and/or services.

See id. (“[L]iability under § 271(a) can also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance.”). The activities of each third party (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) in providing services to holders of Defendants’ Mastercard Transaction Instruments, cardholders of Defendants’ Mastercard Cards, and users of other products, systems, methods, and/or services are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

290. In addition to the liability arising from the Defendants’ relationship with third parties, Defendants also directly infringe, individually and/or jointly, the ‘207 patent via their own provision of products, systems, methods, and services that implement the EMV 3D Secure standards for securing card-not-present transactions (e.g., Mastercard Identity Check). On information and belief, Defendants design and develop software and services used in connection with Mastercard 3D Secure product offerings. These products are offered to merchants that accept payments through online portals.

291. For example, Defendants infringe claim 1 of the ‘207 patent via their Accused Instrumentalities that implement EMV standards for processing services in connection with commercial transactions that implement the EMV 3-D Secure specification; payment processing for merchant customers; and/or gateway services for merchant customers. Mastercard Identity Check is an example of a method for processing a commercial transaction that implements the EMV 3-D Secure specification.

292. The Accused Instrumentalities implement the method of claim 1 of the '207 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff's allegations that each of those limitations is met. For example, the Accused Instrumentalities include a method for processing a commercial transaction. The method implements the steps: submitting a card payment request to a merchant; initiating a communication between a cardholder submitting the card payment request and an authorization computer of an issuer; receiving an authorization request from said merchant in response to said card payment request; authenticating an identity of said cardholder using information received from said cardholder, said authenticating including matching said information received from said cardholder with a corresponding predetermined stored value and generating an authentication score representing a relative reliability of the identity of the cardholder based on the information from said cardholder; matching the authorization request to said cardholder; authorizing the authorization request and, if the authorization request is approved, generating a private payment number; and issuing an authorization confirmation including the authorization score and the private payment number to said merchant upon authorizing the authorization request.

293. At a minimum, Defendants have known of the '207 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '207 patent on numerous occasions. For example, Defendants have known about the patent portfolio including the '207 patent, since at least March 15, 2018, when, via email, Colm J. Dobbyn (General Counsel, Intellectual Property, Mastercard) responded to email correspondence from a representative of Plaintiff affiliate Dominion Harbor Group, LLC ("DHG") that informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in acquisition

discussions relating to Plaintiff's patent portfolio, and offered a phone call and email address to discuss the acquisition opportunity. At least as early as on or around October 11, 2018, Defendants were provided with access to a presentation and data room containing information related to the American Express patent portfolio and the '207 patent. On October 3, 2022, via email, DHG again requested a call to discuss an acquisition opportunity (e.g., licensing opportunity) for the American Express patent portfolio on behalf of Plaintiff and again provided access to a data room containing information related to the American Express patent portfolio and the '207 patent. The data rooms included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '207 patent.

294. On information and belief, since at least each of the above-mentioned dates when Defendants were on notice of their infringement, Defendants have actively induced, under U.S.C. § 271(b), intermediaries, distributors, suppliers, partners, developers, issuers, acquirers, merchants, customers, clients, consumers, and/or payment platforms (e.g., Samsung and Google mobile wallets) that distribute, make, purchase, offer to sell, sale, use, and/or service the Accused Instrumentalities to directly infringe one or more claims of the '207 patent by distributing, making, using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date and/or dates, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '207 patent.

295. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, developers, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment

standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Mastercard Transaction Instruments and/or Mastercard Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction instruments with the payment applications, generating and installing cryptographic keys, and processing transactions; creating and/or maintaining established distribution channels for the Accused Instrumentalities into and within the United States; manufacturing and designing, including without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing and/or inducing third parties to test Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., [mastercard.us](https://www.mastercard.us) and developer.mastercard.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, in the United States. *See, e.g., Improve security without sacrificing the customer experience with Mastercard Identity Check™*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview/safety-and-security/identity-check.html> (last visited Jan. 23, 2024) ("As a merchant, you accept more and more payments digitally every day, yet you need to ensure that every transaction is secure. Mastercard

Identity Check leverages the latest authentication standards of EMV® 3-D Secure (replacing 3DS 1.0) to complete more transactions without disruption.”); *Top 10 Things to Know About EMV 3-D Secure*, MASTERCARD, <https://www.mastercard.com/content/dam/public/mastercardcom/globalrisk/pdf/Top-10-Things-to-Know-About-3DS.pdf> (last visited Jan. 23, 2024) (“3DS Server: Server option for merchants, PSPs & Acquirers that want to build their own MI.”); *Find a credit card*, MASTERCARD, <https://www.mastercard.us/en-us/personal/find-card-products/index.php> (last visited Jan. 22, 2024) (advertising Mastercard’s “most popular features and benefits,” including rewards, cash back, travel / airline, 0% APR, low interest, and balance transfers, and stating “[f]ind a Mastercard from your favorite financial institution.”); *Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024); *Contactless Toolkit for Issuers*, MASTERCARD, https://www.mastercard.com/contactless/doc/MC_Contactless_Toolkit_Issuers.pdf (last visited Jan. 19, 2024); *More than 50 years of payments experience combined with innovative technology*, MASTERCARD, <https://www.mastercard.us/en-us/business/issuers.html> (last visited Jan. 22, 2024) (advertising that Mastercard “work[s] with issuers of all sizes to create more efficient and secure ways to pay”); *Access to Capital*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview.html> (last visited Jan. 22, 2024) (indicating “[Mastercard] can help you access sources of capital so you can have more freedom and flexibility when it comes to building, managing or growing your business,” and “Mastercard connects you to capital, technology, financial tools, partnerships and more to help grow and protect your business every step of the way.”).

296. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients to directly infringe via Mastercard’s developer resources and website (e.g., developer.mastercard.com), which includes APIs and invites developers to “[c]heck out our full product catalog.” *See developers, MASTERCARD, https://developer.mastercard.com/* (last visited Jan. 22, 2024).

297. On information and belief, despite having knowledge of the ‘207 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ‘207 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Defendants’ infringing activities relative to the ‘207 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

298. Plaintiff LPV has been damaged as a result of Defendants’ infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to LPV in an amount that adequately compensates LPV for Defendants’ infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT X

(INFRINGEMENT OF U.S. PATENT NO. 6,886,101)

299. Plaintiff incorporates paragraphs 1 through 298 herein by reference.

300. Plaintiff is the assignee of the ‘101 patent, entitled “Privacy Service,” with ownership of all substantial rights in the ‘101 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

301. The '101 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '101 patent issued from U.S. Patent Application No. 10/283,434.

302. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '101 patent in this District and elsewhere in Florida and the United States.

303. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '101 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., Mastercard Transaction Instruments and/or Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

304. Defendants directly infringe, individually and/or jointly with at least one other entity, the '101 patent via 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the

‘101 patent for and/or to, for example, its alter egos, agents, intermediaries, licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients. Defendants’ infringement involves Defendants’ own action and/or direction and control of third parties’ actions.

305. Defendant MINC directly infringes the ‘101 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant MINT, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants’ divisions, subsidiaries, partners, developers, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the ‘101 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, MINT, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants’ licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants’ card products (e.g., Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

306. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and/or consumers to perform one or more steps of the claimed methods of the ‘101 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) (“[A]n actor is liable for infringement under § 271(a) if it acts through an agent ... or contracts with another to

perform one or more steps of a claimed method.”). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants’ cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants’ agreements with such third parties to provide access to Defendants’ products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants’ products, systems, methods, and/or services, for example, Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for contactless and mobile payments, as a condition of each third party’s access to, use of, and/or participation in such products, systems, methods, and/or services. *See id.* (“[L]iability under § 271(a) can also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance.”). The activities of each third party (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, developers, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) in providing services to holders of Defendants’ Mastercard Transaction Instruments, cardholders of Defendants’ Mastercard Cards, and users of other products, systems, methods, and/or services are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

307. In addition to the liability arising from the Defendants' relationship with third parties, Defendants also directly infringe, individually and/or jointly, the '101 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Mastercard Transaction Instruments and/or Mastercard Cards. On information and belief, Defendants design and develop payment applications for accounts used in connection with Mastercard Transaction Instruments and/or Mastercard Cards, which are used with physical Mastercard Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Find a Card*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview/cards.html> (last visited Jan. 22, 2024) (showing Mastercard offers payment solutions, for example, contactless payments and digital payments, and various cards including debit, credit, ATM, prepaid and gift cards); *EMV Technology at Work*, MASTERCARD, <https://sea.mastercard.com/en-region-sea/business/issuers/products-and-solutions/payment-innovations/chip-emv.html> (last visited Jan. 22, 2024) ("For 15 years, Mastercard has played a leading role in the creation, management and continued development of the EMV standard. We [Mastercard] offer a unique set of EMV solutions to help issuers and merchants implement new payment solutions quickly.")

308. For example, Defendants infringe claim 1 of the '101 patent via its Accused Instrumentalities that utilize methods that facilitate self audit of a user's privacy data. Defendants provide, for example, account creation and registration processes to developers allowing users to sign up for a Mastercard developer account, for example, via Defendants' website, developer.mastercard.com. The enrollment process includes prompts from Defendants' website for a user's privacy data which is stored on web servers. Users are allowed to review and change their

privacy data, for example, utilizing the My Account section of their online account or the user can change communications preferences, for example, by using a subscribe or unsubscribe option. Defendants, as the owners and operators of the Mastercard developer website, direct and control, including via their alter egos, suppliers, agents, affiliates, partners, developers, and subsidiaries, the operation of these self-auditing processes conducted using Defendants' online interfaces with users.

309. The Accused Instrumentalities implement the method of claim 1 of the '101 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Instrumentalities include a method for facilitating a self audit of a first privacy data associated with a first user and a second privacy data associated with a second user. The method includes the following steps: collecting the first privacy data associated with the first user; storing the first privacy data in a central database; collecting the second privacy data associated with the second user; storing the second privacy data in the central database; facilitating the first user to self audit the first privacy data, wherein the first user is restricted from auditing the second privacy data, and wherein the self audit comprises: retrieving audit information for the stored first privacy data; reviewing the retrieved audit information; and changing a first privacy policy and the first privacy data associated with the first user based on the first user's review of the audit information; and facilitating the second user to self audit the second privacy data, wherein the second user is restricted from auditing the first privacy data, and wherein the self audit comprises: retrieving audit information for the stored second privacy data; reviewing the retrieved audit information; and changing a second privacy policy and the second privacy data associated with the second user based on the second user's review of the audit information.

310. At a minimum, Defendants have known of the ‘101 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff’s American Express patent portfolio and the ‘101 patent on numerous occasions. For example, Defendants have known about the patent portfolio including the ‘101 patent, since at least March 15, 2018, when, via email, Colm J. Dobbyn (General Counsel, Intellectual Property, Mastercard) responded to email correspondence from a representative of Plaintiff affiliate Dominion Harbor Group, LLC (“DHG”) that informed Defendants of Plaintiff’s acquisition of the American Express patent portfolio, invited Defendants to engage in acquisition discussions relating to Plaintiff’s patent portfolio, and offered a phone call and email address to discuss the acquisition opportunity. At least as early as on or around October 11, 2018, Defendants were provided with access to a presentation and data room containing information related to the American Express patent portfolio and the ‘101 patent. On October 3, 2022, via email, DHG again requested a call to discuss an acquisition opportunity (e.g., licensing opportunity) for the American Express patent portfolio on behalf of Plaintiff and again provided access to a data room containing information related to the American Express patent portfolio and the ’101 patent. The data rooms included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the ‘101 patent.

311. On information and belief, since at least each of the above-mentioned dates when Defendants were on notice of their infringement, Defendants have actively induced, under U.S.C. § 271(b), intermediaries, distributors, suppliers, partners, developers, issuers, acquirers, merchants, customers, clients, consumers, and/or payment platforms (e.g., Samsung and Google mobile wallets) that distribute, make, purchase, offer to sell, sale, use, and/or service the Accused Instrumentalities to directly infringe one or more claims of the ‘101 patent by distributing, making,

using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date and/or dates, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '101 patent.

312. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, developers, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; providing websites (e.g., mastercard.us and developer.mastercard.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; creating and/or maintaining established distribution channels for the Accused Instrumentalities into and within the United States; manufacturing and designing, including without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing and/or inducing third parties to test Defendants' self-auditing features in the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients, in the United States, including, for example, requiring a developer account as a condition for access to resources in connection with: (i) adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; (ii) provision of products, systems, methods, and services associated with Mastercard Transaction Instruments and/or Mastercard

Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; and/or (iii) maintaining such EMV payment applications by personalizing transaction instruments with the payment applications, generating and installing cryptographic keys, and processing transactions. *See, e.g., developers*, MASTERCARD, <https://developer.mastercard.com/> (last visited Jan. 23, 2024) (“Find the product that is right for you.”); *Log in*, MASTERCARD, <https://developer.mastercard.com/account/log-in> (last visited Jan. 23, 2024) (stating “You can request access for this page after logging in with your Mastercard Developers account,” and offering developers an option to “Create an Account” or “Log in”); *Find a credit card*, MASTERCARD, <https://www.mastercard.us/en-us/personal/find-card-products/index.php> (last visited Jan. 22, 2024) (advertising Mastercard’s “most popular features and benefits,” including rewards, cash back, travel / airline, 0% APR, low interest, and balance transfers, and stating “[f]ind a Mastercard from your favorite financial institution.”); *Chip Cards / EMV Credit Cards*, MASTERCARD, <https://www.mastercard.us/categories/emv-and-smart-chip/> (last visited Jan. 19, 2024); *Contactless Toolkit for Issuers*, MASTERCARD, https://www.mastercard.com/contactless/doc/MC_Contactless_Toolkit_Issuers.pdf (last visited Jan. 19, 2024); *More than 50 years of payments experience combined with innovative technology*, MASTERCARD, <https://www.mastercard.us/en-us/business/issuers.html> (last visited Jan. 22, 2024) (advertising that Mastercard “work[s] with issuers of all sizes to create more efficient and secure ways to pay”); *Access to Capital*, MASTERCARD, <https://www.mastercard.us/en-us/business/overview.html> (last visited Jan. 22, 2024) (indicating “[Mastercard] can help you access sources of capital so you can have more freedom and flexibility when it comes to building,

managing or growing your business,” and “Mastercard connects you to capital, technology, financial tools, partnerships and more to help grow and protect your business every step of the way.”).

313. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, developers, customers, consumers, and/or clients to directly infringe via Mastercard’s developer resources and website (e.g., developer.mastercard.com), which includes APIs and invites developers to “[c]heck out our full product catalog.” *See developers, MASTERCARD, https://developer.mastercard.com/* (last visited Jan. 22, 2024).

314. On information and belief, despite having knowledge of the ‘101 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ‘101 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Defendants’ infringing activities relative to the ‘101 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

315. Plaintiff LPV has been damaged as a result of Defendants’ infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to LPV in an amount that adequately compensates LPV for Defendants’ infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

CONCLUSION

316. Plaintiff is entitled to recover from Defendants the damages sustained by Plaintiff as a result of Defendants' wrongful acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court.

317. Plaintiff has incurred and will incur attorneys' fees, costs, and expenses in the prosecution of this action. The circumstances of this dispute may give rise to an exceptional case within the meaning of 35 U.S.C. § 285, and Plaintiff is entitled to recover its reasonable and necessary attorneys' fees, costs, and expenses.

JURY DEMAND

318. Plaintiff hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

319. Plaintiff requests that the Court find in its favor and against Defendants, and that the Court grant Plaintiff the following relief:

1. A judgment that Defendants have infringed the Asserted Patents as alleged herein, directly and/or indirectly by way of inducing infringement of such patents;
2. A judgment for an accounting of damages sustained by Plaintiff as a result of the acts of infringement by Defendants;
3. A judgment and order requiring Defendants to pay Plaintiff damages under 35 U.S.C. § 284, including up to treble damages as provided by 35 U.S.C. § 284, and any royalties determined to be appropriate;
4. A judgment and order requiring Defendants to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;

5. A judgment and order finding this to be an exceptional case and requiring Defendants to pay the costs of this action (including all disbursements) and attorneys' fees as provided by 35 U.S.C. § 285; and
6. Such other and further relief as the Court deems just and equitable.

Dated: February 5, 2024

Respectfully submitted,

Javier Sobrado

Javier Sobrado(Fla. Bar No. 44992)

Attorney Email Address: jsobrado@brickellip.com

THE BRICKELL IP GROUP, PLLC

1101 Brickell Avenue, South Tower, Suite 800

Miami FL, 33131

Telephone: (305) 728-8831

Pro hac vice forthcoming for:

Terry A. Saad (lead attorney)

(Texas Bar No. 24066015)

Attorney Email Address: tsaad@bosfirm.com

Jeffrey R. Bragalone (Texas Bar No. 02855775)

Attorney Email Address: jbragalone@bosfirm.com

Marcus Benavides (Texas Bar No. 24035574)

Attorney Email Address: mbenavides@bosfirm.com

Brandon V. Zuniga (Texas Bar No. 24088720)

Attorney Email Address : bzuniga@bosfirm.com

Mark M.R. Douglass (Texas Bar No. 24131184)

Attorney Email Address : mdouglass@bosfirm.com

BRAGALONE OLEJKO SAAD PC

901 Main Street

Suite 3800

Dallas, Texas 75202

Telephone: (214) 785-6670

Facsimile: (214) 785-6680

**ATTORNEYS FOR PLAINTIFF LIBERTY
PEAK VENTURES, LLC**