

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION**

LIBERTY PEAK VENTURES, LLC,

Plaintiff,

v.

VISA INC. and VISA U.S.A. INC.,

Defendants.

§
§
§
§
§
§
§
§
§
§

CIVIL ACTION NO. **1:23-cv-00716**

JURY TRIAL DEMANDED

PLAINTIFF’S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Liberty Peak Ventures, LLC files this Complaint in this Western District of Texas (the “District”) against Defendants VISA INC. and VISA U.S.A. INC. (collectively, “Defendants” or “VISA” or “VISA Defendants”) for infringement of U.S. Patent Nos. 8,851,369 (the “369 patent”), 8,584,938 (the “938 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”), and 8,150,746 (the “746 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 VISA INC. (“VISA INC”) is a corporation organized under the laws of the state of Delaware, with its principal place of business located at 900 Metro Center Blvd, Foster City, California 94404 USA and having at least one office located at 12301 Research Blvd, Austin, Texas 78759 USA and 12401 Research Blvd, Austin, Texas 78759 USA. VISA INC 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 USA, and/or via VISA INC's corporate officers. VISA INC is a publicly traded company on the New York Stock Exchange under the symbol "V."

3. On information and belief, Defendant VISA U.S.A. INC. ("VISA USA") is a corporation organized under the laws of the state of Delaware, with its principal place of business located at 900 Metro Center Blvd, Foster City, California 94404 USA and having at least one office located at 12301 Research Blvd, Austin, Texas 78759 USA and 12401 Research Blvd, Austin, Texas 78759 USA. VISA USA may be served with process via its registered agents, including at least Corporation Service Company d/b/a/ CSC-Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701-3218 USA and/or VISA USA's corporate officers. VISA USA is a wholly owned subsidiary of Defendant VISA INC.

4. VISA INC and VISA USA are collectively referred to as VISA in this complaint. According to VISA's annual report for the fiscal year ending September 30, 2022, VISA's "activities are interrelated and each activity is dependent upon and supportive of the other." *See Annual Report for the Fiscal Year Ended September 30, 2022*, VISA INC., p. 59, <https://investor.visa.com/SEC-Filings/> (last accessed Nov. 28, 2022) [hereinafter "*2022 Annual Report*"]. "All significant operating decisions are based on analysis of [VISA] as a single global business." *Id.* "Accordingly, the Company has one reportable segment, Payment Services." *Id.*

5. The term "Visa Cards" is used herein to refer collectively to all payment, banking, credit, debit and/or prepaid cards that are Visa-branded, subject to a license from VISA Defendants, provisioned by VISA Defendants, provided by VISA Defendants, issued by VISA Defendants or a third-party subject to terms of use of the Visa payment network, and/or include the name "Visa" on the cards or in advertising for the cards.

6. On information and belief, VISA “is one of the world’s leaders in digital payments” and “is focused on extending, enhancing and investing in [VISA’s] proprietary network, VisaNet, to offer a single connection point for facilitating payment transactions to multiple endpoints through various form factors.” *Id.* at 4. “Through [VISA’s] network, [VISA] offer[s] products, solutions and services that facilitate secure, reliable and efficient money movement for participants in the ecosystem.” *Id.* “[VISA] facilitate[s] secure, reliable and efficient money movement among consumers, issuing and acquiring financial institutions, and merchants. [VISA] ha[s] traditionally referred to this as the “four-party” model . . . [further referred to as] Our Core Business.” *Id.* As the payments ecosystem continues to evolve, [VISA] ha[s] broadened this model to include digital banks, digital wallets and a range of financial technology companies (fintechs), governments and non-governmental organizations (NGOs).” *Id.* “[VISA] provide[s] transaction processing services (primarily authorization, clearing and settlement) to [VISA’s] financial institution and merchant clients through VisaNet, [VISA’s] advanced transaction processing network.” *Id.*

7. “During fiscal year 2022, [VISA] saw 258 billion payments and cash transactions with [VISA’s] brand, equating to an average of 707 million transactions per day.” *Id.* “Of the 258 billion total transactions, 193 billion were processed by [VISA].” As of June 30, 2022, “[VISA] offer[s] a wide range of Visa-branded payment products that [VISA’s] clients, including nearly 15,000 financial institutions, use to develop and offer core business solutions, including credit, debit, prepaid and cash access programs for individual, business and government account holders.” *Id.* During fiscal year 2022, [VISA’s] total payments and cash volume was \$14 trillion, and 4.1 billion credentials[] were available worldwide to be used at more than 80 million merchant locations, plus an estimated 20 million locations through payment facilitators.” *Id.*

8. “[VISA] enable[s] consumer payments . . . as digital commerce, new technologies and new participants continue to transform the payments ecosystem.” *Id.* at 8. Examples include “Tap to Pay” and “Tokenization.” *Id.* “[C]ontactless payments or tap to pay, which is the process of tapping a contactless card or mobile device on a terminal to make a payment, has emerged as a preferred way to pay among consumers in many countries around the world.” *Id.* “Globally, [VISA] ha[s] more than 30 countries and territories with more than 90 percent contactless penetration and more than 90 countries where tap to pay is more than 50 percent of face-to-face transactions.” *Id.* “In the U.S., [VISA] has 28 percent contactless penetration and 495 million tap-to-pay-enabled Visa cards.” *Id.* “[VISA] ha[s] activated more than 600 contactless public transport projects worldwide.” *Id.* “In addition, [VISA] surpassed one billion contactless transactions on global transit systems in fiscal year 2022, an increase of 70% year over year.” *Id.*

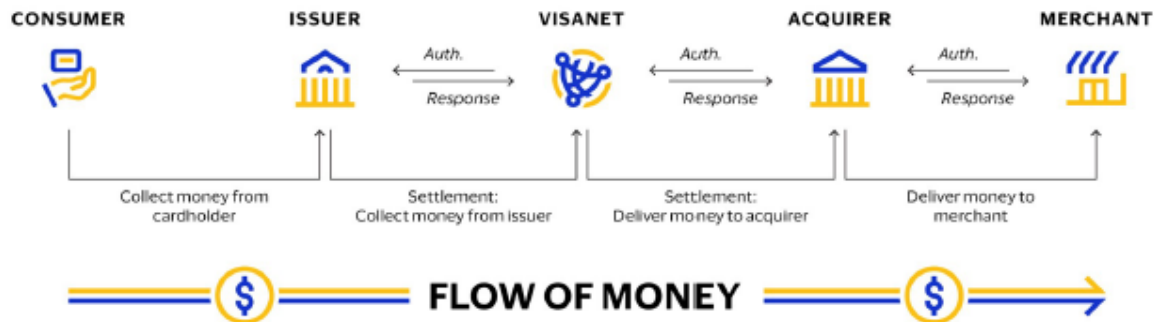
9. With respect to Tokenization, “[a]s consumers increasingly rely on digital transactions, [Visa Token Service] VTS is designed to enhance the digital ecosystem through improved authorization, reduced fraud and improved consumer experience.” *Id.* VTS operates to “protect digital transactions by replacing 16-digit Visa account numbers with a token that includes a surrogate account number, cryptographic information and other data to protect the underlying account information.” *Id.* “This security technology can work for a variety of payment transactions, both in the physical and online space.” *Id.*

10. [VISA’s] “provisioning of network tokens continues to accelerate.” *Id.* “As of the end of fiscal year 2022, [VISA] provisioned more than 4 billion network tokens, surpassing the number of physical cards in circulation.” *Id.*

11. On information and belief, the VISA Defendants, individually and via their subsidiaries and affiliates, “are focused on extending, enhancing and investing in [VISA’s]

proprietary network, VisaNet, to offer a single connection point for facilitating payment transactions to multiple endpoints through various form factors.” *Id.* at 4. Through VISA’s network, VISA Defendants offer “products, solutions and services that facilitate secure, reliable and efficient money movement for participants in the ecosystem.” *Id.* VISA Defendants contract with entities (“issuers”) that issue Visa Cards to cardholders and VISA Defendants facilitate transactions, for example, the flow of money, for cardholders, consumers, issuers, acquirers and merchants via processes that VISA Defendants refer to as “OUR CORE BUSINESS”:

OUR CORE BUSINESS



See id. at 5.

12. VISA Defendants state that their “Core Products” include, for example, “credit, debit and prepaid.” *Id.* at 7-8. VISA Defendants also enable transactions and payments in digital commerce and new technologies including “Tap to Pay” and “Tokenization,” for example, using Visa Token Service (VTS). *Id.* at 8. VISA Defendants state that their “Value Added Services” are services that “represent an opportunity for [VISA] to diversify [VISA’s] revenue with products and solutions that differentiate [VISA’s] network, deepen [VISA’s] client relationships and deliver innovative solutions across other networks.” *Id.* at 10. VISA Defendants indicate that VISA’s “Value Added Services” include “Issuing Solutions,” which, in turn, include VISA DPS. *Id.* VISA Defendants state:

“Visa DPS is one of the largest issuer processors of Visa debit transactions in the world. In addition to multi-network transaction processing, Visa DPS also provides a wide range of value added services, including fraud mitigation, dispute management, data analytics, campaign management, a suite of digital solutions and contact center services. Our capabilities in API-based issuer processing solutions, like DPS Forward, allow our clients to create new payments use cases and provide them with modular capabilities for digital payments.”

Id.

13. “[VISA] has established rules that are designed to minimize risks and provide a common, convenient, secure, and reliable global payment experience while supporting geography-specific rules that allow for variations and unique marketplace needs.” *Visa Core Rules and Visa Product and Service Rules*, VISA, Version 1.1 (17 August 2022), at 52, available at <https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf> (last visited December 2, 2022) [hereinafter “*Visa Core Rules*”]; *see also Visa Core Rules and Visa Product and Service Rules*, VISA, Version 1.1 (11 December 2020), available at https://resource.payrix.com/__attachments/23045734557/visa-rules-public.pdf?inst-v=43cab82-f941-44bd-9def-617b6f60e792 (last visited June 14, 2023) (showing the continuity of several required rules from 11 December 2020 to 17 August 2022). “They are set and modified by Visa to support the use and advancement of Visa products and services, and represent a binding contract between Visa and each Member.” *Id.* According to VISA’s *Visa Core Rules*, a “Member” includes, but is not limited to, any “client of Visa U.S.A.” *Id.* As used herein, Visa Requirements includes without limitation the Visa Charter Documents, Visa Core Rules, Visa Product and Service Rules, and any standards or requirements that VISA has established for those who use or access VISA’s products, methods, systems, brands, marks or property.

14. “The Visa Core Rules contain fundamental rules that apply to all Visa system participants and specify the minimum requirements applicable to all Members to uphold the safety, security, soundness, integrity, and interoperability of the Visa system.” *Id.* “The Visa Product and

Service Rules contain rules that apply to Visa system participants based on use of a product, service, the Visa-Owned Marks, VisaNet, the dispute resolution process, and other aspects of the Visa payment system.” *Id.* “The Visa Product and Service Rules also include operational requirements related to the Visa Core Rules.” *Id.* “The Visa Supplemental Requirements are Visa- or third-party-administered documents or websites that contain requirements beyond the content of the *Visa Core Rules and Visa Product and Service Rules* (for example: *Visa Product Brand Standards, BASE II Clearing Services, Visa Integrated Circuit Card Specification, Payment Card Industry (PCI) Card Production and Provisioning – Logical Security Requirements*).” *Id.*

15. “All participants in the Visa system are subject to and bound by the Visa Charter Documents and the Visa Rules, as applicable based on the nature of their participation and geography.” *Id.* at 55. “Any entity that accesses or uses a Visa system and/or service must both: [i] Restrict its use of the Visa system and/or service to purposes expressly approved by Visa [and] [ii] Comply with Visa requirements and documentation for system and/or service access and use.” *Id.* at 57.

16. With respect to VISA products and services, “[i]n the event any updates are made available to Members or if Visa requires a Member to make system changes, the Member must do all of the following: [i] Respond to and implement, as specified by Visa, the updates or system changes required by Visa [and] [ii] Ensure that its agreements with Cardholders, Merchants, Visa-approved manufacturers, Third-Party Personalizers, and agents allow for the implementation of updates or system changes required by Visa.” *Id.*

17. According to VISA’s *Visa Core Rules*, “An Acquirer must have a Merchant Agreement with each of its Merchants to accept Visa Cards and, if applicable, Visa Electron Cards.” *Id.* at 96. “A Payment Facilitator must have a Merchant Agreement with each of its Sponsored

Merchants.” *Id.* “The Merchant Agreement must include language that requires the Merchant to do all of the following: . . . Comply with the Visa Rules regarding use of the Visa-Owned Marks, Visa acceptance, risk management, Transaction processing, and any Visa products, programs, or services in which the Merchant is required to, or chooses to, participate . . . [and] [i]nclude the right of Visa to limit or terminate the Acquirer’s agreement with the Merchant or the Payment Facilitator’s agreement with the Sponsored Merchant. *Id.* at 97-97.

18. 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 December 12, 2022). 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, VISA co-owns EMVCo, along with five other member organizations, who each serve on EMVCo’s Board of Managers. *See id.*

19. On information and belief, VISA not only manages the development of the EMV specifications, it also requires its partners, issuers, acquirers, merchants, and other customers and clients to utilize EMV processes documented in the specifications during any VISA-based transaction using an account for any of the Visa Cards, including in contactless payments using a physical card or mobile device. According to VISA’s Visa Core Rules, “[a]ll Chip Card Issuers must perform, and be capable of acting on the results of, validation of EMV Online Card Authentication Cryptograms for all Chip-initiated Authorization messages processed through

VisaNet.” *Id.* at 218. “Online Card Authentication support may be provided by the Issuer directly, or through either: [i] VisaNet or [ii] Third party/VisaNet Processor or Visa Scheme Processor.” *Id.*

20. VISA also requires partners, issuers, acquirers, merchants, and other customers and clients to utilize EMV specifications specifically directed to the tokenization process. Per VISA’s requirements, “[i]f a Transaction is initiated with a Token, the Transaction must be submitted for Online Authorization,” and “[VISA] reserves the right to decline, on an Issuer’s behalf, a Transaction initiated with a Token if the Token does not comply with domain control requirements specified in the *EMV Payment Tokenisation Specification*.” *Id.* at 207. VISA establishes requirements for Acceptance Devices, which are “Card-reading device[s] managed by a Member or a Merchant for the purpose of completing a Visa Transaction.” *Id.* at 366-78, 801. For example, Contact Chip Acceptance Devices must be EMV-Compliant and approved by EMVCo and Contactless Chip Acceptance Devices be approved by EMVCo or VISA. *Id.* The Asserted Patents cover VISA’s products, services, and methods related to offering, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from transactions and payments, for example, via Visa Cards and associated accounts, which products, services and methods are designed, developed, manufactured, distributed, sold, offered for sale, and/or used by the VISA Defendants and/or their customers, licensees, partners, issuers, acquirers, merchants, consumers, and clients. For example, within VISA’s single reportable segment, Payment Services, Defendants infringe the Asserted Patents via at least VISA’s “CORE BUSINESS” of facilitating transactions and via VISA’s “Enablers” such as “Tap to Pay” and “Tokenization,” which are products, services and/or methods that allow VISA’s clients and consumers to conduct financial and banking transactions via Visa Cards and their associated accounts. *See 2022 Annual Report*, at 5-11; <https://usa.visa.com/pay-with->

[visa/contactless-payments/contactless-payments.html](https://usa.visa.com/contactless-payments/contactless-payments.html) (last visited Nov. 29, 2022); <https://usa.visa.com/pay-with-visa/featured-technologies/mobile-payments.html> (last visited Nov. 29, 2022); <https://usa.visa.com/pay-with-visa/featured-technologies/apple-pay.html> (last visited Nov. 29, 2022); <https://usa.visa.com/pay-with-visa/featured-technologies/google-pay-consumer.html> (last visited Nov. 29, 2022); <https://usa.visa.com/pay-with-visa/featured-technologies/samsung-pay-consumer.html> (last visited Nov. 29, 2022). Moreover, Defendants' infringing Visa Cards and associated systems and processes are compatible with application ("app")-based mobile payment methods via third-party services, such as Google Pay and Samsung Pay that are installed on a consumer's device, such as a mobile phone, tablet, or smartwatch. *See, e.g.,* <https://usa.visa.com/pay-with-visa/featured-technologies/mobile-payments.html> (last visited Nov. 29, 2022).

21. 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 Texas and this District, via at least their 1) physical offices in Texas, including this District; 2) VISA's online presence (e.g., [visa.com](https://usa.visa.com)) that provides VISA's clients and consumers with access to and/or markets VISA's products and services, including those identified as infringing herein; and 3) consumers and clients of VISA who utilize Visa Cards and associated products and 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 Visa Cards. *See, e.g., Find local businesses to support*, VISA.COM, <https://usa.visa.com/support/small-business/back-to-business-project.html> (last visited Nov. 29, 2022) ("Use the Back to Business search tool below to find and help local businesses that have processed a Visa transaction in the past 24 hours."). Such services associated with Visa Cards include systems and methods for

processing digital transactions via online transactions and mobile payment solutions. *See, e.g., 2022 Annual Report*, at 5-11. Defendants, on their own and/or via alter egos, agents, subsidiaries, partners, and affiliates, maintain at least one office in this District located at 12301 Research Blvd, Austin, Texas 78759 USA and 12401 Research Blvd, Austin, Texas 78759 USA, among other properties identified herein. On information and belief, this office is a location where Defendants, on their own and/or via alter egos, agents, subsidiaries, partners, and affiliates, maintain employees, including, for example, employees who develop VISA's payment processing products, systems and methods, which include without limitation systems used for payment via Visa Cards, VisaNet or other products, systems and methods that infringe the Asserted Patents. *See, e.g., Join our team*, VISA.COM, https://cw.visa.com/en_cw/jobs/?cities=Austin (last visited Nov. 30, 2022) (showing 51 job postings for Austin, Texas). Accordingly, VISA Defendants do business, including committing infringing acts, in the U.S., the state of Texas, and in this District.

JURISDICTION AND VENUE

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

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

A. Defendant VISA INC

24. On information and belief, Defendant VISA INC is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas 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 Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, partners, subsidiaries, clients, customers, affiliates, and/or consumers.

25. For example, VISA INC owns and/or controls multiple subsidiaries and affiliates, and at least one, including, but not limited to, Defendant VISA USA, has a significant business presence in the U.S. and in Texas. VISA INC, via its own activities and via at least wholly owned subsidiary VISA USA, has at least one office and/or global IT Center in Austin, Texas, in this District, at 12301 Research Blvd, Austin, Texas 78759 USA and 12401 Research Blvd, Austin, Texas 78759 USA. *See What Are the Largest Companies in Austin, Texas Today?*, AQUILACOMMERCIAL.COM, <https://aquilacommercial.com/learning-center/largest-companies-in-austin-texas-today/> (last visited Nov. 30, 2022); *Join our team*, VISA.COM, https://cw.visa.com/en_cw/jobs/?cities=Austin (last visited Nov. 30, 2022) (showing 51 job postings for Austin, Texas). Travis County CAD search results show that Defendant VISA INC's subsidiary VISA USA is listed as the owner of the property at VISA's office or offices at 12301 and 12401 Research Blvd in Austin, Texas. *See Property Search*, TRAVIS CENTRAL APPRAISAL DISTRICT, <https://stage.travis.prodigycad.com/property-search> (last visited Nov. 30, 2022) (search for "visa inc"). VISA USA is registered to do business in Texas and is 100% owned by VISA INC. On information and belief, VISA's at least one office and/or Global IT Center employs nearly 2,000 or more residents of the state of Texas and this District. *See, e.g., Visa grows tech center in North Austin*, BIZJOURNALS.COM, <https://www.bizjournals.com/austin/news/2019/05/14/visa-grows-tech-center-in-north-austin.html> (May 15, 2019) (last visited Dec. 1, 2022); *Visa to hire 400 new employees at Austin office*, KCAN.COM <https://www.kxan.com/news/visa-to-hire-400-new-employees-at-austin-office>,

employees-at-austin-office/ (Mar. 20, 2015) (last visited Nov. 30, 2022). Moreover, numerous issuers provide Visa Cards that are issued pursuant to a license from VISA USA, a wholly-owned subsidiary of VISA INC, for consumers in Texas and in this District. Additionally, VISA payment applications are stored on mobile devices, smart phones, tablets and computer chips embedded on Visa Cards used in transactions in Texas and in this District. VISA payment applications utilize tokenization processes for facilitating transactions, including, for example, payments. Further, on information and belief, infringing Visa DPS products, including, for example, issuer processing services, are advertised, offered, sold, made available, used, and provided in Texas and in this District. *See, e.g., Visa DPS*, VISA.COM, <https://usa.visa.com/sites/visa-dps.html> (last visited May 17, 2023) (stating “Grow your business with a trusted partner,” “[I]inking issuers to the payments ecosystem and managing network compliance,” and “[a]t Visa DPS, we handle more than 40 billion transactions¹ every year for more than 190 million active cards. We connect issuers to the networks they choose, making payments a breeze.”).

26. Such a corporate and commercial presence in Texas, including in this District, by Defendant VISA INC furthers the development, design, manufacture, distribution, sale, and use of VISA INC’s and VISA’s infringing products, services, and methods for offering, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from transactions via Visa Cards and associated accounts. Through direction and control of its alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers, VISA INC has committed acts of direct and/or indirect patent infringement within Texas, this District, and elsewhere in the United States, giving rise to this action

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

27. On information and belief, VISA INC directs and controls and/or otherwise directs and authorizes all activities of its alter egos, intermediaries, agents, subsidiaries, and affiliates, including, but not limited to Defendant VISA USA and Visa DPS. *See, e.g., 2022 Annual Report*, at 10, 59 (“All significant operating decisions are based on analysis of [VISA] as a single global business. Accordingly, the Company has one reportable segment, Payment Services.”). Via its own activities and via at least these entities, VISA INC has substantial business operations in Texas, which include without limitation the provision of products, methods and services, for example, payment processing services, to various entities including without limitation partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers. VISA INC has placed and continues to place infringing products, services, and methods for offering, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from commercial transactions via Visa Cards and associated accounts, including without limitation related mobile, contactless, and online payment systems, into the U.S. stream of commerce. VISA INC has placed such products, services, and methods into the stream of commerce with the knowledge and understanding that such products are, will be, and continue to be sold, offered for sale, and/or used in this District and the State of Texas. *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.”).

28. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391 and 1400(b). As alleged herein, Defendant VISA INC has committed acts of infringement in this District. As further alleged herein, Defendant VISA INC, via its own operations and employees located there and via

ratification of Defendant VISA USA's presence and/or the presence of other subsidiaries as agents and/or alter egos of VISA INC, has a regular and established place of business, in this District at least at an office and/or global IT center located at 12301 Research Blvd, Austin, Texas 78759 USA and 12401 Research Blvd, Austin, Texas 78759 USA. Accordingly, VISA INC may be sued in this district under 28 U.S.C. § 1400(b).

B. Defendant VISA USA

29. On information and belief, Defendant VISA USA is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas 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 Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas 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, VISA USA, including as an agent and alter ego of parent company VISA INC, is listed as the owner of the property at VISA's office or offices at 12301 and 12401 Research Blvd in Austin, Texas. *See Property Search, TRAVIS CENTRAL APPRAISAL DISTRICT, <https://stage.travis.prodigycad.com/property-search> (last visited Nov. 30, 2022) (search for "visa inc")*. The at least one office and/or global IT center in Austin, Texas, employs nearly 2,000 or more employees that develop and/or provide products, services, and methods that include VISA INC and/or VISA USA offering, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from services

related to Visa Cards, via Visa Cards and associated accounts, including without limitation related mobile, contactless, and online payment systems, for VISA's customers, consumers, and clients in Texas and this District. *See, e.g., What Are the Largest Companies in Austin, Texas Today?*, AQUILACOMMERCIAL.COM, <https://aquilacommercial.com/learning-center/largest-companies-in-austin-texas-today/> (last visited Nov. 30, 2022); *Join our team*, VISA.COM, https://cw.visa.com/en_cw/jobs/?cities=Austin (last visited Nov. 30, 2022) (showing 51 job postings for Austin, Texas). Moreover, numerous issuers provide Visa Cards that are issued pursuant to a license from VISA USA for consumers in Texas and in this District. Additionally, VISA payment applications are stored on mobile devices, smart phones, tablets and computer chips embedded on Visa Cards used in transactions in Texas and in this District. VISA payment applications utilize tokenization processes for facilitating transactions, including, for example, payments.

30. On information and belief, VISA INC and VISA USA require any entity that accesses or uses a VISA system and/or service, for example, all merchant systems handling Visa-based transactions, conform to the applicable requirements, for example, EMV standards, when effecting those transactions. Through direction and control of its alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers, VISA USA has committed acts of direct and/or indirect patent infringement within Texas, this District, and elsewhere in the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over VISA INC would not offend traditional notions of fair play and substantial justice.

31. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). Defendant VISA USA has committed acts of infringement in this District. As further alleged herein,

Defendant VISA USA, via its own operations and employees located there and/or via ratification of its subsidiaries as agents and/or via alter egos of VISA USA, has a regular and established place of business, in this District at least at an office and/or global IT center located at 12301 Research Blvd, Austin, Texas 78759 USA and 12401 Research Blvd, Austin, Texas 78759 USA. Accordingly, VISA USA may be sued in this district under 28 U.S.C. § 1400(b).

32. Upon information and belief, Defendants VISA INC and VISA USA each have significant ties to, and presence in, the State of Texas and this District making venue in this District both proper and convenient for this action.

THE ASSERTED PATENTS AND TECHNOLOGY

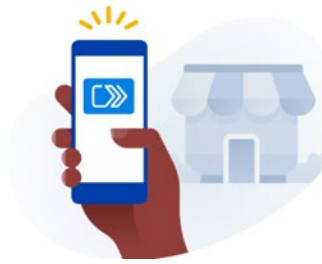
33. The Asserted Patents cover various aspects of products, systems, services, and methods that include Defendants' providing, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from financial transactions and payments for accounts for Visa Cards and related products, processes, and services for Defendants' licensees, partners, customers, consumers, and clients, including Defendants' internal payment processing, authentication, authorization, validation, and fraud detection systems and methods, referred to herein collectively as the "Accused Instrumentalities."

34. The Asserted Patents cover Accused Instrumentalities of Defendants that facilitate, maintain, transact, authenticate, validate, reconcile, and process financial data, financial transactions, mobile payments, contactless payments, and online payments using Visa Cards and related access to Visa's payment networks, APIs, software development kits, Visa DPS system, Visa DPS services and other product solutions licensed by Defendants to their licensees, issuers, acquirers, partners, and clients. Defendants use the Accused Instrumentalities to process financial data and transactions, including, for example, reconciling financial data. Additionally, Defendants use the Accused Instrumentalities to facilitate the issuance of accounts (for cardholders of Visa

Cards) by, for, and/or to Defendants' licensees and partners, consumers, and customers and clients of Defendants. Cardholders then use the accounts to conduct financial transactions, e.g., make purchases via mobile payment, contactless payment, or online payments. Defendants provide their payment network, i.e., VisaNet, to process such payments. At the point of purchase, Defendants further provide digital solutions, including offering mobile wallets for contactless payments to cardholders (via Defendants' licensees) which are installed onto a mobile device of a cardholder. Such mobile wallets include an appropriate Visa smartcard, API, and/or app installed on the mobile device (and in some cases, the software is native to the device). Defendants also provide to cardholders (via Defendants' licensees) 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 is registering, activating, or maintaining the account.

35. On information and belief, Defendants' account services for Visa 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 Visa 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 wallets applications such as Google Pay, Samsung Pay, and Visa's Click to Pay, which include software, APIs, or firmware provided by Defendants, such as shown below:

Visa Click to Pay



Deliver an easy, smart, and secure checkout experience

Visa enables you to build a simple and secure digital checkout experience. Using EMV® standards for Secure Remote Commerce (SRC), Visa is moving towards an open, best practices approach with the goal of improving security, interoperability, and user experience.

See *Visa Click to Pay*, VISA DEVELOPER CENTER, <https://developer.visa.com/capabilities/visa-secure-remote-commerce> (last visited November 29, 2022).

36. 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/>

37. On information and belief, VISA is not only using and infringing the claimed inventions, which utilize EMV, VISA is responsible for developing the EMV standard. In other words, from VISA's development of the standard to its implementation and use, Visa is deeply involved in steps that individually, or in combination with other actions, including via direction and control of third parties, result in infringement of the Asserted Patents.

38. On information and belief, as indicated below, Defendants provide their payment technology to their licensees, issuers, acquirers, partners, and clients who in turn provide accounts for Visa Cards to consumers, customers, cardholders, and other users. These payment products utilize Visa's In-App Provisioning to implement digital wallet services (e.g., Google Pay and Samsung Pay) that provides a distribution channel by which Defendants' payment applications (e.g., via the Secure Element on the mobile device) can be accessed and used.

Visa In-App Provisioning

Provision to major mobile pay wallets from your banking application



Implementing push provisioning is now easier than ever



It's now easier than ever to digitally activate newly issued digital cards, and accelerate adoption of mobile payment wallets for an existing card portfolio. Visa In-App Provisioning helps issuers and partners such as Mobile App Developers, Processors, Fintechs and Solution Providers to more easily implement a "Add to Apple Pay¹, Google Pay² or Samsung Pay³⁺ button in mobile banking applications.

See *Visa In-App Provisioning*, VISA DEVELOPER CENTER, <https://developer.visa.com/capabilities/visa-in-app-provisioning> (last visited November 29, 2022).

39. The Accused Instrumentalities also include at least Visa Cards; related products, processes, services, and methods for card payments using a physical banking, payment, credit, debit, or prepaid card having an embedded chip or smartcard; mobile payment systems (e.g., mobile wallets) and methods using Visa Cards to conduct transactions over the internet and/or mobile devices, including, for example, smart phones, tablets, and computers; and systems and methods provisioned, directly or indirectly, by VISA Defendants with tokens that can be used in the place of or in combination with primary account numbers to conduct transactions (collectively, all Accused Instrumentalities listed in this sentence are herein referred to as “Visa Transaction Instruments”). See *Visa Credit Cards*, VISA, <https://usa.visa.com/pay-with-visa/find-card/apply-credit-card> (listing issuer-branded Visa Cards) (last visited Nov. 29, 2022). For example, as indicated below, Defendants’ payment applications reside on microchips embedded on Visa 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.




See Tap to Pay with Visa contactless payments, VISA, <https://usa.visa.com/pay-with-visa/contactless-payments/contactless-payments.html> (last visited Nov. 29, 2022).

40. On information and belief, the Accused Instrumentalities include at least Defendants' payment card (e.g., banking, credit, debit, and prepaid card) related products, services, and methods for contactless payments that utilize EMV standards for contactless payment. *See, e.g., id.* ("The EMVCo Contactless Indicator" ) indicates acceptance. When featured on a card, it means the card can be used to tap to pay."). Defendants' Visa Cards include EMV compliant contactless payment functionality indicated by the "Contactless Indicator"  which appears prominently on the cards.



See *Contactless payments provide your cardholders with a secure, convenient and touch-free way to pay*, VISA, <https://usa.visa.com/partner-with-us/payment-technology/contactless-payments/contactless-for-issuers.html> (explaining to issuers of VISA’s card products that “Cardholders can pay with a contactless card by holding the card flat and tapping it at a contactless-enabled checkout terminal.”) (last visited Nov. 30, 2022).


41. 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.

Reader = 

↕

Form Factor = 

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

42. 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 Visa 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>

43. 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>

44. Defendants, as licensors of technology to account issuers for Visa Cards and merchant acquirers involved in transactions associated with Visa Cards, direct and control the activities of third parties, including, but not limited to, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, consumers, and cardholders, in the operation of the Visa Transaction Instruments using the Visa payment network. Defendants direct and control the infringing activities of third parties by conditioning and permitting the use of Visa Cards and Visa 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 network, i.e., the VisaNet, Defendants further direct and control the activities of third parties in infringing the Asserted Patents. For example, Defendants require that third parties use “the quick Visa Smart Debit/ Credit (qVSDC) transaction path,” i.e., a Visa Transaction Instrument, as part of “Visa’s EMV-based contactless solution” in order to process Visa Card transactions on the VisaNet network. *EMV® Chip News*, VISA (May 2019), at 1, available at <https://usa.visa.com/dam/VCOM/regional/na/us/run-your-business/documents/emv-newsletter-may2019.pdf> (last visited June 1, 2023). According to VISA Defendants:

qVSDC is Visa’s solution for contactless card acceptance. qVSDC is a minimized EMV contact-chip transaction over the contactless interface where multiple EMV commands are compressed into as few commands as possible to streamline and expedite transaction processing. All newly issued Visa contactless cards and newly deployed contactless readers are required to support qVSDC.

VSDC Contact & Contactless, VISA, Version 3.0 (Effective: June 2020), at 1, available at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjIi9XbpY7_AhW5lmoFHdTbBAk4ChAWegQIAxAB&url=https%3A%2F%2Ftechnologypartner.visa.com%2FDownload.aspx%3Fid%3D574&usg=AOvVaw026klfm6c8RUzIfOo2tJv5 (last visited June 1, 2023).

45. Additionally, the *Visa Core Rules* indicate that, among other requirements, “Support for [the] qVSDC Transaction Path” is “Required” for “Contactless Payment Devices issued or replaced on or after: 1 October 2015” in the “US Region.”

4.1.19.10 Contactless Issuer Requirements

A Contactless Payment Device Issuer must comply with the following:

Table 4-10: Contactless Payment Device Issuer Requirements

Applies to Contactless Payment Devices issued or replaced on or after:	Region/Country	Required VCPS Version	Support for qVSDC Transaction Path	Support for MSD Transaction Path	Form Factor Indicator
...					
1 October 2015	Canada Region, US Region	2.1 or later	Required	Optional	Required

Visa Core Rules 4.1.19.10.

46. VISA Defendants have established various other requirements as can be seen from the following passages in the *Visa Core Rules*.

4.1.19.33 Mobile Payment Devices – Issuer Requirements

An Issuer of a Mobile Payment Device must both:

- Register with Visa
- Ensure that the Mobile Payment Device is approved by Visa

An Issuer may use any of the following:

- A Visa-approved secure element and a Visa-approved Visa Mobile Payment Application
- A Visa-approved cloud-based payments Visa Mobile Payment Application

4.1.19.38 Visa Contactless Application Requirement – AP Region (Australia, Malaysia), Canada Region, and US Region

In the AP Region (Australia, Malaysia), US Region: An Issuer that issues a Card with contactless payment capability must enable the Visa Contactless Application on the Card.

4.1.19.54 Visa-Owned Chip Technology Use

Visa-owned Chip technology must be used solely for the purpose of facilitating a Visa Transaction, Interlink transaction, Visa Electron Transaction, or Plus Transaction.¹ Any other use requires the prior written permission of Visa.

Visa-owned Chip technology includes, but is not limited to, all of the following:

- Visa Integrated Circuit Card Specification
- Visa Smart Debit/Credit (VSDC) applet
- Visa Contactless Payment Specification
- Visa Mobile Contactless Payment Specification
- Visa Cloud-Based Payments Contactless Specification
- Visa Mobile Payment Application
- Visa, Interlink, Visa Electron, and Plus Payment Application Identifiers

4 Issuance

4.1 General Issuance

4.1.1 General Issuer Requirements

4.1.1.1 Card and Token Positioning

...

An Issuer must ensure that a Token both:

- Maintains the same product characteristics of the Card represented by that Token
- Is presented to the Cardholder as a Visa product or service

If an Issuer provisions a non-Visa payment credential³ for a co-resident network on a Card, it must also both:

- Provision a Visa Token before or at the same time as the non-Visa payment credential³
- Ensure that the applicable Token Requestor has received Visa Token Service approval of its digital wallet or other payment solution

Visa Core Rules 4.1.1.1, 4.1.19.33, 4.1.19.38, 4.1.19.54.

47. Additionally, Defendants, as licensors of payment card technology to account issuers of Visa Cards and merchant acquirers involved in transactions associated with Visa Cards, direct and control 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

48. As an example of how Defendants direct and control mobile wallets, Defendants provision third-party mobile wallets with Defendants' own credentials and EMV payment applications, e.g., via Visa's "Token Service."



Pay your way with Google Pay™

Google Pay is the fast, simple way to pay with your eligible, enrolled Visa card in stores and in-app. And you'll continue receiving all the benefits and protections you enjoy with Visa.

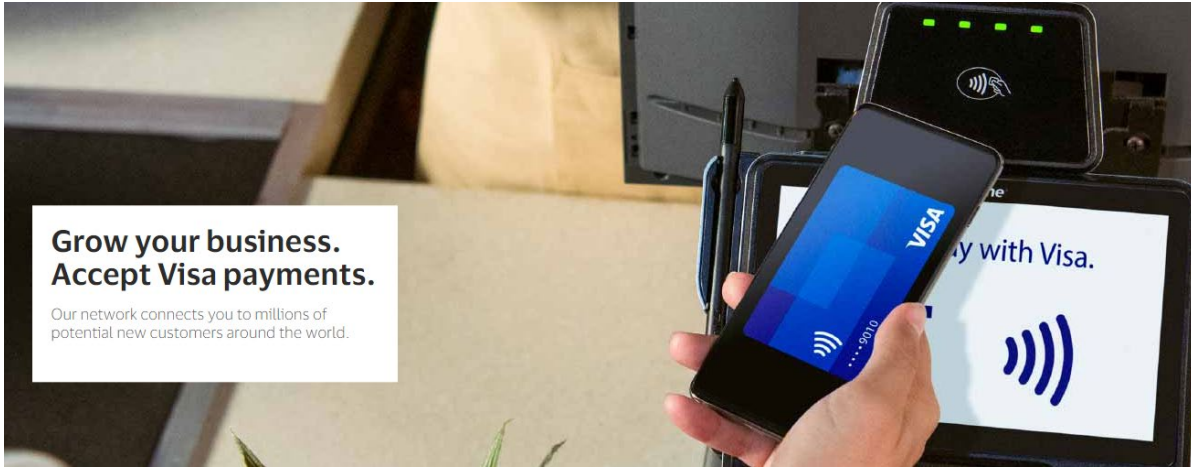
[Get the app](#) 

Google Pay with Visa Token Service is compatible on Android devices that support HCE.

Confident Payments with Google Pay™ and Visa Cards, VISA, <https://usa.visa.com/pay-with-visa/featured-technologies/google-pay-consumer.html> (last visited Nov. 30, 2022).

49. Accordingly, VISA Defendants use at least agreements, the required implementation of specified protocols, and/or design of products, software, and applications to condition participation in an activity or receipt of a benefit, for example, access to and use of VISA's products and systems, upon performance of a step or steps of a patented method and establish the manner or timing of that performance.

50. The Accused Instrumentalities include Defendants' providing, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from financial transactions and payments for accounts for Visa Cards and related products, processes, and services for Defendants' licensees, acquirers, partners, customers, consumers, and clients, including Defendants' internal payment processing, authentication, authorization, validation, and fraud detection systems and methods, related to at least Defendants' card products (e.g., Visa Cards).



See *Grow your business. Accept Visa payments.*, VISA, <https://usa.visa.com/run-your-business/accept-visa-payments.html> (“Our network connects you to millions of potential new customers around the world.”) (last visited Nov. 30, 2022).

51. The Accused Instrumentalities also include at least Defendants’ financial data and transaction processing products and services. See *Visa DPS*, VISA, <https://usa.visa.com/sites/visa-dps.html> (describing Visa DPS services) (last visited May 17, 2023). For example, as indicated below, Defendants’ Visa DPS products provide financial data and transaction processing.



Grow your business with a trusted partner

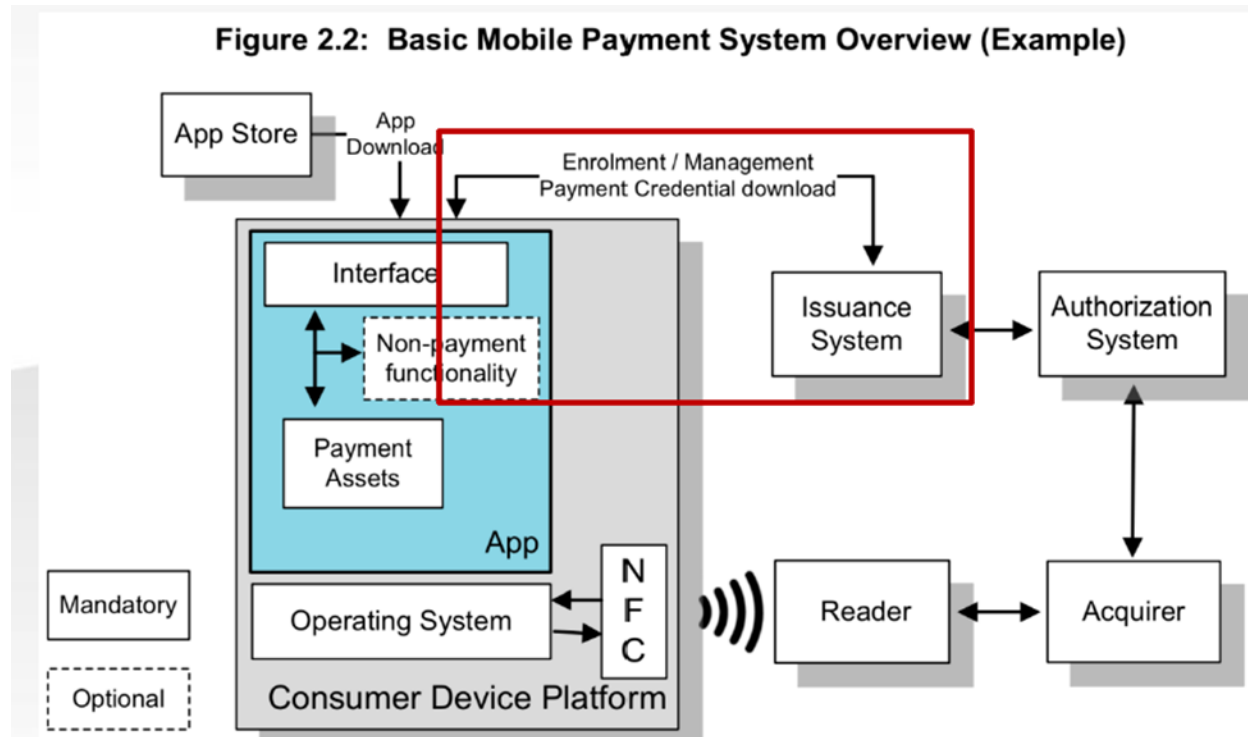
For more than two decades, we’ve worked hard to make processing easier for our issuing customers. Visa DPS helps you stay innovative, stay agile and deliver at scale. In today’s market, this is a critical need. Visa DPS can connect you to a payments universe and support your payment processing needs, from speed to authorization and fraud protection, and more.

See id.

52. 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 Visa Cards to secure direct and safe transactions between consumers and merchants.

53. Defendants infringe the '671 patent via Defendants' computer-based systems that conduct user enrollment processes for mobile wallet payments associated with Visa Cards and via direction and control of third parties in connection with these systems. 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 direct and control third parties, including issuers and vendors, to configure the mobile wallets of cardholders to conform to EMV standards. As part of utilizing a consumer's mobile wallet, Defendants direct and control the

activities of third parties, including issuers and vendors, to conduct an enrollment process, which forwards a challenge to a cardholder’s mobile device, i.e., an intelligent token, as shown below.



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

54. 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

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

2.1.1 Issuer Master Keys and Data

EMV personalization cannot take place unless the card issuer creates master keys and other specific data. The master keys are used in two ways, firstly to support secure transmission of personalization data and secondly to create application-level data for personalization of an EMV application. Some of the data may be used to manage the personalization process and some will be placed on the card during personalization.

EMV Card Personalization Specification, Version 1.1 July 2007

Data Preparation

Data preparation is the process that creates the data that is to be placed in an IC card application during card personalization. Some of the data created may be the same across all cards in a batch; other data may vary by card. Some data, such as keys, may be secret and may need to be encrypted at all times during the personalization process.

56. 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. As described below, Defendants validate the consumer's credentials using the 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

https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_4_Other_Interfaces_20120607062305603.pdf

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:

https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_2_Security_and_Key_Management_20120607061923900.pdf

57. 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

58. The Accused Instrumentalities of Defendants infringe at least the 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 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.

59. Defendants infringe the '985 patent via Defendants' 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. 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

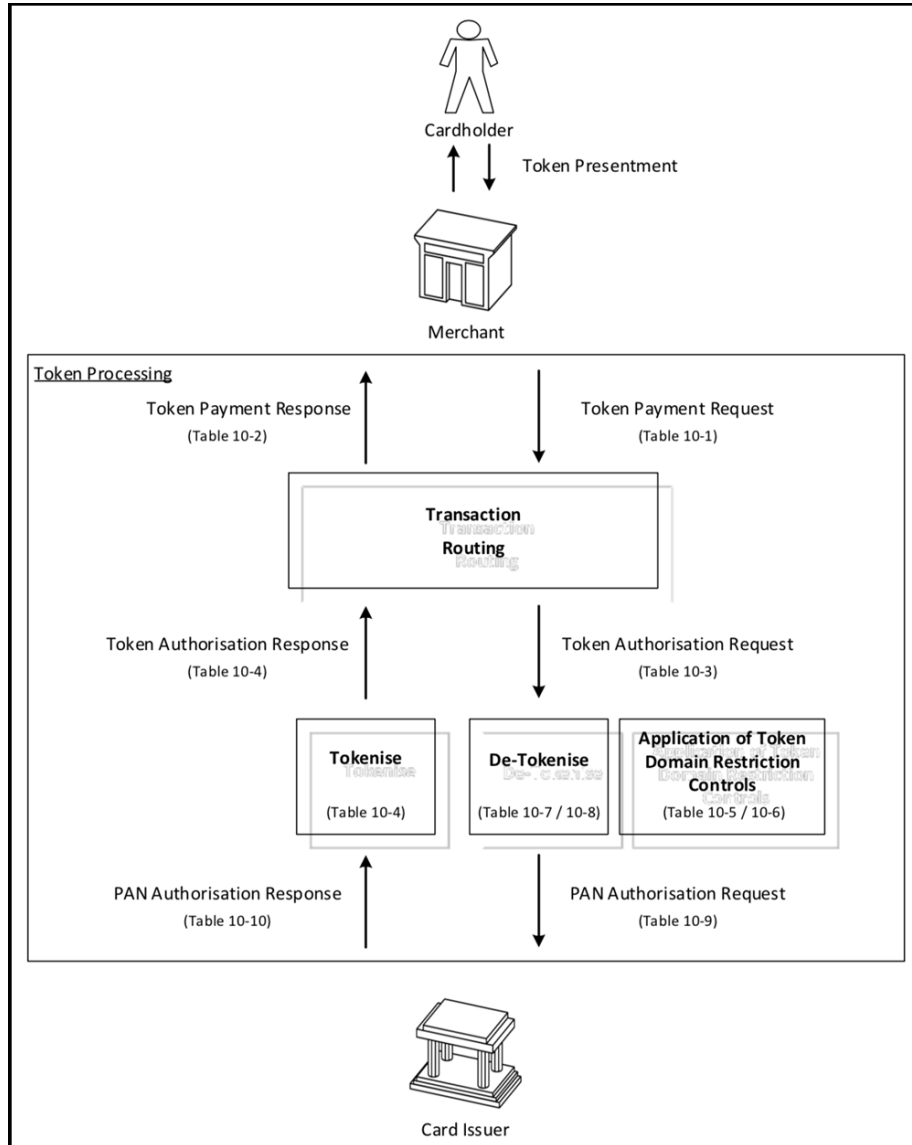
Visa Cards. Transactions associated with Visa Cards made online by consumers may also utilize virtual account numbers via “tokenization,” as shown below in relation to Google Pay.

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>

60. 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.



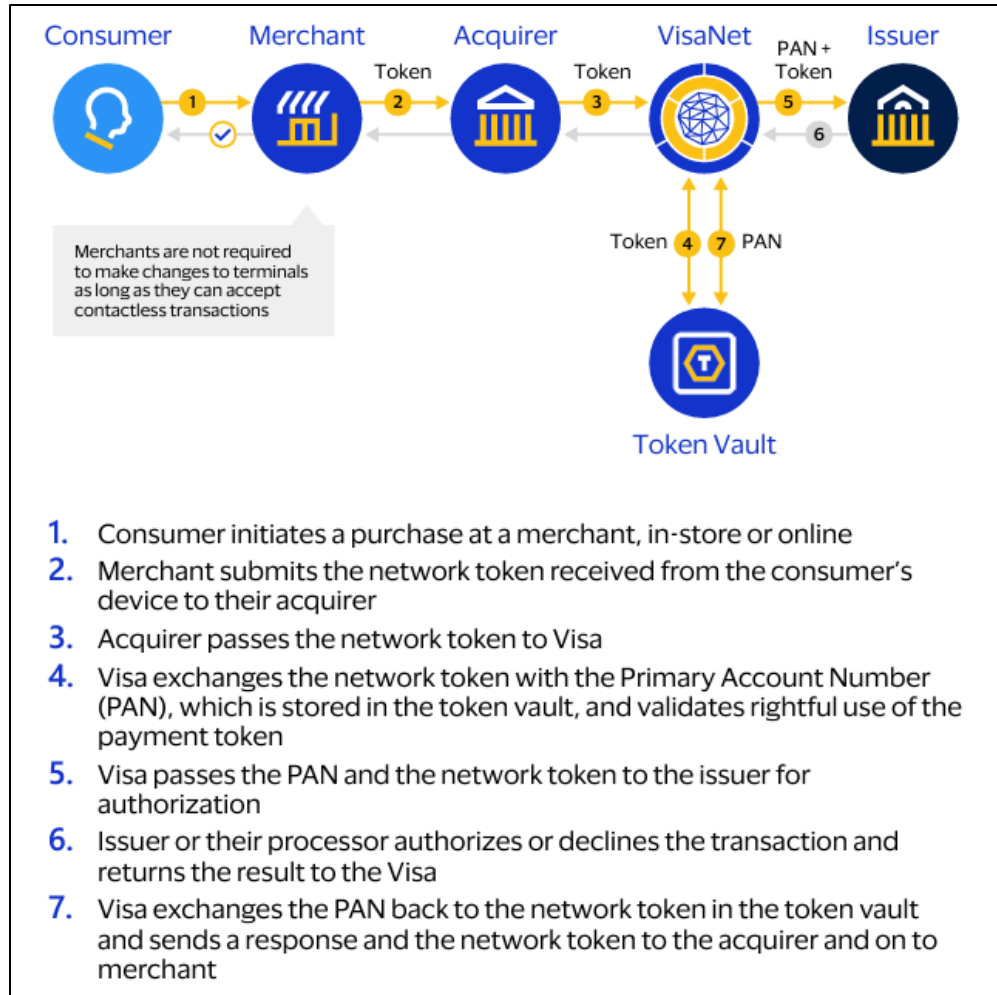
Token Payment Request: includes the request that originates from the point of interaction with the Merchant (such a Terminal, website or application) and the response that provides the results of the authorisation decision

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

61. 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.

<p>Payment Token</p>	<p>An existing payment processing field that is passed through the authorisation, capture, clearing, and exception messages in place of the PAN.</p> <p>After De-Tokenisation, the Payment Token is replaced with the underlying PAN. The PAN is then passed to the Card Issuer as part of the PAN Authorisation in this field.</p> <p>The Payment Token may optionally be passed to the Card Issuer as part of the PAN Authorisation using a Payment Network specific Token Processing field.</p>
<p>De-Tokenisation: includes the request and corresponding response processing converting a Payment Token and Token Expiry Date to an underlying PAN and PAN Expiry Date. De-Tokenisation may or may not include the application of Token Domain Restriction Controls</p>	
<p><i>EMV Payment Tokenisation Specification, Technical Framework v2.0, September 2017</i></p>	

62. As shown below, Visa, via its VisaNet, provides token processing for financial transactions by “exchang[ing] the network token with the primary account number (PAN), which is stored in [Visa’s] token vault, and validates rightful use of the payment token.”



See *Product Fact Sheet Visa Token Service*, VISA, accessible via <https://usa.visa.com/dam/VCOM/global/products/documents/visa-token-service-fact-sheet.pdf> (last visited December 29, 2022).

63. As part of their analysis of data associated with the transaction, Defendants “pass the PAN and the network token to the issuer for authorization.” *Id.* Data analyzed by Defendants indirectly, directly and in some cases jointly with (i.e., 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, as explained below in relation to an EMV-type transaction.

10.9 Online Processing

Purpose:

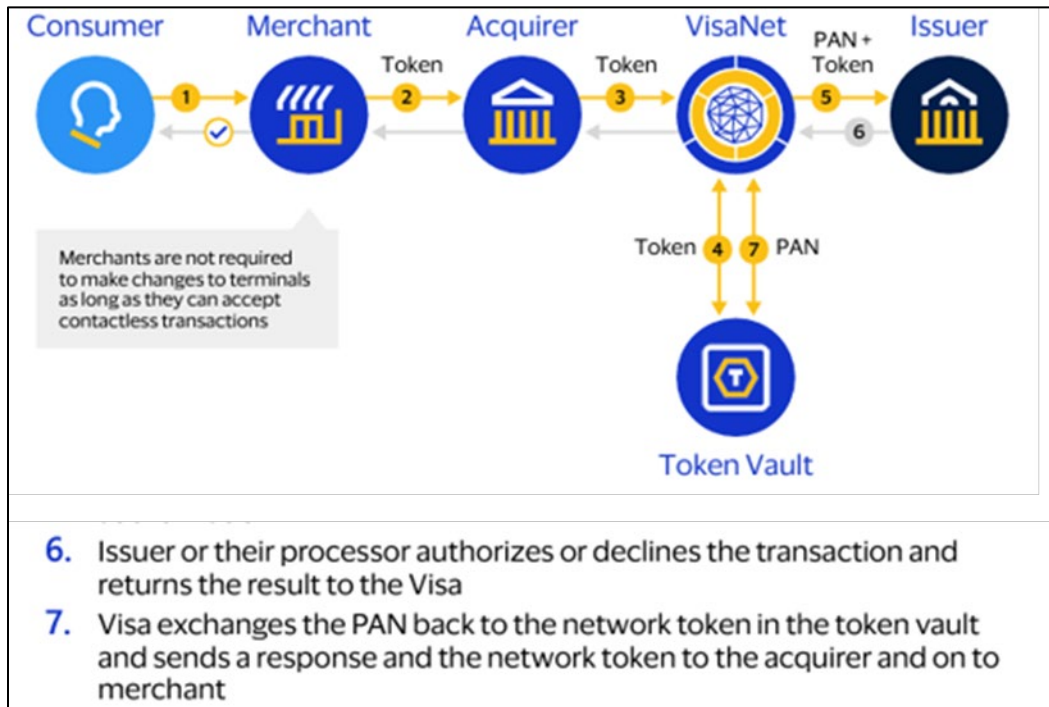
Online processing is performed to ensure that the issuer can review and authorise or reject transactions that are outside acceptable limits of risk defined by the issuer, the payment system, or the acquirer.

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

https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_2_Security_and_Key_Management_20120607061923900.pdf

64. The issuer returns the authorization result back to Visa, which then sends a response to the acquirer and merchant.



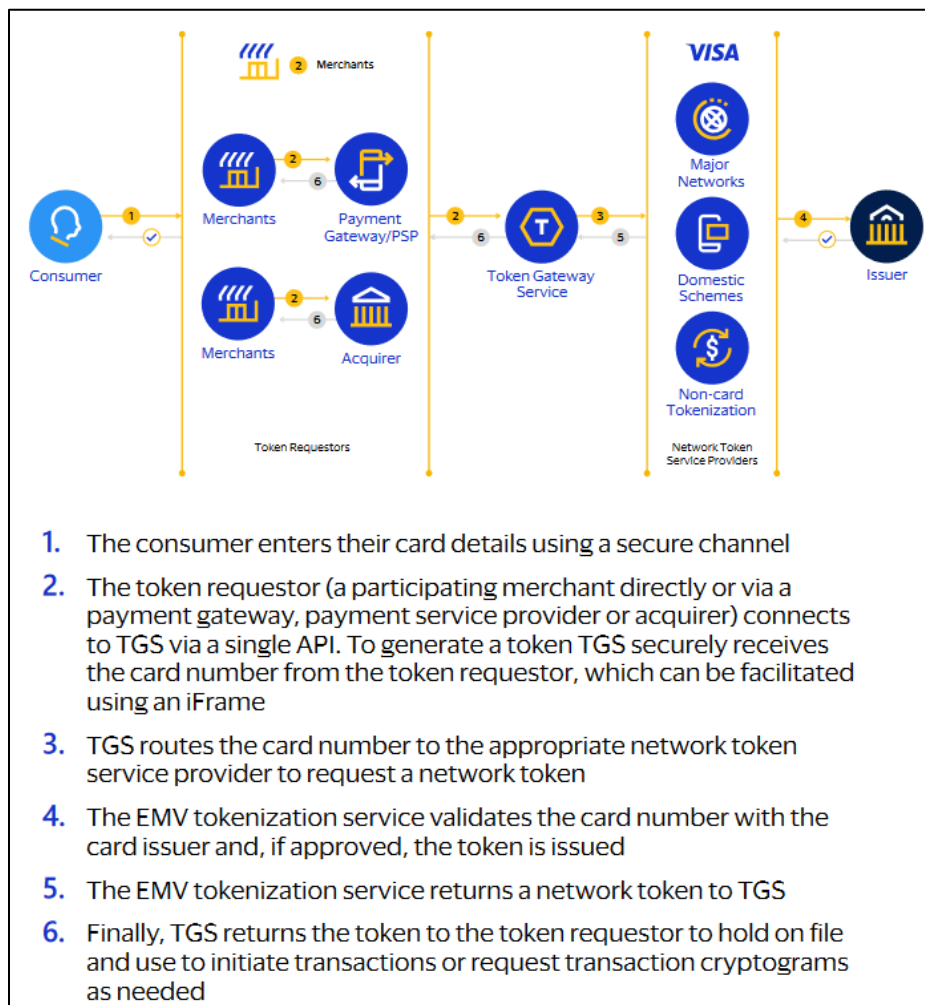
See Product Fact Sheet Visa Token Service, VISA, accessible via <https://usa.visa.com/dam/VCOM/global/products/documents/visa-token-service-fact-sheet.pdf> (last visited December 29, 2022).

65. The Accused Instrumentalities of Defendants directly and 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.

66. 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.

67. As shown below, Defendants infringe the '938 patent by creating virtual account numbers, i.e., tokens, for accounts for Visa Cards and/or directing and controlling the actions of third parties in connection with the creation of these virtual account numbers. Visa utilizes its Token Gateway Service as an intermediary to “receive[] the card number from the token requestor,” and “return[] the token to the token requestor.”



See VisaNet | Electronic Payments Network, VISA, accessible via <https://usa.visa.com/about-visa/visanet.html> (last visited Nov 28, 2022).

68. The virtual account numbers, created and utilized by Defendants’ Token Service, must begin with the same Issuer Identification Number 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., Visa) to route transaction information.



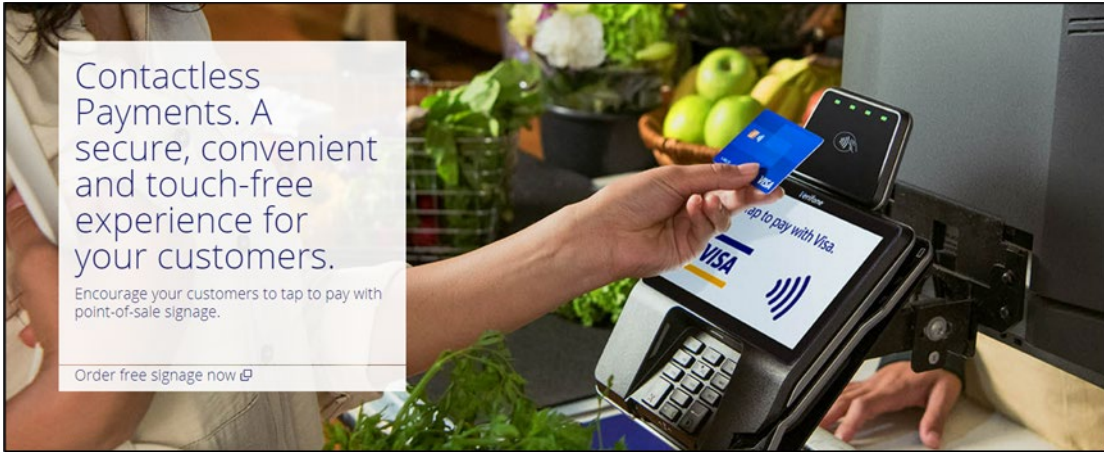
69. Defendants provide these virtual account numbers to token requestors, including merchants and acquirers, who directly or indirectly “hold [the tokens] on file to initiate transactions.”




70. The Accused Instrumentalities of Defendants infringe at least the 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 at least the claims of the '756 patent via at least their providing directly and indirectly the Visa payment ecosystem that facilitates securing RFID transactions, including directing and controlling third parties which use the Visa payment ecosystems or provide the Visa payment ecosystems to consumers, such as at least providing merchant systems, to issuers, acquirers, merchants, and consumers that participate in Visa's Mobile Point of Sale (mPOS) program. Defendants also infringe the claims of the '756 patent by requiring, via the Visa Requirements, that any entity that accesses or uses a Visa system and/or service, for example, all merchant systems handling Visa-based transactions, conform to the applicable requirements, for example, EMV standards, when effecting those transactions (e.g., RF transactions).




<https://usa.visa.com/run-your-business/small-business-tools/payment-technology/contactless-payments.html>



Visa Contactless Chip Cards

If your Visa card features the Contactless Indicator  on either the front or back, you can use it to tap to pay where you see the Contactless Symbol  at many of your favorite stores.



Devices

Don't have a contactless chip card? You can still tap to pay by loading an eligible payment card into your payment-enabled phone or wearable device.

[Learn more about Visa + Apple Pay >](#)
[Learn more about Visa + Google Pay >](#)
[Learn more about Visa + Samsung Pay >](#)
[Learn more about Wearables >](#)

<https://usa.visa.com/pay-with-visa/contactless-payments/contactless-payments.html>

<u>Applies to Contactless Payment Devices issued or replaced on or after:</u>	Region/Country	Required VCPS Version	<u>Support for qVSDC Transaction Path</u>	Support for MSD Transaction Path	Form Factor Indicator
1 October 2015	AP Region, CEMEA Region, Europe Region, LAC Region	2.1 or later	Required	Not permitted, except for Mobile Payment Devices	Required
<u>1 October 2015</u>	Canada Region, <u>US Region</u>	2.1 or later	<u>Required</u>	Optional	Required

<https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf>

Quick Chip for EMV and qVSDC — Specification

This specification introduces modifications to the use of standard processes for contact chip transactions that is compatible with EMV kernels and optimizes processing time by removing or reducing dependencies for chip insertion time in the reader, referred to as Quick Chip.

Version 2 of this specification adds guidance for supporting EMV contactless, i.e., qVSDC (quick Visa Smart Debit Credit), with Quick Chip.


<https://usa.visa.com/dam/VCOM/regional/na/us/run-your-business/documents/quick-chip-emv-specification.pdf>

<p>The Visa Rules</p> <p>The Visa Core Rules and Visa Product and Service Rules</p> <p>Introduction to the Visa Core Rules and Visa Product and Service Rules</p> <p>Visa has established rules that are designed to minimize risks and provide a common, convenient, secure, and reliable global payment experience while supporting geography-specific rules that allow for variations and unique marketplace needs. They are set and modified by Visa to support the use and advancement of Visa products and services, and represent a binding contract between Visa and each Member.</p> <p>The Visa Core Rules contain fundamental rules that apply to all Visa system participants and specify the minimum requirements applicable to all Members to uphold the safety, security, soundness, integrity, and interoperability of the Visa system.</p> <p>The Visa Product and Service Rules contain rules that apply to Visa system participants based on use of a product, service, the Visa-Owned Marks, VisaNet, the dispute resolution process, and other aspects of the Visa payment system. <u>The Visa Product and Service Rules also include operational requirements related to the Visa Core Rules.</u></p> <p>The Visa Supplemental Requirements are Visa- or third-party-administered documents or websites that contain requirements beyond the content of the <i>Visa Core Rules and Visa Product and Service Rules</i> (for example: <i>Visa Product Brand Standards, BASE II Clearing Services, Payment Card Industry (PCI) Card Production and Provisioning – Logical Security Requirements</i>).</p>	<p>1.1.1.7 Restricted Use of Visa Systems and Services</p> <p><u>Any entity that accesses or uses a Visa system and/or service must both:</u></p> <ul style="list-style-type: none"> Restrict its use of the Visa system and/or service to purposes expressly approved by Visa <u>Comply with Visa requirements and documentation for system and/or service access and use</u> <p>8.4.1 Mandatory Functionality for EMV Terminals</p> <p>The EMV Specifications include mandatory requirements for all terminals, classified by terminal type. <u>These requirements may vary from terminal to terminal; any individual terminal must support the minimum requirements for its type.</u></p> <p>To ensure EMV compliance, the terminal management software should include profiles or logic validating that all mandatory functions for a terminal type are active.</p> <p>4.1.22.22 Chip Card Authentication</p> <p><u>All Chip Card Issuers must perform, and be capable of acting on the results of, validation of EMV Online Card Authentication Cryptograms for all Chip-initiated Authorization messages processed through VisaNet.</u> Online Card Authentication support may be provided by the Issuer directly, or through either:</p> <ul style="list-style-type: none"> VisaNet Third party/VisaNet Processor or Visa Scheme Processor <p>Contactless Chip • <u>Be approved by EMVCo or Visa</u></p>
--	--

See *Visa Core Rules and Visa Product and Service Rules*, VISA, available for download as a pdf file at <https://usa.visa.com/support/consumer/visa-rules.html> (last accessed Dec. 5, 2022).

72. Visa conditions the benefit of not being liable for counterfeit fraud on merchants accepting EMV transactions.

Fraud protection



When you upgrade to chip technology, you continue to be protected from counterfeit fraud losses. As of October 1, 2015, businesses that don't accept Visa chip card transactions may be responsible for any resulting counterfeit fraud. Similarly, effective April 17, 2021, Visa transactions made at ATMs and Automated Fuel Dispensers (AFDs) will be included in the Liability Shift Policy.

<https://usa.visa.com/run-your-business/small-business-tools/payment-technology/visa-chip-technology-merchants.html>

B. PAYMENT CARD LIABILITY RULES IN THE UNITED STATES

In the United States, the liability for unauthorized payment card transactions is allocated partially by statute and partially by private ordering. Federal law generally limits individual consumer liability for unauthorized transactions to \$50 for credit and debit cards, albeit with important exceptions discussed in Part IV, *infra*.⁶⁶ The liability of merchants and financial institutions is determined through private ordering under payment card network rules. The payment card networks’ rules technically bind only the card networks’ member institutions—issuer and acquirer banks. Acquirers, however, uniformly pass on their liability to their merchants by contract, sometimes adding fees.

<https://scholarship.law.georgetown.edu/facpub/613/>

73. The VISA mPOS systems “enable[] smartphones, tablets and dedicated wireless devices to accept payments without the need for a full payment terminal. Visa Ready provides guidelines for the traditional mPOS.” *See mPOS Traditional*, VISA PARTNER, <https://partner.visa.com/site/programs/visa-ready/mpos.html> (last visited Dec. 5, 2022). These EMV-compliant merchant systems communicate with Visa’s payment applications embedded on Visa Cards to secure transactions.

74. VISA requires that EMV-compliant merchant systems (i.e., the payment terminal) determine a first action analysis result as part of an “Initiate Application Processing” phase. As explained below, the card performs a “Card Action Analysis [that] generates the Application Cryptogram, generates the signature for Offline Data Authentication (conditional), and returns card application data”.

<p>4. Initiate Application Processing</p>	<p>During Initiate Application Processing, the reader signals to the card that transaction processing is beginning by sending the GET PROCESSING OPTIONS command to the card. When issuing this command, the reader supplies the card with any data elements requested by the card in the PDOL.</p> <p>Initiate Application Processing is where the card performs Card Action Analysis, generates the Application Cryptogram, generates the signature for Offline Data Authentication (conditional), and returns card application data.</p>
--	---

75. As exemplified by Kernel 3, specific to VISA, EMV terminals determine a first action analysis result based on Offline Data Authentication (ODA), risk management factor or a process restriction analysis.

Requirements – Offline Data Authentication – EMV Mode Path Processing

5.6.1.1 (Offline capable readers) [5.3]

Offline capable readers shall support fDDA as defined in Annex C.

5.6.1.2 (fDDA Verification) [5.78]

The kernel shall verify the DDA dynamic signature according to [EMV 4.3 Book 2] and the definition of fDDA in Annex C.

If fDDA fails

or the kernel is unable to perform fDDA,

then the kernel shall examine the Card Transaction Qualifiers (CTQ) to determine further processing:

- **If** 'Go online if ODA fails' indicated by card (CTQ byte 1 bit 6 is 1b) **and** Online supported by reader, **then** the kernel shall set the Online Required by Reader Indicator to 1 and continue processing the transaction.

Requirements – Processing Restrictions – EMV Mode Path Processing

5.5.1.1 (Application Expired Check) [5.74]

Implementation-Conditional: The Application Expired Check shall be implemented for readers supporting offline transactions.

If the card application returns a Transaction Certificate (TC),

and the Terminal Transaction Date (local to the reader) is greater than the Application Expiration Date (or the Application Expiration Date is not returned by the card application),

then the application has expired and the kernel shall examine the Card Transaction Qualifiers (CTQ) to determine further processing:

- **If** 'Go online if application expired' indicated by card (CTQ byte 1 bit 4 is 1b), **then** the kernel shall set the Online Required by Reader Indicator to 1.

Reader risk parameter

A reader limit or check used to perform reader risk management during the Pre-Processing phase of Entry Point, or during Kernel 3 Dynamic Reader Limits (DRL) processing.

Requirements – Online Processing – EMV Mode Path Processing

5.8.1.1 (EMV Mode Online Authorisation) [5.82]

If the Online Required by Reader Indicator is 1, **and** the Decline Required by Reader Indicator is 0, **then** the kernel shall provide an **Online Request** Outcome with the following parameters:

Online Request:

<https://www.emvco.com/wp-content/plugins/pmpro-customizations/ov-getfile.php?u=/wp-content/uploads/documents/C-3 Kernel 3 V 2 7 Final.pdf>

76. Furthermore, online processing “allows the issuer host to review and authorize or decline transactions using the issuer’s host-based risk management parameters.” *EMV Contactless Book C-3, Kernel 3 Spec v2.7*, EMVCo, p. 71, Version 2.7 (April 2018).

77. The authentication of the transaction also includes a risk management factor performed as a part of a reader limit or check.

<p>Reader risk parameter</p>	<p>A reader limit or check used to perform reader risk management during the Pre-Processing phase of Entry Point, or during Kernel 3 Dynamic Reader Limits (DRL) processing.</p>
-------------------------------------	--

Id.

78. The authentication of the transaction also includes processing restrictions such as the “Application Expired Check” shown below.

Requirements – Processing Restrictions – EMV Mode Path Processing

5.5.1.1 (Application Expired Check) [5.74]

Implementation-Conditional: The Application Expired Check shall be implemented for readers supporting offline transactions.

If the card application returns a Transaction Certificate (TC), and the Terminal Transaction Date (local to the reader) is greater than the Application Expiration Date (or the Application Expiration Date is not returned by the card application), then the application has expired and the kernel shall examine the Card Transaction Qualifiers (CTQ) to determine further processing:

- If 'Go online if application expired' indicated by card (CTQ byte 1 bit 4 is 1b), then the kernel shall set the Online Required by Reader Indicator to 1.

Id.

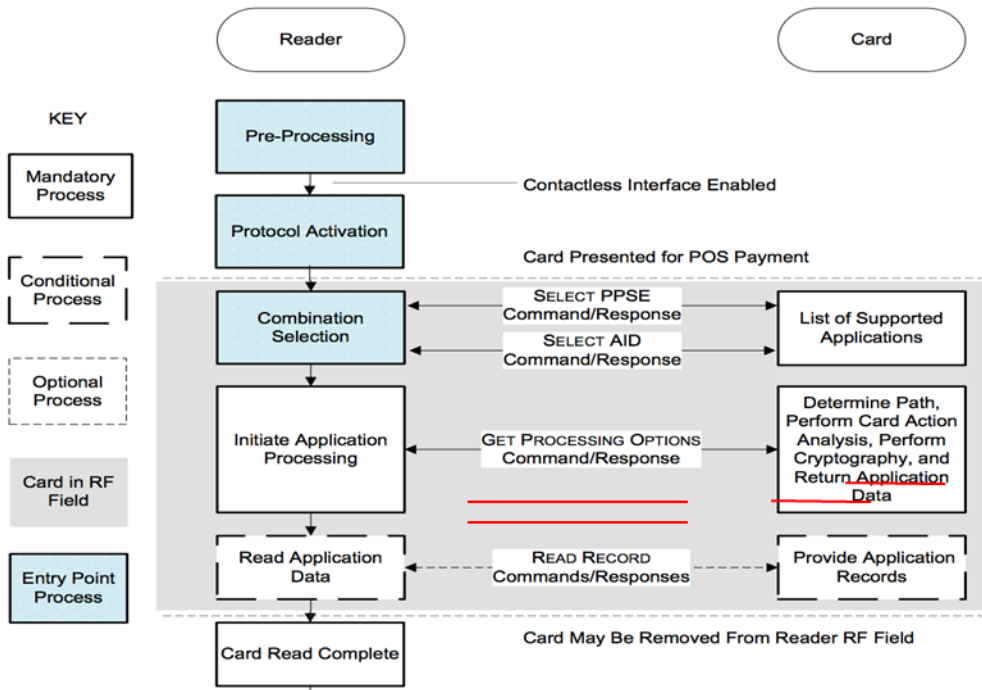
79. The terminal requests an application cryptogram from a transaction device (GENERATE AC Command), which may be for approving/denying the transaction, or for online approval. And a first card action analysis is performed by the PIC transaction device; the result is transmitted to the merchant system along with the requested cryptogram.

<p>2.4.1 Initiate Application Processing</p> <p>The status word from the response to the SELECT AID command has been evaluated by Entry Point, thus only a successful SELECT AID response including the Processing Options Data Object List (PDOL) be passed to Kernel 3.</p> <p><u>Kernel 3 processing for a transaction starts with sending a GET PROCESSING OPTIONS (GPO) command to the card. This includes the data elements requested by the card in the PDOL returned in the response to the SELECT command, which will include the Terminal Transaction Qualifiers.</u></p> <p><u>In the GPO response, the kernel is expected to receive data elements from the card that are appropriate to the conditions indicated in the Terminal Transaction Qualifiers:</u></p> <ul style="list-style-type: none"> • <u>a cryptogram with supporting/additional data</u>, and for offline approved transactions, an Application File Locator (AFL) which points to additional data. Signatures and other data that would cause the response to exceed its size limit are not included, but are instead provided in a record which is indicated in the AFL. <p>Note that the reader is expected to handle situations where the data elements – or some of them – are received during the Read Application Data function.</p> <p>If the conditions for usage of the card application have not been fulfilled, the reader must retry or end the transaction.</p>				
Name (Format; Tag; Length; Source; Path)	Requirement	Description	Retrieval	Values
<p><u>Cryptogram Information Data (CID)</u> F: b 8 T: '9F27' L: 1 S: Card</p>	Required	Indicates the type of cryptogram (TC, ARQC, or AAC) returned by the card and the actions to be performed by the reader.	GPO	<p>bits 8-7</p> <p>00 = AAC 01 = TC 10 = ARQC 11 = RFU</p> <p>bits 6-5: RFU (0,0) bits 4-1: Not used for Kernel 3</p>

Id.

80. The transaction device, at the direction of the terminal, determines a card action analysis result.

Figure 2-1: Sample Transaction Flow



<https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/C-3 Kernel 3 V 2 7 Final.pdf>

81. 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.

2.4.7 Online Processing

Online Processing is implemented for EMV mode readers supporting online transactions. The kernel indicates the need for online processing by means of the Outcome and parameters.

The data provided by the kernel for an online authorisation includes an Application Cryptogram – either an ARQC, or a TC if the card indicates that online processing is preferred if Offline Data Authentication fails.

Requirements – Online Processing – EMV Mode Path Processing

5.8.1.1 (EMV Mode Online Authorisation) [5.82]

If the Online Required by Reader Indicator is 1, and the Decline Required by Reader Indicator is 0, then the kernel shall provide an **Online Request** Outcome with the following parameters:

Online Request:

https://www.emvco.com/wp-content/plugins/pmpro-customizations/ov-getfile.php?u=/wp-content/uploads/documents/C-3_Kernel_3_V_2_7_Final.pdf

82. 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 2016080902 3257319.pdf>

83. 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.

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.			

[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/Book_A_Architecture_and_General_Rqmts_v2_6_Final_20160422011856105.pdf)

84. 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.

85. Defendants infringe one or more claims of the '750 patent via their providing directly and/or indirectly merchant systems to merchants that participate in Visa's Mobile Point of Sale (mPOS) program, including directing and controlling third parties in connection with the use

of those merchant systems. For example, Defendants direct and control the infringing activities of third parties by requiring partners, licensees, clients, merchants, issuers, acquirers, and other vendors to abide by the Visa Requirements in order to and as a condition for accessing or using a Visa system and/or service. As part of the Visa Requirements, Visa requires that all merchant systems handling Visa-based transactions, which include Visa Cards, Visa Transaction Instruments, and Visa payment networks, implement and utilize EMV standards, when effecting those transactions.

86. When a consumer's RF transaction device (i.e., any of the Visa Cards) is brought into the proximity of a merchant's terminal, the reader receives a financial transaction request comprising an ARQC cryptogram and a Token (tokenized Primary Account Number (PAN)), wherein 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.

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:

1. Use the session key derivation function specified in Annex A1.3 to derive an Application Cryptogram Session Key SK_{AC} from the ICC Application Cryptogram Master Key MK_{AC} and the 2-byte Application Transaction Counter (ATC) of the ICC.
2. Generate the 8-byte Application Cryptogram by applying the MAC algorithm specified in Annex A1.2 to the data selected and using the Application Cryptogram Session Key derived in the previous step. For AES the 8-byte Application Cryptogram is created by setting the parameter s to 8.

https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/EMV_v4.3_Book_2_Security_and_Key_Management_20120607061923900.pdf

87. The financial transaction request is transmitted to a transaction processor (e.g., the issuer) and may result in the issuer declining the transaction, due to thresholds of the LUK being

exceeded, e.g., number of transactions indicated by ATC being more than 15 transactions, as shown below.

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.

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

	<u>LUK Parameters</u>	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>

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/sections/2015-psr-conf-session4-paneldiscussion.pdf?la=en>

88. 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.

89. 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.

90. The Accused Instrumentalities of Defendants infringe at least the 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.

91. Defendants infringe the claims of the '039 patent and '509 patent by providing their computer-based systems (e.g., the Visa's payment network) for transaction processing associated with Visa Cards, including via transactions conducted using an EMV payment application issued to a user and stored in a mobile wallet. Defendants also infringe the claims of the '039 patent and '509 patent via Defendants' direction and control of third parties in connection with their activities including processing transactions associated with Visa Cards using Visa's computer-based systems.

92. In response to a command from a point-of-sale terminal, Defendants, via Visa's computer-based system, i.e., VisaNet, 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

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.

https://www.emvco.com/wp-content/uploads/2017/05/Book_A_Architecture_and_General_Rqmts_v2_6_Final_20160422011856105.pdf

93. The payment application stored in a mobile wallet, for example, provides an identification of each supported candidate payment system, including the Visa candidate payment system, which Visa provides to purchasers via Visa's licensed issuers of Visa Cards and acquirers involved in transactions associated with Visa Cards. Visa's candidate payment system is located on the VisaNet for processing a transaction related to use of Visa Cards. The Visa candidate payment system receives payment information related to the transaction to develop a payment authorization.

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.

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.

https://www.emvco.com/wp-content/uploads/2017/05/Book_A_Architecture_and_General_Rqmts_v2_6_Final_20160422011856105.pdf

94. As explained below, VISA directly performs various steps and/or exercises direction and control of third parties performing steps. For example, VISA’s payment application stored in a mobile wallet sends transaction information to the issuer, through the Visa payment network, for authorization.

<p>A.1.117 Outcome Parameter Set</p> <p>Tag: 'DF8129'</p> <p>Template: —</p> <p>Length: 8</p> <p>Format: b</p> <p>Update: K</p> <p>Description: <u>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.</u></p>	<p>Online authorization and transaction logging</p> <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>																																								
<table border="1"> <thead> <tr> <th colspan="3">Outcome Parameter Set</th> </tr> <tr> <th>Byte 1</th> <th>b8-5</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td>0001: APPROVED</td> </tr> <tr> <td></td> <td></td> <td>0010: DECLINED</td> </tr> <tr> <td></td> <td></td> <td><u>0011: ONLINE REQUEST</u></td> </tr> <tr> <td></td> <td></td> <td>0100: END APPLICATION</td> </tr> <tr> <td></td> <td></td> <td>0101: SELECT NEXT</td> </tr> <tr> <td></td> <td></td> <td>0110: TRY ANOTHER INTERFACE</td> </tr> <tr> <td></td> <td></td> <td>0111: TRY AGAIN</td> </tr> <tr> <td></td> <td></td> <td>1111: N/A</td> </tr> <tr> <td></td> <td></td> <td>Other values: RFU</td> </tr> <tr> <td>b4-1</td> <td></td> <td>Each bit RFU</td> </tr> </tbody> </table>	Outcome Parameter Set			Byte 1	b8-5	Status			0001: APPROVED			0010: DECLINED			<u>0011: ONLINE REQUEST</u>			0100: END APPLICATION			0101: SELECT NEXT			0110: TRY ANOTHER INTERFACE			0111: TRY AGAIN			1111: N/A			Other values: RFU	b4-1		Each bit RFU	<p>Table 6.2—Mandatory EMV Mode Data Objects</p> <table border="1"> <thead> <tr> <th>Data Object</th> </tr> </thead> <tbody> <tr> <td><u>Application Expiration Date</u></td> </tr> <tr> <td><u>Application PAN</u></td> </tr> <tr> <td>CDOL1</td> </tr> </tbody> </table> <p>https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/C-2_Kernel_2_V_2_7_Final.pdf</p>	Data Object	<u>Application Expiration Date</u>	<u>Application PAN</u>	CDOL1
Outcome Parameter Set																																									
Byte 1	b8-5	Status																																							
		0001: APPROVED																																							
		0010: DECLINED																																							
		<u>0011: ONLINE REQUEST</u>																																							
		0100: END APPLICATION																																							
		0101: SELECT NEXT																																							
		0110: TRY ANOTHER INTERFACE																																							
		0111: TRY AGAIN																																							
		1111: N/A																																							
		Other values: RFU																																							
b4-1		Each bit RFU																																							
Data Object																																									
<u>Application Expiration Date</u>																																									
<u>Application PAN</u>																																									
CDOL1																																									

95. As explained below, Defendants store or direct and control third parties to store a token provisioned by Visa or a third party at Visa direction and control, in place of a primary account number (“PAN”), in a mobile wallet application.

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>

96. Moreover, Visa utilizes its “Token Service Provisioning and Credential Management APIs” to “provide issuers with flexible and scalable ways to help securely issue tokens and enable their use in e-commerce, m-commerce, in-app, and contactless purchases.” *See Visa Token Service Provisioning and Credential Management*, VISA DEVELOPMENT CENTER, <https://developer.visa.com/capabilities/token-service-provisioning> (last visited Dec. 1, 2022). Visa’s “API’s allow issuers to participate in the tokenization process in order to securely provision a token on a device in partnership with Visa and wallet providers.” *Id.* Visa’s tokenization processes are “based on the EMVCo payment tokenization standard and aligns with EMV” technology. *Id.*

97. Defendants’ card application stored in a mobile wallet transmits a payment authorization request, related to the transaction, through the payment system for processing. As indicated below, the card application receives the issuer authorization through the payment system.

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).

https://www.emvco.com/wp-content/plugins/pmp-pro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/C-2_Kernel_2_V_2_7_Final.pdf

98. The Accused Instrumentalities of Defendants infringe at least the 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. The '369 patent provides systems and methods that can be used by smartcards, including contactless Visa 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. Systems 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.

99. Defendants infringe the '369 patent via their computer-based systems for transaction processing of Visa 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 and/or via direction and control of third parties, provide contactless Visa Cards and mobile wallet payment applications configured with smartcards that receive payment requests from POS

terminals. For example, in a Kernel 3 application (i.e., a Visa transaction) a card responds to an Application Cryptogram (AC) command from the terminal, as indicated below.

2.4.1 Initiate Application Processing

The status word from the response to the SELECT AID command has been evaluated by Entry Point, thus only a successful SELECT AID response including the Processing Options Data Object List (PDOL) be passed to Kernel 3.

Kernel 3 processing for a transaction starts with sending a GET PROCESSING OPTIONS (GPO) command to the card. This includes the data elements requested by the card in the PDOL returned in the response to the SELECT command, which will include the Terminal Transaction Qualifiers.

In the GPO response, the kernel is expected to receive data elements from the card that are appropriate to the conditions indicated in the Terminal Transaction Qualifiers:

- a cryptogram with supporting/additional data, and for offline approved transactions, an Application File Locator (AFL) which points to additional data. Signatures and other data that would cause the response to exceed its size limit are not included, but are instead provided in a record which is indicated in the AFL.

Note that the reader is expected to handle situations where the data elements – or some of them – are received during the Read Application Data function.

If the conditions for usage of the card application have not been fulfilled, the reader must retry or end the transaction.

EMV Contactless Book C-3, Kernel 3 Spec v2.7, EMVCo, accessible as a pdf file at https://www.emvco.com/terms-of-use/?u=/wp-content/uploads/documents/C-3_Kernel_3_V_2_7_Final.pdf (last accessed Dec. 5, 2022).

100. By their own actions and/or via direction and control of third parties, Defendants provide smartcards and also direct and control the activities of third parties in connection with smartcards. The smartcards provided in contactless Visa Cards and in connection with mobile wallets query a payment system directory in response to a command from the POS terminal. The contactless card or mobile wallet, via the smartcard, will transmit an identification of each supported payment system. The identification is usable by the POS terminal. As shown below, a POS device may support one or more applications (payment systems), where each payment system is associated with an Application Identifier (AID), e.g., Visa AIDs are routed through VisaNet—the payment system.

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>

101. The Accused Instrumentalities of Defendants infringe at least claims of the '746 patent, which provide technological solutions and improvements for reconciling remote financial data. In exemplary embodiments, the '746 patent addresses this need by using a system for managing remote financial data to establish an enhanced data structure template for reconciling information pertaining to remote financial transactions and accounts.

102. The methods and systems of the '746 patent provide innovations that enable the flexible, scalable, and cost-effective reconciliation of data in computer-based systems. As an example, Claim 1 is directed to a computer-based solution for the problem of extracting remote financial data from a data system and reconciling the financial data with master financial data using a standardized template and a customized template. Conventional systems suffer from a lack of scalability and operability across different computer systems and accounting programs. *See* '746, Abstract, 1:26-60. Advantageously, computer-based tools incorporating the standardized and customized templates of the claimed invention facilitate flexibility in accepting data in different formats, operability on a plurality of operating systems, and/or the ability to interface with a plurality of accounting software applications, while avoiding the financial burdens and impediments to standardized implementation that may occur with conventional systems. *See id.* at 1:15-2:9. This capability can be especially useful in the context of remote point-of-sale terminals that conduct financial transactions. *See id.* at 4:35-42.

103. Defendants infringe one or more claims of the ‘746 patent via their providing Visa DPS products, including financial transaction processing services and/or directing and controlling the actions of third parties in connection with these products. Visa DPS converges the processing of financial transactions in multiple formats onto a single platform for issuer transaction accounts.



 <p>Connect</p> <p>Linking issuers to the payments ecosystem and managing network compliance.</p>	 <p>Transact</p> <p>An industry leader in transaction processing, delivering performance at scale.</p>	 <p>Manage</p> <p>Making it easy to manage your card portfolio and build best-in-class customer experiences.</p>
--	---	---

<https://usa.visa.com/sites/visa-dps.html>

104. The Visa DPS system extracts remote financial data from a financial data system using standardized and/or customized templates. For example, Visa DPS uses a template (map) to parse and standardize incoming remote financial data including at least issuer card funding data and transaction data, as can be seen from the non-limiting examples of website screenshots below.



DPS-Managed Authorization

As your processor, DPS Payment Account Solutions is your host system and will perform transaction and authorization processes on your behalf. Based on the criteria you define, DPS Payment Account Solutions does all the heavy lifting, delivering services such as verifying PIN and CVV2 in support of your unique business rules.



Single Connection to Multiple Networks

The burden on financial institutions to integrate and manage card programs and network compliance is costly and resource intensive. DPS Payment Account Solutions offers a single solution to connect to the most common networks, providing you with resources and cost savings.

<https://developer.visa.com/capabilities/dps-payment-account-solutions/docs-getting-started>

Transaction Networks Basics

Transaction networks manage the traffic for all financial transaction messages. The burden on you to integrate with each network, manage network compliance, and settle with each network is costly and resource intensive. DPS Payment Account Solutions offers a single network connection to the most common networks, providing you with resources and cost savings.

<https://developer.visa.com/capabilities/dps-payment-account-solutions/transaction-networks>

Card Funding Methods

Your institution is responsible for establishing the processes and procedures required to support its funding methods, which is handled outside the DPS Payment Account Solutions.

<https://developer.visa.com/capabilities/dps-payment-account-solutions/card-funding-methods>

105. The Visa DPS system converts the remote financial data to a first format from a second format via the standardized template. For example, Visa DPS uses a first map to convert the transaction data into a first format, as can be seen from the non-limiting examples of website screenshots below.

Transaction Basics

A **transaction** is a message sent through payment networks and used to exchange a payment for goods and services, and/or perform other transaction processes. DPS Forward consolidates all the network traffic into a single connection interface for you to consume.

A typical transaction is comprised of three stages:

- **Authorization** is the process of approving or declining a transaction amount submitted by the cardholder. This is done by sending authorization and advice messages that verify a cardholder, card credentials, and availability of funds at the time of purchase.
- **Clearing** is the process of collecting final transaction data from the source, validating the transaction, calculating fees and charges, and delivering the transaction data to the issuer.

Transaction History

Because DPS Payment Account Solutions is the database of record, the transaction history is only available on Visa's system. Use the *Retrieve Transaction History Prepaid API* to retrieve transaction history.

<https://developer.visa.com/capabilities/dps-payment-account-solutions/transactions-authorizations>

106. The Visa DPS system converts the remote financial data to the first format from a third format via the customized template. For example, Visa DPS uses a second map to convert the issuer funding data into the first format, as can be seen from the non-limiting examples of website screenshots below.

Card Funding Methods

Your institution is responsible for establishing the processes and procedures required to support its funding methods, which is handled outside the DPS Payment Account Solutions.

For system reporting purposes and to help manage your card program's centralized funds pool, you must communicate loads and funding for your cards via one of these methods:

- APIs
- Administrative Portal
- CSV Bulk Upload
- Batch file

<https://developer.visa.com/capabilities/dps-payment-account-solutions/card-funding-methods>

107. The Visa DPS system reconciles the remote financial data from the standardized template and the customized template to master financial data stored in the first format. For example, on information and belief, Visa DPS stores the remote financial data in the first format in the DPS Payment Account Solutions database, where the remote financial data is used to calculate

account ledger and available balances, and to determine the net financial position of issuers and acquirers, as can be seen from the non-limiting examples of website screenshots below.

US Settlement

With each card program, your institution serves as both the Issuer and Merchant when settling funds. Your role depends on the type of transactions performed.

These types of transaction activity are part of your card program settlement:

- Card purchases
- Card transactions
- Card program fees
- Adjustments posted to cards
- Adjustments submitted for funding transactions

<https://developer.visa.com/capabilities/dps-payment-account-solutions/settlement>

- Settlement is the process of calculating, determining, reporting and transferring the net financial position of issuers and acquirers for all transactions that are cleared. The actual exchange of funds is a separate process.

DPS Payment Account Solutions is the system of record for your cardholders' available and ledger balances.

<https://developer.visa.com/capabilities/dps-payment-account-solutions/transactions-authorizations>

108. By utilizing EMV standards and performing the patented methods for transaction processing, the Accused Instrumentalities include products, services, systems, and methods for offering, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from commercial transactions via Visa Cards and associated accounts that are covered by the Asserted Patents.

109. By utilizing EMV standards and performing the patented methods for transaction processing, the Accused Instrumentalities include Defendants' products, services, systems, and methods for offering, providing, registering, facilitating, maintaining, authenticating, validating,

processing, directing, controlling and/or deriving substantial revenue from commercial transactions via Visa Cards and other associated accounts that are covered by the Asserted Patents. Furthermore, the Accused Instrumentalities include products, services, systems, and methods 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)

110. Plaintiff incorporates paragraphs 1 through 97 herein by reference.

111. 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.

112. 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.

113. 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 Texas and the United States.

114. 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, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing and controlling, and/or deriving substantial revenue from financial

transactions and payments for accounts for Visa Cards and related products, processes, and services for Defendants' licensees, acquirers, partners, merchants, customers, consumers, and clients, including Defendants' internal payment processing, authentication, authorization, validation, and fraud detection systems and methods, related to at least Defendants' card products (e.g., Visa Cards), as used in contactless chips, mobile payments, and digital wallets.

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

116. Defendant VISA INC directly infringes the '369 patent through its direct involvement in the activities of its subsidiaries, including Defendant VISA USA, including by distributing, selling, offering for sale, and servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '369 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using those Accused Instrumentalities. Specifically, VISA USA, as VISA INC's operational company in the U.S., identifies itself, including via branding, as the entity that provides Visa Cards to Defendants' licensees, acquirers, issuers, partners, merchants, customers, consumers, and clients.

117. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and

consumers to perform one or more steps of the claimed methods of the '369 patent. *Akamai Techs.*, 797 F.3d, 1023-24 (“[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’ Visa Card, Visa Transaction Instrument, and Visa payment network users may utilize such features in a point-of-sale transaction. As part of the Defendants’ agreements with such third parties to provide access to Visa payment networks (i.e., VisaNet), Defendants establish the manner of the performance of such services, e.g., that such Visa Card transactions must support EMV standards for contactless and mobile payments, as a condition of each third party’s participation in Visa Card-related transactions and in order to receive the benefit of a user of Visa’s brand or trademark, the Visa Cards, Visa Transaction Instruments, the VisaNet, and other related Visa products and 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.”). Each third party’s (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) activities in providing Visa Card services to cardholders are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

118. 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 card products, methods, and services that implement EMV standards in mobile or contactless transactions associated with Visa Cards. On information and belief, Defendants design

and develop payment applications for accounts for Visa Cards, which are used with physical Visa Cards and digital wallets. These products are issued by partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial credit, debit, or prepaid account. *See, e.g., Find Your Visa Card*, VISA, <https://usa.visa.com/pay-with-visa/find-card/> (last visited Dec. 5, 2022) (providing examples of Visa Cards).

119. For example, Defendants infringe claim 1 of the '369 patent via their Accused Instrumentalities that implement EMV standards for mobile or contactless payments, including Visa's contactless chip devices 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 incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Visa Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and use the VisaNet for the authorization and settlement of payment transactions. Defendants' mobile payments can be facilitated by Visa provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Visa Cards. Or such contactless payments can be facilitated by using contactless chips embedded on the physical Visa Cards. Defendants perform and/or direct and control the infringing systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, customers, consumers, and clients, for the authorization of and settlement of these mobile or contactless payments conducted using Visa Cards.

120. 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 of 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.

121. 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 repeatedly to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '369 patent. Defendants have known about the '369 patent, since at least on or around April 3, 2018, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC ("DHG"), informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff's patent portfolio, and offered to provide Defendants with access to a data room containing information related to the American Express patent portfolio. A representative of Visa, Timothy Bedard, replied to the email on April 4, 2018. Further, Defendants have known about the American Express patent portfolio and the '369 patent, since at least on or around August 15, 2018, when Defendants sent correspondence to Plaintiff's indirect parent Dominion Harbor Enterprises, LLC, regarding a request that "Visa access an electronic data room containing certain patents/patent applications purportedly owned by Dominion Harbor Enterprises,

LLC.” Defendants have known about the American Express patent portfolio and the ‘369 patent since at least on or around September 18, 2018, when Visa was sent, on behalf of Plaintiff, access to a data room containing claim charts for patents in the American Express patent portfolio, including the ‘369 patent. Moreover, Defendants have known about the American Express patent portfolio and the ‘369 patent since at least on or around October 3, 2022, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC (“DHG”), again informed Defendants of Plaintiff’s acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff’s patent portfolio, and again offered to provide Defendants with access to a data room containing information related to Defendants’ use of the American Express patent portfolio and the ‘369 patent. These are non-limiting examples of notice to Defendants, and Defendants received notice on further occasions.

122. 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), distributors, partners, issuers, acquirers, merchants, customers, clients, and/or consumers and payment platforms (e.g., Samsung and Google mobile wallets) that distribute, purchase, offer to sell, sale, use, and service the Accused Instrumentalities to directly infringe one or more claims of the ’369 patent by using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the ’369 patent.

123. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, licensees, issuers, acquirers, merchants, partners, customers, consumers, and clients and other 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 other mobile payment systems, including with mobile wallet applications; as provider of products, systems and services associated with Visa Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet providers, point of sale terminal providers, merchants (including online and mail order), and users; maintaining such EMV payment applications by personalizing transaction devices 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 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 Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., usa.visa.com; partner.visa.com; technologypartner.visa.com) and mobile applications for clients, customers, and consumers for registering, activating, maintaining, and using (including accessing infringing features of) the Accused Instrumentalities; and/or providing technical support and services for these products and services to licensees, issuers, acquirers, partners, customers, consumers, and clients, in the United States. *See, e.g., Visa Ready, VISA PARTNER, <https://partner.visa.com/site/programs/visa-ready.html> (last visited Dec. 5, 2022) ("The Visa Ready certification program helps technology companies build and launch payment solutions that meet Visa's global standards around security and functionality.")*.

124. Moreover, Defendants induce licensees, issuers, acquirers, partners, customers, consumers, and clients to directly infringe by requiring these parties to register with Visa and to enter license and other agreements. These agreements provide access to Visa’s “chip and mobile technology, software applets as well as Visa Ready and Approval Services testing materials.” *See Registration & Licensing, VISA*, <https://technologypartner.visa.com/Registration/> (describing the access that registrants and licensees are provided to, for example, “Visa’s Chip Specifications and Software,” “Mobile Specifications and Software,” and “Visa payWave for Mobile Developers”) (last visited Dec. 5, 2022).

125. 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.

126. 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. 8,584,938)

127. Plaintiff incorporates paragraphs 1 through 113 herein by reference.

128. 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.

129. 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. US 13/713,976.

130. 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 Texas and the United States.

131. 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, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling, and/or deriving substantial revenue from financial transactions and payments for accounts for Visa Cards and related products, processes, and services for Defendants' licensees, acquirers, partners, merchants, customers, consumers, and clients, including Defendants' internal payment processing, authentication, authorization, validation, and fraud detection systems and methods, related to at least Defendants' card products (e.g., Visa Cards), as used in contactless chips, mobile payments and digital wallets.

132. Defendants directly infringe, individually and/or jointly with at least one other entity, the '938 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '938 patent to, for example, its alter

egos, agents, intermediaries, licensees, acquirers, issuers, merchants, partners, customers, consumers, and clients. Defendants' infringement involves Defendants' own actions and/or direction and control of third parties' actions.

133. Defendant VISA INC also directly infringes the '938 patent through its direct involvement in the activities of its divisions, including Defendant VISA USA, including by distributing, selling, offering for sale, and servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '938 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using those Accused Instrumentalities. Specifically, VISA USA, as VISA INC's operational company in the U.S., identifies itself, including via branding, as the entity that provides Visa Cards to Defendants' licensees, acquirers, issuers, partners, merchants, customers, consumers, and clients.

134. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers to perform one or more steps of the claimed methods of the '938 patent. *Akamai Techs.*, 797 F.3d at 1023-24 (“[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 implementing and performing methods pursuant to at least EMV standards incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements so that Defendants' Visa Card, Visa Transaction Instrument, and Visa payment network users may utilize such features in a point-of-sale transaction. As part of the

Defendants' agreements with such third parties to provide access to Visa payment networks (i.e., VisaNet), Defendants establish the manner of the performance of such services, e.g., that such Visa Card transactions must support EMV standards for contactless and mobile payments, as a condition of each third party's participation in Visa Card-related transactions and in order to receive the benefit of a user of Visa's brand or trademark, the Visa Cards, Visa Transaction Instruments, the VisaNet, and other related Visa products and 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.”). Each third party's (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) activities in providing Visa Card services to cardholders are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

135. 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 card products, methods, and services that implement EMV standards in mobile or contactless card transactions associated with Visa Cards. On information and belief, Defendants design and develop payment applications for accounts for Visa Cards, which are used with physical Visa Cards and digital wallets. These products are issued by partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial credit, debit, or prepaid account. *See, e.g., Find Your Visa Card*, VISA, <https://usa.visa.com/pay-with-visa/find-card/> (last visited Dec. 5, 2022) (providing examples of Visa Cards).

136. For example, Defendants infringe claim 14 of the '938 patent via their Accused Instrumentalities that implement EMV standards for mobile or contactless payments, including Visa 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 incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements. Moreover, these devices and technology enable the tokenization of consumers' primary account numbers (PANs) to facilitate secure financial transactions for Visa Cards, via at least Visa's Token Service, Token Vault, Token Gateway, and VisaNet. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Visa 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 Visa provisioning mobile wallets such as Google Pay and Samsung Pay contactless payment functions for financial accounts associated with Visa Cards. Or such contactless payments can be facilitated by using contactless chips embedded on the physical Visa Cards. Defendants perform and/or direct and control the infringing systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, customers, consumers, and clients, for the authorization of and settlement of these mobile or contactless payments conducted using Visa Cards.

137. The Accused Instrumentalities implement the method of claim 14. 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.

138. 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 repeatedly to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '938 patent. Defendants have known about the '938 patent, since at least on or around April 3, 2018, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC ("DHG"), informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff's patent portfolio, and offered to provide Defendants with access to a data room containing information related to the American Express patent portfolio. A representative of Visa, Timothy Bedard, replied to the email on April 4, 2018. Further, Defendants have known about the American Express patent portfolio and the '938 patent, since at least on or around August 15, 2018, when Defendants sent correspondence to Plaintiff's indirect parent Dominion Harbor Enterprises, LLC, regarding a request that "Visa access an electronic data room containing certain patents/patent applications purportedly owned by Dominion Harbor Enterprises, LLC." Defendants have known about the American Express patent portfolio and the '938 patent since at least on or around September 18, 2018, when Visa was sent, on behalf of Plaintiff, access to a data room containing claim charts for patents in the American Express patent portfolio, including the '938 patent. Moreover, Defendants have known about the American Express patent portfolio and the '938 patent since at least on or around October 3, 2022, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC ("DHG"), again informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in licensing

discussions relating to Plaintiff's patent portfolio, and again offered to provide Defendants with access to a data room containing information related to Defendants' use of the American Express patent portfolio and the '938 patent. These are non-limiting examples of notice to Defendants, and Defendants received notice on further occasions.

139. 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), distributors, partners, issuers, acquirers, merchants, customers, clients, and/or consumers and payment platforms (e.g., Samsung and Google mobile wallets) that distribute, purchase, offer to sell, sale, use, and service the Accused Instrumentalities to directly infringe one or more claims of the '938 patent by using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '938 patent.

140. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, licensees, issuers, acquirers, merchants, partners, customers, consumers, and clients and other 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 other mobile payment systems, including with mobile wallet applications; as provider of products, systems and services associated with Visa Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet providers, point of sale terminal providers, merchants (including online and mail order), and users;

maintaining such EMV payment applications by personalizing transaction devices 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 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 Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., usa.visa.com; partner.visa.com; technologypartner.visa.com) and mobile applications for clients, customers, and consumers for registering, activating, maintaining, and using (including accessing infringing features of) the Accused Instrumentalities; and/or providing technical support and services for these products and services to licensees, issuers, acquirers, partners, customers, consumers, and clients, in the United States. *See, e.g., Visa Ready, VISA PARTNER, <https://partner.visa.com/site/programs/visa-ready.html> (last visited Dec. 5, 2022) ("The Visa Ready certification program helps technology companies build and launch payment solutions that meet Visa's global standards around security and functionality.")*.

141. Moreover, Defendants induce licensees, issuers, acquirers, partners, customers, consumers, and clients to directly infringe by requiring these parties to register with Visa and to enter license and other agreements. These agreements provide access to Visa's "chip and mobile technology, software applets as well as Visa Ready and Approval Services testing materials." *See Registration & Licensing, VISA, <https://technologypartner.visa.com/Registration/> (describing the access that registrants and licensees are provided to, for example, "Visa's Chip Specifications and*

Software,” “Mobile Specifications and Software,” and “Visa payWave for Mobile Developers”) (last visited Dec. 5, 2022).

142. 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.

143. 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. 8,814,039)

144. Plaintiff incorporates paragraphs 1 through 129 herein by reference.

145. 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.

146. 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.

147. 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 Texas and the United States.

148. 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, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling, and/or deriving substantial revenue from financial transactions and payments for accounts for Visa Cards and related products, processes, and services for Defendants' licensees, acquirers, partners, merchants, customers, consumers, and clients, including Defendants' internal payment processing, authentication, authorization, validation, and fraud detection systems and methods, related to at least Defendants' card products (e.g., Visa Cards), as used in contactless chips, mobile payments, and digital wallets.

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

150. Defendant VISA INC directly infringes the '039 patent through its direct involvement in the activities of its subsidiaries, including Defendant VISA USA, including by distributing, selling, offering for sale, and servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '039 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using those Accused Instrumentalities. Specifically, VISA USA, as VISA INC's operational company in the U.S., identifies itself, including via branding, as the entity that provides Visa Transaction Instruments, including without limitation Visa Cards, to Defendants' licensees, acquirers, issuers, partners, merchants, customers, consumers, and clients.

151. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers to perform one or more steps of the claimed methods of the '039 patent. *Akamai Techs.*, 797 F.3d at 1023-24 (“[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 implementing and performing methods pursuant to at least EMV standards incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements so that Defendants' Visa Card, Visa Transaction Instrument, and Visa payment network users may utilize such features in a point-of-sale transaction. As part of the Defendants' agreements with such third parties to provide access to Visa payment networks (i.e., VisaNet), Defendants establish the manner of the performance of such services, e.g., that such Visa

Card transactions must support EMV standards for contactless and mobile payments, as a condition of each third party's participation in Visa Card-related transactions and in order to receive the benefit of a user of Visa's brand or trademark, the Visa Cards, Visa Transaction Instruments, the VisaNet, and other related Visa products and 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.”). Each third party's (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) activities in providing Visa Card services to cardholders are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

152. 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 card products, methods, and services that implement EMV standards in mobile or contactless card transactions associated with Visa Cards. On information and belief, Defendants design and develop payment applications for accounts for Visa Cards, which are used with physical Visa Cards and digital wallets. These products are issued by partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial credit, debit, or prepaid account. *See, e.g., Find Your Visa Card, VISA*, <https://usa.visa.com/pay-with-visa/find-card/> (last visited Dec. 5, 2022) (providing examples of Visa Cards).

153. For example, Defendants infringe claim 1 of the '039 patent via their Accused Instrumentalities that implement EMV standards for mobile or contactless payments, including Visa's contactless chip devices 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 incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Visa Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and use the VisaNet for the authorization and settlement of payment transactions. Defendants' mobile payments can be facilitated by Visa provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Visa Cards. Or such contactless payments can be facilitated by using contactless chips embedded on the physical Visa Cards. Defendants perform and/or direct and control the infringing systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, customers, consumers, and clients, for the authorization of and settlement of these mobile or contactless payments conducted using Visa Cards.

154. 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 including 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.

155. 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 repeatedly to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '039 patent. Defendants have known about the '039 patent, since at least on or around April 3, 2018, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC ("DHG"), informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff's patent portfolio, and offered to provide Defendants with access to a data room containing information related to the American Express patent portfolio. A representative of Visa, Timothy Bedard, replied to the email on April 4, 2018. Further, Defendants have known about the American Express patent portfolio and the '039 patent, since at least on or around August 15, 2018, when Defendants sent correspondence to Plaintiff's indirect parent Dominion Harbor Enterprises, LLC, regarding a request that "Visa access an electronic data room containing certain patents/patent applications purportedly owned by Dominion Harbor Enterprises, LLC." Defendants have known about the American Express patent portfolio and the '039 patent since at least on or around September 18, 2018, when Visa was sent, on behalf of Plaintiff, access to a data room containing claim charts for patents in the American Express patent portfolio, including the '039 patent. Moreover, Defendants have known about the American Express patent portfolio and the '039 patent since at least on or around October 3, 2022, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC ("DHG"), again informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in licensing

discussions relating to Plaintiff's patent portfolio, and again offered to provide Defendants with access to a data room containing information related to Defendants' use of the American Express patent portfolio and the '039 patent. These are non-limiting examples of notice to Defendants, and Defendants received notice on further occasions.

156. 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), distributors, partners, issuers, acquirers, merchants, customers, clients, and/or consumers and payment platforms (e.g., Samsung and Google mobile wallets) that distribute, purchase, offer to sell, sale, use, and service the Accused Instrumentalities to directly infringe one or more claims of the '039 patent by using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '039 patent.

157. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, licensees, issuers, acquirers, merchants, partners, customers, consumers, and clients and other 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 other mobile payment systems, including with mobile wallet applications; as provider of products, systems and services associated with Visa Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet providers, point of sale terminal providers, merchants (including online and mail order), and users;

maintaining such EMV payment applications by personalizing transaction devices 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 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 Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., usa.visa.com; partner.visa.com; technologypartner.visa.com) and mobile applications for clients, customers, and consumers for registering, activating, maintaining, and using (including accessing infringing features of) the Accused Instrumentalities; and/or providing technical support and services for these products and services to licensees, issuers, acquirers, partners, customers, consumers, and clients, in the United States. *See, e.g., Visa Ready, VISA PARTNER, <https://partner.visa.com/site/programs/visa-ready.html> (last visited Dec. 5, 2022) ("The Visa Ready certification program helps technology companies build and launch payment solutions that meet Visa's global standards around security and functionality.")*.

158. Moreover, Defendants induce licensees, issuers, acquirers, partners, customers, consumers, and clients to directly infringe by requiring these parties to register with Visa and to enter license and other agreements. These agreements provide access to Visa's "chip and mobile technology, software applets as well as Visa Ready and Approval Services testing materials." *See Registration & Licensing, VISA, <https://technologypartner.visa.com/Registration/> (describing the access that registrants and licensees are provided to, for example, "Visa's Chip Specifications and*

Software,” “Mobile Specifications and Software,” and “Visa payWave for Mobile Developers”) (last visited Dec. 5, 2022).

159. 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.

160. 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. 8,794,509)

161. Plaintiff incorporates paragraphs 1 through 145 herein by reference.

162. 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.

163. 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.

164. 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 Texas and the United States.

165. 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, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling, and/or deriving substantial revenue from financial transactions and payments for accounts for Visa Cards and related products, processes, and services for Defendants' licensees, acquirers, partners, merchants, customers, consumers, and clients, including Defendants' internal payment processing, authentication, authorization, validation, and fraud detection systems and methods, related to at least Defendants' card products (e.g., Visa Cards), as used in contactless chips, mobile payments, and digital wallets.

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

167. Defendant VISA INC directly infringes the '509 patent through its direct involvement in the activities of its subsidiaries, including Defendant VISA USA, including by

distributing, selling, offering for sale, and servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '509 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using those Accused Instrumentalities. Specifically, VISA USA, as VISA INC's operational company in the U.S., identifies itself, including via branding, as the entity that provides Visa Cards to Defendants' licensees, acquirers, issuers, partners, merchants, customers, consumers, and clients.

168. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers to perform one or more steps of the claimed methods of the '509 patent. *Akamai Techs.*, 797 F.3d at 1023-24 (“[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 implementing and performing methods pursuant to at least EMV standards incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements so that Defendants' Visa Card, Visa Transaction Instrument, and Visa payment network users may utilize such features in a point-of-sale transaction. As part of the Defendants' agreements with such third parties to provide access to Visa payment networks (i.e., VisaNet), Defendants establish the manner of the performance of such services, e.g., that such Visa Card transactions must support EMV standards for contactless and mobile payments, as a condition of each third party's participation in Visa Card-related transactions and in order to receive the benefit of a user of Visa's brand or trademark, the Visa Cards, Visa Transaction Instruments, the

VisaNet, and other related Visa products and 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.”). Each third party’s (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) activities in providing Visa Card services to cardholders are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

169. 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 card products, methods, and services that implement EMV standards in mobile or contactless card transactions associated with Visa Cards. On information and belief, Defendants design and develop payment applications for accounts for Visa Cards, which are used with physical Visa Cards and digital wallets. These products are issued by partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial credit, debit, or prepaid account. *See, e.g., Find Your Visa Card*, VISA, <https://usa.visa.com/pay-with-visa/find-card/> (last visited Dec. 5, 2022) (providing examples of Visa Cards).

170. For example, Defendants infringe claim 1 of the ‘509 patent via their Accused Instrumentalities that implement EMV standards for mobile or contactless payments, including Visa’s contactless chip devices 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 incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS),

and the Visa Requirements. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Visa Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and use the VisaNet for the authorization and settlement of payment transactions. Defendants' mobile payments can be facilitated by Visa provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Visa Cards. Or such contactless payments can be facilitated by using contactless chips embedded on the physical Visa Cards. Defendants perform and/or direct and control the infringing systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, customers, consumers, and clients, for the authorization of and settlement of these mobile or contactless payments conducted using Visa Cards.

171. 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.

172. 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 repeatedly to provide Defendants with notice of Plaintiff’s American Express patent portfolio that includes the ‘509 patent. Defendants have known about the American Express patent portfolio, which includes the ‘509 patent, since at least on or around April 3, 2018, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC (“DHG”), informed Defendants of Plaintiff’s acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff’s patent portfolio, and offered to provide Defendants with access to a data room containing information related to the American Express patent portfolio. A representative of Visa, Timothy Bedard, replied to the email on April 4, 2018. Defendants have known about the American Express patent portfolio, which includes the ‘509 patent, since at least on or around August 15, 2018, when Defendants sent correspondence to Plaintiff’s indirect parent Dominion Harbor Enterprises, LLC, regarding a request that “Visa access an electronic data room containing certain patents/patent applications purportedly owned by Dominion Harbor Enterprises, LLC.” Defendants have known about the American Express patent portfolio, which includes the ‘509 patent, since at least on or around September 18, 2018, when Visa was sent, on behalf of Plaintiff, access to a data room containing claim charts for patents in the American Express patent portfolio. Moreover, Defendants have known about the American Express patent portfolio, which includes the ‘509 patent, since at least on or around October 3, 2022, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC (“DHG”), again informed Defendants of Plaintiff’s acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff’s patent

portfolio, and again offered to provide Defendants with access to a data room containing information related to Defendants' use of the American Express patent portfolio, which portfolio includes the '509 patent. These are non-limiting examples of notice to Defendants, and Defendants received notice on further occasions.

173. 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), distributors, partners, issuers, acquirers, merchants, customers, clients, and/or consumers and payment platforms (e.g., Samsung and Google mobile wallets) that distribute, purchase, offer to sell, sale, use, and service the Accused Instrumentalities to directly infringe one or more claims of the '509 patent by using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '509 patent.

174. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, licensees, issuers, acquirers, merchants, partners, customers, consumers, and clients and other 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 other mobile payment systems, including with mobile wallet applications; as provider of products, systems and services associated with Visa Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet providers, point of sale terminal providers, merchants (including online and mail order), and users;

maintaining such EMV payment applications by personalizing transaction devices 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 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 Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., usa.visa.com; partner.visa.com; technologypartner.visa.com) and mobile applications for clients, customers, and consumers for registering, activating, maintaining, and using (including accessing infringing features of) the Accused Instrumentalities; and/or providing technical support and services for these products and services to licensees, issuers, acquirers, partners, customers, consumers, and clients, in the United States. *See, e.g., Visa Ready, VISA PARTNER, <https://partner.visa.com/site/programs/visa-ready.html> (last visited Dec. 5, 2022) ("The Visa Ready certification program helps technology companies build and launch payment solutions that meet Visa's global standards around security and functionality.")*.

175. Moreover, Defendants induce licensees, issuers, acquirers, partners, customers, consumers, and clients to directly infringe by requiring these parties to register with Visa and to enter license and other agreements. These agreements provide access to Visa's "chip and mobile technology, software applets as well as Visa Ready and Approval Services testing materials." *See Registration & Licensing, VISA, <https://technologypartner.visa.com/Registration/> (describing the access that registrants and licensees are provided to, for example, "Visa's Chip Specifications and*

Software,” “Mobile Specifications and Software,” and “Visa payWave for Mobile Developers”) (last visited Dec. 5, 2022).

176. 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.

177. 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. 7,953,671)

178. Plaintiff incorporates paragraphs 1 through 161 herein by reference.

179. 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.

180. 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.

181. 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 Texas and the United States.

182. 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, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling, and/or deriving substantial revenue from financial transactions and payments for accounts for Visa Cards and related products, processes, and services for Defendants' licensees, acquirers, partners, merchants, customers, consumers, and clients, including Defendants' internal payment processing, authentication, authorization, validation, and fraud detection systems and methods, related to at least Defendants' card products (e.g., Visa Cards), as used in contactless chips, mobile payments, and digital wallets.

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

184. Defendant VISA INC directly infringes the '671 patent through its direct involvement in the activities of its subsidiaries, including Defendant VISA USA, including by

distributing, selling, offering for sale, and servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '671 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using those Accused Instrumentalities. Specifically, VISA USA, as VISA INC's operational company in the U.S., identifies itself, including via branding, as the entity that provides Visa Cards to Defendants' licensees, acquirers, issuers, partners, merchants, customers, consumers, and clients.

185. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers to perform one or more steps of the claimed methods of the '671 patent. *Akamai Techs.*, 797 F.3d at 1023-24 (“[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 implementing and performing methods pursuant to at least EMV standards incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements so that Defendants' Visa Card, Visa Transaction Instrument, and Visa payment network users may utilize such features in a point-of-sale transaction. As part of the Defendants' agreements with such third parties to provide access to Visa payment networks (i.e., VisaNet), Defendants establish the manner of the performance of such services, e.g., that such Visa Card transactions must support EMV standards for contactless and mobile payments, as a condition of each third party's participation in Visa Card-related transactions and in order to receive the benefit of a user of Visa's brand or trademark, the Visa Cards, Visa Transaction Instruments, the

VisaNet, and other related Visa products and 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.”). Each third party’s (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) activities in providing Visa Card services to cardholders are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

186. 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 card products, methods, and services that implement EMV standards in mobile or contactless card transactions associated with Visa Cards. On information and belief, Defendants design and develop payment applications for accounts for Visa Cards, which are used with physical Visa Cards and digital wallets. These products are issued by partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial credit, debit, or prepaid account. *See, e.g., Find Your Visa Card, VISA, <https://usa.visa.com/pay-with-visa/find-card/>* (last visited Dec. 5, 2022) (providing examples of Visa Cards).

187. For example, Defendants infringe claim 1 of the ‘671 patent via their Accused Instrumentalities that implement EMV standards for mobile or contactless payments, including Visa’s contactless chip devices 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 incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS),

and the Visa Requirements. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Visa Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and use the VisaNet for the authorization and settlement of payment transactions. Defendants' mobile payments can be facilitated by Visa provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Visa Cards. Or such contactless payments can be facilitated by using contactless chips embedded on the physical Visa Cards. Defendants perform and/or direct and control the infringing systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, customers, consumers, and clients, for the authorization of and settlement of these mobile or contactless payments conducted using Visa Cards.

188. 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.

189. Defendants have been contacted repeatedly to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '671 patent. Defendants have known about the '671 patent, since at least on or around April 3, 2018, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC ("DHG"), informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff's patent portfolio, and offered to provide Defendants with access to a data room containing information related to the American Express patent portfolio. A representative of Visa, Timothy Bedard, replied to the email on April 4, 2018. Further, Defendants have known about the American Express patent portfolio and the '671 patent, since at least on or around August 15, 2018, when Defendants sent correspondence to Plaintiff's indirect parent Dominion Harbor Enterprises, LLC, regarding a request that "Visa access an electronic data room containing certain patents/patent applications purportedly owned by Dominion Harbor Enterprises, LLC." Defendants have known about the American Express patent portfolio and the '671 patent since at least on or around September 18, 2018, when Visa was sent, on behalf of Plaintiff, access to a data room containing claim charts for patents in the American Express patent portfolio, including the '671 patent. These are non-limiting examples of notice to Defendants, and Defendants received notice on further occasions.

190. 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), distributors, partners, issuers, acquirers, merchants, customers, clients, and/or consumers and payment platforms (e.g., Samsung and Google mobile wallets) that distribute, purchase, offer

to sell, sale, use, and service the Accused Instrumentalities to directly infringe one or more claims of the '671 patent by using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '671 patent.

191. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, licensees, issuers, acquirers, merchants, partners, customers, consumers, and clients and other 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 other mobile payment systems, including with mobile wallet applications; as provider of products, systems and services associated with Visa Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet providers, point of sale terminal providers, merchants (including online and mail order), and users; maintaining such EMV payment applications by personalizing transaction devices 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 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 Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., usa.visa.com; partner.visa.com;

technologypartner.visa.com) and mobile applications for clients, customers, and consumers for registering, activating, maintaining, and using (including accessing infringing features of) the Accused Instrumentalities; and/or providing technical support and services for these products and services to licensees, issuers, acquirers, partners, customers, consumers, and clients, in the United States. *See, e.g., Visa Ready, VISA PARTNER, <https://partner.visa.com/site/programs/visa-ready.html>* (last visited Dec. 5, 2022) (“The Visa Ready certification program helps technology companies build and launch payment solutions that meet Visa's global standards around security and functionality.”).

192. Moreover, Defendants induce licensees, issuers, acquirers, partners, customers, consumers, and clients to directly infringe by requiring these parties to register with Visa and to enter license and other agreements. These agreements provide access to Visa’s “chip and mobile technology, software applets as well as Visa Ready and Approval Services testing materials.” *See Registration & Licensing, VISA, <https://technologypartner.visa.com/Registration/>* (describing the access that registrants and licensees are provided to, for example, “Visa’s Chip Specifications and Software,” “Mobile Specifications and Software,” and “Visa payWave for Mobile Developers”) (last visited Dec. 5, 2022).

193. 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.

194. 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. 9,195,985)

195. Plaintiff incorporates paragraphs 1 through 177 herein by reference.

196. 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.

197. 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.

198. 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 Texas and the United States.

199. 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, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling, and/or deriving substantial revenue from financial

transactions and payments for accounts for Visa Cards and related products, processes, and services for Defendants' licensees, acquirers, partners, merchants, customers, consumers, and clients, including Defendants' internal payment processing, authentication, authorization, validation, and fraud detection systems and methods, related to at least Defendants' card products (e.g., Visa Cards), as used in contactless chips, mobile payments and digital wallets.

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

201. Defendant VISA INC also directly infringes the '985 patent through its direct involvement in the activities of its divisions, including Defendant VISA USA, including by distributing, selling, offering for sale, and servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '985 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using those Accused Instrumentalities. Specifically, VISA USA, as VISA INC's operational company in the U.S., identifies itself, including via branding, as the entity that provides Visa Cards to Defendants' licensees, acquirers, issuers, partners, merchants, customers, consumers, and clients.

202. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and

consumers to perform one or more steps of the claimed methods of the '985 patent. *Akamai Techs.*, 797 F.3d at 1023-24 (“[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 implementing and performing methods pursuant to at least EMV standards incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements so that Defendants’ Visa Card, Visa Transaction Instrument, and Visa payment network users may utilize such features in a point-of-sale transaction. As part of the Defendants’ agreements with such third parties to provide access to Visa payment networks (i.e., VisaNet), Defendants establish the manner of the performance of such services, e.g., that such Visa Card transactions must support EMV standards for contactless and mobile payments, as a condition of each third party’s participation in Visa Card-related transactions and in order to receive the benefit of a user of Visa’s brand or trademark, the Visa Cards, Visa Transaction Instruments, the VisaNet, and other related Visa products and 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.”). Each third party’s (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) activities in providing Visa Card services to cardholders are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

203. 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 card products, methods, and services that implement EMV standards in mobile or contactless card transactions associated with Visa Cards. On information and belief, Defendants design and develop payment applications for accounts for Visa Cards, which are used with physical Visa Cards and digital wallets. These products are issued by partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial credit, debit, or prepaid account. *See, e.g., Find Your Visa Card*, VISA, <https://usa.visa.com/pay-with-visa/find-card/> (last visited Dec. 5, 2022) (providing examples of Visa Cards).

204. For example, Defendants infringe claim 1 of the '985 patent via their Accused Instrumentalities that implement EMV standards for mobile or contactless payments, including Visa's contactless chip devices 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 incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements. Moreover, these devices and technology enable the tokenization of consumers' primary account numbers (PANs) to facilitate secure financial transactions for Visa credit, debit, and prepaid card, via at least Visa's Token Service, Token Vault, Token Gateway, and VisaNet. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Visa 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 Visa provisioning mobile wallets such as Google Pay and Samsung Pay contactless payment functions for financial accounts associated with Visa Cards. Or such contactless payments can be facilitated by using contactless chips embedded on the physical Visa Cards. Defendants perform and/or direct and control the infringing systems and methods, including via their alter egos,

agents, intermediaries, licensees, issuers, acquirers, partners, customers, consumers, and clients, for the authorization of and settlement of these mobile or contactless payments conducted using Visa Cards.

205. 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 practice the following method 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.

206. 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 repeatedly to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '985 patent. Defendants have known about the '985 patent, since at least on or around April 3, 2018, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC ("DHG"), informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff's patent portfolio, and offered to provide Defendants with

access to a data room containing information related to the American Express patent portfolio. A representative of Visa, Timothy Bedard, replied to the email on April 4, 2018. Further, Defendants have known about the American Express patent portfolio and the ‘985 patent, since at least on or around August 15, 2018, when Defendants sent correspondence to Plaintiff’s indirect parent Dominion Harbor Enterprises, LLC, regarding a request that “Visa access an electronic data room containing certain patents/patent applications purportedly owned by Dominion Harbor Enterprises, LLC.” Defendants have known about the American Express patent portfolio and the ‘985 patent since at least on or around September 18, 2018, when Visa was sent, on behalf of Plaintiff, access to a data room containing claim charts for patents in the American Express patent portfolio, including the ‘985 patent. Moreover, Defendants have known about the American Express patent portfolio and the ‘985 patent since at least on or around October 3, 2022, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC (“DHG”), again informed Defendants of Plaintiff’s acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff’s patent portfolio, and again offered to provide Defendants with access to a data room containing information related to Defendants’ use of the American Express patent portfolio and the ‘985 patent. These are non-limiting examples of notice to Defendants, and Defendants received notice on further occasions.

207. 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), distributors, partners, issuers, acquirers, merchants, customers, clients, and/or consumers and payment platforms (e.g., Samsung and Google mobile wallets) that distribute, purchase, offer to sell, sale, use, and service the Accused Instrumentalities to directly infringe one or more claims of the ‘985 patent by using, offering for sale, selling, and/or servicing the Accused Instrumentalities.

Since at least the notice provided on the above-mentioned date, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '985 patent.

208. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, licensees, issuers, acquirers, merchants, partners, customers, consumers, and clients and other 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 other mobile payment systems, including with mobile wallet applications; as provider of products, systems and services associated with Visa Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet providers, point of sale terminal providers, merchants (including online and mail order), and users; maintaining such EMV payment applications by personalizing transaction devices 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 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 Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., usa.visa.com; partner.visa.com; technologypartner.visa.com) and mobile applications for clients, customers, and consumers for registering, activating, maintaining, and using (including accessing infringing features of) the

Accused Instrumentalities; and/or providing technical support and services for these products and services to licensees, issuers, acquirers, partners, customers, consumers, and clients, in the United States. *See, e.g., Visa Ready, VISA PARTNER, <https://partner.visa.com/site/programs/visa-ready.html>* (last visited Dec. 5, 2022) (“The Visa Ready certification program helps technology companies build and launch payment solutions that meet Visa's global standards around security and functionality.”).

209. Moreover, Defendants induce licensees, issuers, acquirers, partners, customers, consumers, and clients to directly infringe by requiring these parties to register with Visa and to enter license and other agreements. These agreements provide access to Visa’s “chip and mobile technology, software applets as well as Visa Ready and Approval Services testing materials.” *See Registration & Licensing, VISA, <https://technologypartner.visa.com/Registration/>* (describing the access that registrants and licensees are provided to, for example, “Visa’s Chip Specifications and Software,” “Mobile Specifications and Software,” and “Visa payWave for Mobile Developers”) (last visited Dec. 5, 2022).

210. 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.

211. 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. 7,587,756)

212. Plaintiff incorporates paragraphs 1 through 194 herein by reference.

213. 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.

214. 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.

215. 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 Texas and the United States.

216. 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, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling, and/or deriving substantial revenue from financial transactions and payments for accounts for Visa Cards and related products, processes, and services for Defendants' licensees, acquirers, partners, merchants, customers, consumers, and clients,

including Defendants' internal payment processing, authentication, authorization, validation, and fraud detection systems and methods, related to at least Defendants' card products (e.g., Visa Cards), as used in contactless chips, mobile payments, and digital wallets.

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

218. Defendant VISA INC directly infringes the '756 patent through its direct involvement in the activities of its subsidiaries, including Defendant VISA USA, including by distributing, selling, offering for sale, and servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '756 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using those Accused Instrumentalities. Specifically, VISA USA, as VISA INC's operational company in the U.S., identifies itself, including via branding, as the entity that provides Visa Cards to Defendants' licensees, acquirers, issuers, partners, merchants, customers, consumers, and clients.

219. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers to perform one or more steps of the claimed methods of the '756 patent. *Akamai Techs.*, 797 F.3d at 1023-24 (“[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 implementing and performing methods pursuant to at least EMV standards incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements so that Defendants’ Visa Card, Visa Transaction Instrument, and Visa payment network users may utilize such features in a point-of-sale transaction. As part of the Defendants’ agreements with such third parties to provide access to Visa payment networks (i.e., VisaNet), Defendants establish the manner of the performance of such services, e.g., that such Visa Card transactions must support EMV standards for contactless and mobile payments, as a condition of each third party’s participation in Visa Card-related transactions and in order to receive the benefit of a user of Visa’s brand or trademark, the Visa Cards, Visa Transaction Instruments, the VisaNet, and other related Visa products and 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.”). Each third party’s (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) activities in providing Visa Card services to cardholders are thus attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

220. 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 card products, methods, and services that implement EMV standards in mobile or contactless card transactions associated with Visa Cards. On information and belief, Defendants

design and develop payment applications for accounts for Visa Cards, which are used with physical Visa Cards and digital wallets. These products are issued by partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial credit, debit, or prepaid account. *See, e.g., Find Your Visa Card*, VISA, <https://usa.visa.com/pay-with-visa/find-card/> (last visited Dec. 5, 2022) (providing examples of Visa Cards).

221. For example, Defendants infringe claim 1 of the ‘756 patent via their Accused Instrumentalities that implement EMV standards for mobile or contactless payments, including Visa’s contactless chip devices 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 incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Visa Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and use the VisaNet for the authorization and settlement of payment transactions. Defendants’ mobile payments can be facilitated by Visa provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Visa Cards. Or such contactless payments can be facilitated by using contactless chips embedded on the physical Visa Cards. Defendants perform and/or direct and control the infringing systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, customers, consumers, and clients, for the authorization of and settlement of these mobile or contactless payments conducted using Visa Cards.

222. 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 includes 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; 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.

223. 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 repeatedly to provide

Defendants with notice of Plaintiff's American Express patent portfolio and the '756 patent. Defendants have known about the '756 patent, since at least on or around April 3, 2018, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC ("DHG"), informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff's patent portfolio, and offered to provide Defendants with access to a data room containing information related to the American Express patent portfolio. A representative of Visa, Timothy Bedard, replied to the email on April 4, 2018. Further, Defendants have known about the American Express patent portfolio and the '756 patent, since at least on or around August 15, 2018, when Defendants sent correspondence to Plaintiff's indirect parent Dominion Harbor Enterprises, LLC, regarding a request that "Visa access an electronic data room containing certain patents/patent applications purportedly owned by Dominion Harbor Enterprises, LLC." Defendants have known about the American Express patent portfolio and the '756 patent since at least on or around September 18, 2018, when Visa was sent, on behalf of Plaintiff, access to a data room containing claim charts for patents in the American Express patent portfolio, including the '756 patent. Moreover, Defendants have known about the American Express patent portfolio and the '756 patent since at least on or around October 3, 2022, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC ("DHG"), again informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff's patent portfolio, and again offered to provide Defendants with access to a data room containing information related to Defendants' use of the American Express patent portfolio and the '756 patent. These are non-limiting examples of notice to Defendants, and Defendants received notice on further occasions.

224. 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), distributors, partners, issuers, acquirers, merchants, customers, clients, and/or consumers and payment platforms (e.g., Samsung and Google mobile wallets) that distribute, purchase, offer to sell, sale, use, and service the Accused Instrumentalities to directly infringe one or more claims of the '756 patent by using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '756 patent.

225. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, licensees, issuers, acquirers, merchants, partners, customers, consumers, and clients and other 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 other mobile payment systems, including with mobile wallet applications; as provider of products, systems and services associated with Visa Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet providers, point of sale terminal providers, merchants (including online and mail order), and users; maintaining such EMV payment applications by personalizing transaction devices 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 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 Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., usa.visa.com; partner.visa.com; technologypartner.visa.com) and mobile applications for clients, customers, and consumers for registering, activating, maintaining, and using (including accessing infringing features of) the Accused Instrumentalities; and/or providing technical support and services for these products and services to licensees, issuers, acquirers, partners, customers, consumers, and clients, in the United States. *See, e.g., Visa Ready, VISA PARTNER, https://partner.visa.com/site/programs/visa-ready.html* (last visited Dec. 5, 2022) (“The Visa Ready certification program helps technology companies build and launch payment solutions that meet Visa's global standards around security and functionality.”).

226. Moreover, Defendants induce licensees, issuers, acquirers, partners, customers, consumers, and clients to directly infringe by requiring these parties to register with Visa and to enter license and other agreements. These agreements provide access to Visa's “chip and mobile technology, software applets as well as Visa Ready and Approval Services testing materials.” *See Registration & Licensing, VISA, https://technologypartner.visa.com/Registration/* (describing the access that registrants and licensees are provided to, for example, “Visa's Chip Specifications and Software,” “Mobile Specifications and Software,” and “Visa payWave for Mobile Developers”) (last visited Dec. 5, 2022).

227. 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.

228. 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. 7,668,750)

229. Plaintiff incorporates paragraphs 1 through 209 herein by reference.

230. 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.

231. 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.

232. 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 Texas and the United States.

233. 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, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling, and/or deriving substantial revenue from financial transactions and payments for accounts for Visa Cards and related products, processes, and services for Defendants' licensees, acquirers, partners, merchants, customers, consumers, and clients, including Defendants' internal payment processing, authentication, authorization, validation, and fraud detection systems and methods, related to at least Defendants' card products (e.g., Visa Cards), as used in contactless chips, mobile payments, and digital wallets.

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

235. Defendant VISA INC directly infringes the '750 patent through its direct involvement in the activities of its subsidiaries, including Defendant VISA USA, including by distributing, selling, offering for sale, and servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '750 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using those Accused Instrumentalities. Specifically, VISA USA, as VISA INC's operational company in the U.S., identifies itself, including via branding, as the entity that provides Visa Cards to Defendants' licensees, acquirers, issuers, partners, merchants, customers, consumers, and clients.

236. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers to perform one or more steps of the claimed methods of the '750 patent. *Akamai Techs.*, 797 F.3d at 1023-24 (“[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 implementing and performing methods pursuant to at least EMV standards incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements so that Defendants’ Visa Card, Visa Transaction Instrument, and Visa payment network users may utilize such features in a point-of-sale transaction. As part of the Defendants’ agreements with such third parties to provide access to Visa payment networks (i.e., VisaNet), Defendants establish the manner of the performance of such services, e.g., that such Visa Card transactions must support EMV standards for contactless and mobile payments, as a condition of each third party’s participation in Visa Card-related transactions and in order to receive the benefit of a user of Visa’s brand or trademark, the Visa Cards, Visa Transaction Instruments, the VisaNet, and other related Visa products and 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.”). Each third party’s (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) activities in providing Visa Card services to cardholders are thus

attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

237. 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 card products, methods, and services that implement EMV standards in mobile or contactless card transactions associated with Visa Cards. On information and belief, Defendants design and develop payment applications for accounts for Visa Cards, which are used with physical Visa Cards and digital wallets. These products are issued by partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial credit, debit, or prepaid account. *See, e.g., Find Your Visa Card*, VISA, <https://usa.visa.com/pay-with-visa/find-card/> (last visited Dec. 5, 2022) (providing examples of Visa Cards).

238. For example, Defendants infringe claim 1 of the ‘750 patent via their Accused Instrumentalities that implement EMV standards for mobile or contactless payments, including Visa’s contactless chip devices 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 incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Visa Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and use the VisaNet for the authorization and settlement of payment transactions. Defendants’ mobile payments can be facilitated by Visa provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Visa Cards. Or such

contactless payments can be facilitated by using contactless chips embedded on the physical Visa Cards. Defendants perform and/or direct and control the infringing systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, customers, consumers, and clients, for the authorization of and settlement of these mobile or contactless payments conducted using Visa Cards.

239. 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.

240. 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 repeatedly to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '750 patent. Defendants have known about the '750 patent, since at least on or around April 3, 2018, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC ("DHG"), informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff's patent portfolio, and offered to provide Defendants with

access to a data room containing information related to the American Express patent portfolio. A representative of Visa, Timothy Bedard, replied to the email on April 4, 2018. Further, Defendants have known about the American Express patent portfolio and the ‘750 patent, since at least on or around August 15, 2018, when Defendants sent correspondence to Plaintiff’s indirect parent Dominion Harbor Enterprises, LLC, regarding a request that “Visa access an electronic data room containing certain patents/patent applications purportedly owned by Dominion Harbor Enterprises, LLC.” Defendants have known about the American Express patent portfolio and the ‘750 patent since at least on or around September 18, 2018, when Visa was sent, on behalf of Plaintiff, access to a data room containing claim charts for patents in the American Express patent portfolio, including the ‘750 patent. Moreover, Defendants have known about the American Express patent portfolio and the ‘750 patent since at least on or around October 3, 2022, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC (“DHG”), again informed Defendants of Plaintiff’s acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff’s patent portfolio, and again offered to provide Defendants with access to a data room containing information related to Defendants’ use of the American Express patent portfolio and the ‘750 patent. These are non-limiting examples of notice to Defendants, and Defendants received notice on further occasions.

241. 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), distributors, partners, issuers, acquirers, merchants, customers, clients, and/or consumers and payment platforms (e.g., Samsung and Google mobile wallets) that distribute, purchase, offer to sell, sale, use, and service the Accused Instrumentalities to directly infringe one or more claims of the ‘750 patent by using, offering for sale, selling, and/or servicing the Accused Instrumentalities.

Since at least the notice provided on the above-mentioned date, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '750 patent.

242. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, licensees, issuers, acquirers, merchants, partners, customers, consumers, and clients and other 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 other mobile payment systems, including with mobile wallet applications; as provider of products, systems and services associated with Visa Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet providers, point of sale terminal providers, merchants (including online and mail order), and users; maintaining such EMV payment applications by personalizing transaction devices 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 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 Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., usa.visa.com; partner.visa.com; technologypartner.visa.com) and mobile applications for clients, customers, and consumers for registering, activating, maintaining, and using (including accessing infringing features of) the

Accused Instrumentalities; and/or providing technical support and services for these products and services to licensees, issuers, acquirers, partners, customers, consumers, and clients, in the United States. *See, e.g., Visa Ready, VISA PARTNER, <https://partner.visa.com/site/programs/visa-ready.html>* (last visited Dec. 5, 2022) (“The Visa Ready certification program helps technology companies build and launch payment solutions that meet Visa's global standards around security and functionality.”).

243. Moreover, Defendants induce licensees, issuers, acquirers, partners, customers, consumers, and clients to directly infringe by requiring these parties to register with Visa and to enter license and other agreements. These agreements provide access to Visa’s “chip and mobile technology, software applets as well as Visa Ready and Approval Services testing materials.” *See Registration & Licensing, VISA, <https://technologypartner.visa.com/Registration/>* (describing the access that registrants and licensees are provided to, for example, “Visa’s Chip Specifications and Software,” “Mobile Specifications and Software,” and “Visa payWave for Mobile Developers”) (last visited Dec. 5, 2022).

244. 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.

245. 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. 8,150,746)

246. Plaintiff incorporates paragraphs 1 through 225 herein by reference.

247. Plaintiff is the assignee of the '746 patent, entitled "Global Account Reconciliation Tool," with ownership of all substantial rights in the '746 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

248. The '746 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '746 patent issued from U.S. Patent Application No. 13/009,528.

249. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '746 patent in this District and elsewhere in Texas and the United States.

250. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '746 patent, which includes Defendants' offering, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling, and/or deriving substantial revenue from financial transactions and payments for card accounts for Visa Cards and related products, processes, and services for Defendants' licensees, issuers, acquirers, partners, merchants, customers, consumers,

and clients, including Defendants' internal payment processing, authentication, authorization, validation, reconciliation, and fraud detection systems and methods, related to at least Defendants' Visa DPS products, services, systems, and/or Defendants' card products (e.g., Visa Cards), as used in contactless chips, mobile payments, and digital wallets.

251. Defendants directly infringe, individually and/or jointly with at least one other entity, the '746 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '746 patent to, for example, its alter egos, agents, intermediaries, licensees, acquirers, issuers, merchants, partners, customers, consumers, and clients.

252. Defendant VISA INC directly infringes the '746 patent through its direct involvement in the activities of its subsidiaries and/or divisions, including Defendant VISA USA and/or Visa DPS, including by distributing, selling, offering for sale, and servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '746 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using those Accused Instrumentalities. Specifically, VISA USA, as VISA INC's operational company in the U.S., identifies itself, including via branding, as the entity that provides Visa Cards to Defendants' licensees, acquirers, issuers, partners, merchants, customers, consumers, and clients. Additionally, VISA INC identifies Visa DPS as "one of the largest issuer processors of Visa debit transactions in the world" and indicates that Visa DPS is the provider of at least some of VISA INC's "Value Added Services" and "Issuing Solutions."

253. Furthermore, the Defendants act through their agents and/or contract with third parties, including, but not limited to, alter egos, intermediaries, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers to perform one or more steps of the claimed methods of the '746 patent. *Akamai Techs.*, 797 F.3d at 1023-24 (“[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 implementing and performing methods pursuant to at least EMV standards incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements so that Defendants’ Visa Card, Visa Transaction Instrument, and Visa payment network users may utilize such features in a point-of-sale transaction. As part of the Defendants’ agreements with such third parties to provide access to Visa payment networks (i.e., VisaNet), Defendants establish the manner of the performance of such services, e.g., that such Visa Card transactions must support EMV standards for contactless and mobile payments, as a condition of each third party’s participation in Visa Card-related transactions and in order to receive the benefit of a user of Visa’s brand or trademark, the Visa Cards, Visa Transaction Instruments, the VisaNet, and other related Visa products and 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.”). Each third party’s (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) activities in providing Visa Card services to cardholders are thus

attributed to the Defendants such that Defendants become the “single actor” chargeable with the direct infringement.

254. In addition to the liability arising from the Defendants’ relationship with third parties, Defendants also directly infringe, individually and/or jointly, the ‘746 patent via their own provision of Visa DPS services and/or card products, methods, and services that implement EMV standards in mobile or contactless card transactions associated with Visa Cards. On information and belief, Defendants design and develop systems and services for processing financial data and transactions, for example, the products offered by Visa DPS. On information and belief, Defendants design and develop payment applications for accounts for Visa Cards, which are used with physical Visa Cards and digital wallets. These products are issued by partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial credit, debit, or prepaid account. *See, e.g., Find Your Visa Card*, VISA, <https://usa.visa.com/pay-with-visa/find-card/> (last visited Dec. 5, 2022) (providing examples of Visa Cards).

255. As an example, Defendants infringe claim 1 of the ‘746 patent via their Accused Instrumentalities that implement systems and services for processing financial data and transactions and/or that implement EMV standards for mobile or contactless payments, including Visa’s contactless chip devices 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 incorporated into the Visa Smart/Credit Service, the quick VSDC, the Visa Contactless Payment Specification (VCPS), and the Visa Requirements. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Visa Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and use the VisaNet

for the authorization and settlement of payment transactions. Defendants' mobile payments can be facilitated by Visa provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Visa Cards. Or such contactless payments can be facilitated by using contactless chips embedded on the physical Visa Cards. Defendants' systems and services for processing financial data and transactions are provided, for example, via Visa DPS products. Defendants perform and/or direct and control the infringing systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, customers, consumers, and clients, for the processing of, the authorization of, the settlement of, and the reconciliation of financial data and/or transactions, including, for example, mobile or contactless payments conducted using Visa Cards.

256. The Accused Instrumentalities implement the method of claim 1 of the '746 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: extracting, by a computer based system for managing remote financial data, remote financial data from a financial data system using at least one of a standardized template and a customized template; converting, by the computer based system, the remote financial data from a second format to a first format via the standardized template; converting, by the computer based system, the remote financial data from a third format to the first format via the customized template; and reconciling, by the computer based system, the remote financial data from the standardized template and the customized template to master financial data, wherein the master financial data is stored in a first format.

257. At a minimum, Defendants have known of the '746 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted repeatedly to provide

Defendants with notice of Plaintiff's American Express patent portfolio that includes the '746 patent. Defendants have known about the American Express patent portfolio, which includes the '746 patent, since at least on or around April 3, 2018, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC ("DHG"), informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff's patent portfolio, and offered to provide Defendants with access to a data room containing information related to the American Express patent portfolio. A representative of Visa, Timothy Bedard, replied to the email on April 4, 2018. Defendants have known about the American Express patent portfolio, which includes the '746 patent, since at least on or around August 15, 2018, when Defendants sent correspondence to Plaintiff's indirect parent Dominion Harbor Enterprises, LLC, regarding a request that "Visa access an electronic data room containing certain patents/patent applications purportedly owned by Dominion Harbor Enterprises, LLC." Defendants have known about the American Express patent portfolio, which includes the '746 patent, since at least on or around September 18, 2018, when Visa was sent, on behalf of Plaintiff, access to a data room containing claim charts for patents in the American Express patent portfolio. Moreover, Defendants have known about the American Express patent portfolio, which includes the '746 patent, since at least on or around October 3, 2022, when, via email, Plaintiff affiliate Dominion Harbor Group, LLC ("DHG"), again informed Defendants of Plaintiff's acquisition of the American Express patent portfolio, invited Defendants to engage in licensing discussions relating to Plaintiff's patent portfolio, and again offered to provide Defendants with access to a data room containing information related to Defendants' use of the American Express patent portfolio, which portfolio includes the '746 patent. These are non-limiting examples of notice to Defendants, and Defendants received notice on further occasions.

258. 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), distributors, partners, issuers, acquirers, merchants, customers, clients, and/or consumers and/or financial data processing platforms and/or service providers and/or payment platforms (e.g., Samsung and Google mobile wallets) that distribute, purchase, offer to sell, sale, use, and/or service the Accused Instrumentalities to directly infringe one or more claims of the '746 patent by using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '746 patent.

259. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by financial data processing platforms, service providers, intermediaries, licensees, issuers, acquirers, merchants, partners, customers, consumers, clients and/or other payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; making, testing and/or using financial data processing systems; processing and/or reconciling financial data and/or transactions; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with other mobile payment systems, including with mobile wallet applications; as provider of products, systems and services associated with Visa Cards, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet providers, point of sale terminal providers, merchants (including online and mail order), and users; maintaining such EMV payment applications by personalizing transaction devices 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 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 Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., usa.visa.com; partner.visa.com; technologypartner.visa.com) and mobile applications for clients, customers, and consumers for registering, activating, maintaining, and using (including accessing infringing features of) the Accused Instrumentalities; and/or providing technical support and services for these products and services to licensees, issuers, acquirers, partners, customers, consumers, and clients, in the United States. *See, e.g., Visa Ready, VISA PARTNER, <https://partner.visa.com/site/programs/visa-ready.html> (last visited Dec. 5, 2022)* (“The Visa Ready certification program helps technology companies build and launch payment solutions that meet Visa's global standards around security and functionality.”).

260. Moreover, Defendants induce licensees, issuers, acquirers, partners, customers, consumers, and clients to directly infringe by requiring these parties to register with Visa and/or to enter license and/or other agreements. These agreements provide access to Visa DPS systems and/or Visa's “chip and mobile technology, software applets as well as Visa Ready and Approval Services testing materials.” *See Visa DPS, VISA, <https://usa.visa.com/sites/visa-dps.html> (encouraging potential clients to “[g]row your business with a trusted partner,” namely Visa DPS) (last visited May 18, 2023); Visa DPS Solutions – Flexible products and services built around your needs, VISA, <https://usa.visa.com/sites/visa-dps/our-solutions.html#63b17d3f19> (inviting potential clients to “[f]ind out how Visa DPS can support your processing needs,” and explaining “[w]e [Visa DPS] provide our clients with a comprehensive solution and single point of access to Visa payment*

products and services, as well as other global capabilities” and listing “value added services” including “Transaction processing at scale,” “Integration with 20+ network flows,” “Managed settlement and network compliance,” “Payment fraud mitigation,” “Dispute management,” “Visa Data Manager,” “Visa Campaign Solutions,” “Cards and credentials,” “Contact center,” “Terminal Driving,” and “Digital enablement”) (last visited May 18, 2023); *Registration & Licensing*, VISA, <https://technologypartner.visa.com/Registration/> (describing the access that registrants and licensees are provided to, for example, “Visa’s Chip Specifications and Software,” “Mobile Specifications and Software,” and “Visa payWave for Mobile Developers”) (last visited Dec. 5, 2022).

261. On information and belief, despite having knowledge of the ‘746 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the ‘746 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Defendants’ infringing activities relative to the ‘746 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.

262. 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

263. 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.

264. 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

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

PRAYER FOR RELIEF

266. 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: June 21, 2023

Respectfully submitted,

/s/ Terry A. Saad

Terry A. Saad (lead attorney)

Texas Bar No. 24066015

E-mail: tsaad@bosfirm.com

Jeffrey R. Bragalone

Texas Bar No. 02855775

E-mail: jbragalone@bosfirm.com

Marcus Benavides

Texas Bar No. 24035574

E-mail: mbenavides@bosfirm.com

Brandon V. Zuniga

Texas Bar No. 24088720

E-mail: bzuniga@bosfirm.com

Mark M.R. Douglass

Texas Bar No. 24131184

E-mail: 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**