IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

LIBERTY PEAK VENTURES, LLC, Plaintiff, v. FISERV, INC. AND FISERV SOLUTIONS, LLC, Defendants.	§ § § § § § § § § §	CIVIL ACTION NO. _____ JURY TRIAL DEMANDED

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Liberty Peak Ventures, LLC files this Complaint in this Eastern District of Texas (the "District") against Defendants Fiserv, Inc. and Fiserv Solutions, LLC (collectively, "Defendants" or "Fiserv") for infringement of U.S. Patent Nos. 8,851,369 (the "'369 patent"), 8,814,039 (the "'039 patent"), 8,794,509, (the "'509 patent"), 7,953,671 (the "'671 patent"), 9,195,985 (the "'985 patent"), 7,587,756 (the "'756 patent"), 7,668,750 (the "'750 patent"), 7,312,707 (the "'707 patent"), 7,431,207 (the "'207 patent"), and 7,835,960 (the "'960 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 Fiserv, Inc. ("FSI") is a corporation organized under the laws of the state of Wisconsin, with its principal place of business located 255 Fiserv Drive, Brookfield, Wisconsin 53045, United States, and having at least one office located in this District, for example, at 6160 Warren Pkwy, Frisco, Texas 75034, United States. FSI may be served with process via its registered agents, including at least Corporation Service Company, 33 E Main

St, Ste 610, Madison, Wisconsin 53703-4655, United States, and/or via FSI's corporate officers. FSI is a publicly traded company on The NASDAQ Stock Market LLC under the symbol "FISV."

3. On information and belief, Defendant Fiserv Solutions, LLC ("FSS") is a corporation organized under the laws of the state of Wisconsin, with its principal place of business located 255 Fiserv Drive, Brookfield, Wisconsin 53045, United States, and having at least one office located in this District, for example, at 6160 Warren Pkwy, Frisco, Texas 75034, United States. FSS may be served with process via its registered agents, including at least Corporation Service Company dba CSC - Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701-3218, United States and/or FSS's corporate officers. FSS is a wholly owned subsidiary of Defendant Fiserv, Inc.

4. FSI and FSS are collectively referred to as Fiserv in this complaint. According to Fiserv's annual report for the fiscal year ending December 31, 2022, "In this report, all references to 'we,' 'us,' 'our' and 'Fiserv' refer to Fiserv, Inc. ('Fiserv'), and, unless the context otherwise requires, its consolidated subsidiaries." *See Annual Report for the Fiscal Year Ended December 31, 2022*, FISERV, INC., p. 2, https://investors.fiserv.com/sec-filings/annual-reports##document-297-0000798354-23-000004-2 (last accessed Oct. 11, 2023) [hereinafter "2022 Annual Report"].

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

6. The term "Fiserv Cards" is used herein to refer collectively to all payment, banking, credit, debit and/or prepaid cards (including without limitation Mastercard Cards) that are offered

by Fiserv, serviced by Fiserv, provisioned by Fiserv, provided by Fiserv, issued by Fiserv or a third-party subject to terms of use required by Fiserv, and/or procured, supplied, or made by Fiserv.

7. According to the 2020 Annual Report, Fiserv, Inc. is a leading global provider of payments and financial services technology solutions" and [Fiserv] "serve[s] clients around the globe, including merchants, banks, credit unions, other financial institutions and corporate clients." *Id.* Fiserv states that it has "a commitment to innovation and excellence in areas including account processing and digital banking solutions; card issuer processing and network services; payments; e-commerce; merchant acquiring and processing; and the Clover cloud-based point-of-sale ("POS") and business management platform." *Id.*

8. Fiserv states that it "serve[s] [its] global client base by working among [its] geographic teams across various regions, including the United States and Canada; Europe, Middle East and Africa; Latin America; and Asia Pacific." *Id.*

9. "In 2022, [Fiserv] had $17.7 billion in total revenue, $3.7 billion in operating income and $4.6 billion of net cash provided by operating activities." *Id.* "Processing and services revenue, which in 2022 represented 82% of our total revenue, is primarily generated from account- and transaction-based fees under multi-year contracts that generally have high renewal rates." *Id.* [Fiserv] ha[s] operations and offices located both within the United States (the "U.S." or "domestic") and outside of the U.S. ("international") with revenues from domestic and international products and services as a percentage of total revenue as follows for the years ended December 31:"

(In millions)	2022	2021	2020
Total revenue	$ 17,737	$ 16,226	$ 14,852
Domestic	86 %	86 %	87 %
International	14 %	14 %	13 %

Id.

10. "[Fiserv's] operations are comprised of the Merchant Acceptance ('Acceptance') segment, the Financial Technology ('Fintech') segment and the Payments and Network ('Payments') segment." *Id.*

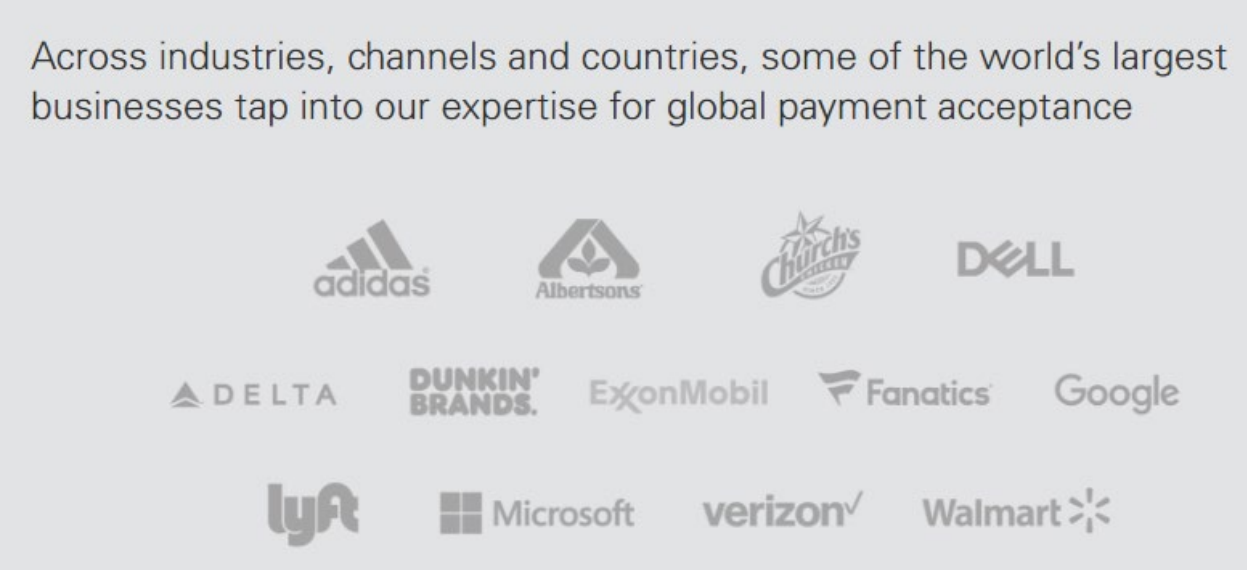
11. EMV specifications are developed and managed by EMVCo, which "is a global technical body that facilitates worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV Specifications and related testing processes." *See Overview of EMVCo*, EMVCo, https://www.emvco.com/about-us/overview-of-emvco/ (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, Fiserv co-owns EMVCo, along with five other member organizations, who each serve on EMVCo's Board of Managers. *See id*.

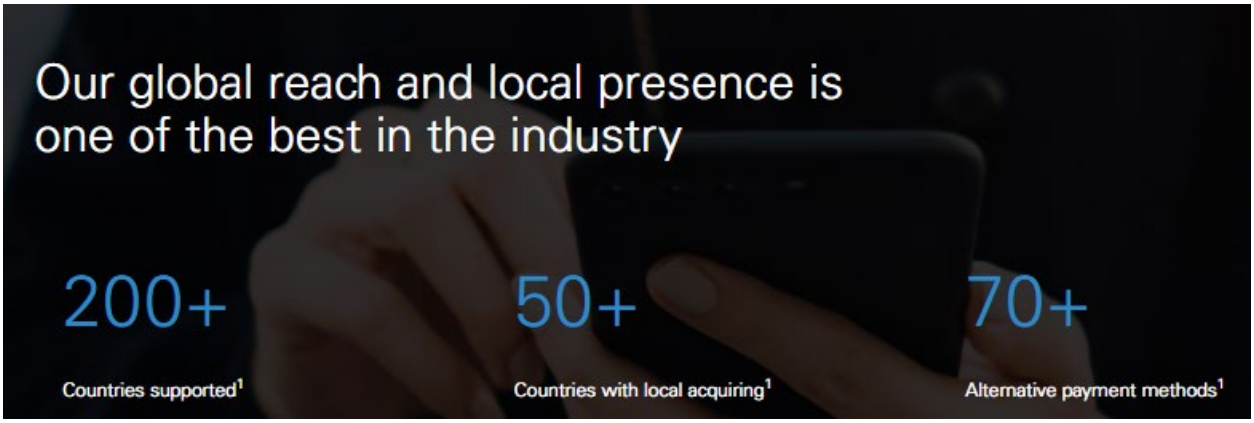
12. On information and belief, Fiserv utilizes and/or requires its partners, issuers, acquirers, merchants, customers and/or clients to utilize EMV processes documented in the specifications during any transaction in connection with Fiserv products, methods, and/or services, for example, transactions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

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

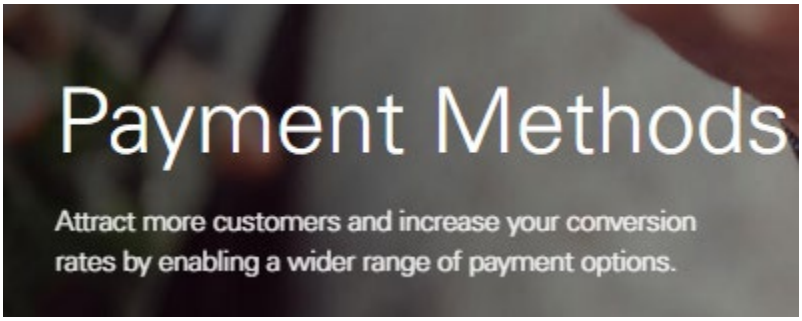
14. The Asserted Patents cover Fiserv's products, methods and/or services related to offering, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from transactions and payments, for example, via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

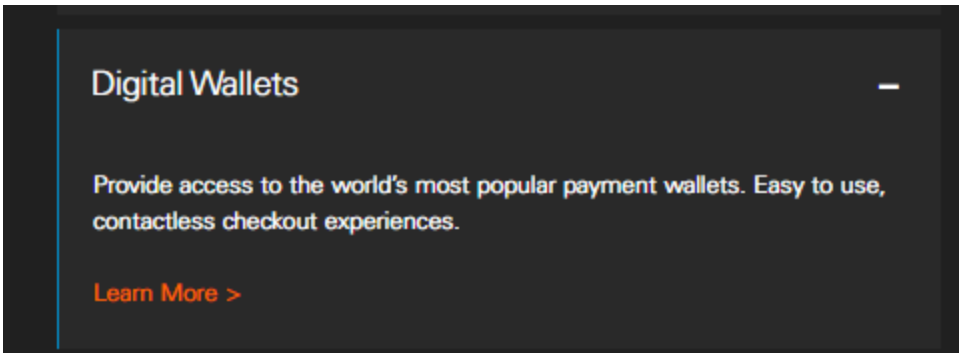
15. On information and belief, Defendants, on their own and/or via alter egos, agents, subsidiaries, partners, and affiliates, maintain a corporate and commercial presence in the United States, including in Texas and this District, via at least their 1) physical offices in Texas, including this District; 2) Fiserv's online presence (e.g., fiserv.com) that provides Fiserv's clients and consumers with access to and/or markets Fiserv's products, methods, and/or services, including those identified as infringing herein; and 3) consumers and clients of Fiserv who utilize, for example, Mastercard Cards and associated products, methods and/or services, at the point of sale, including via contactless payment methods, in numerous merchant physical and online sites, e.g., retail stores, restaurants, and other service providers accepting Mastercard Cards. As can be seen below, Fiserv provides services on a global scale for large, well-known companies.

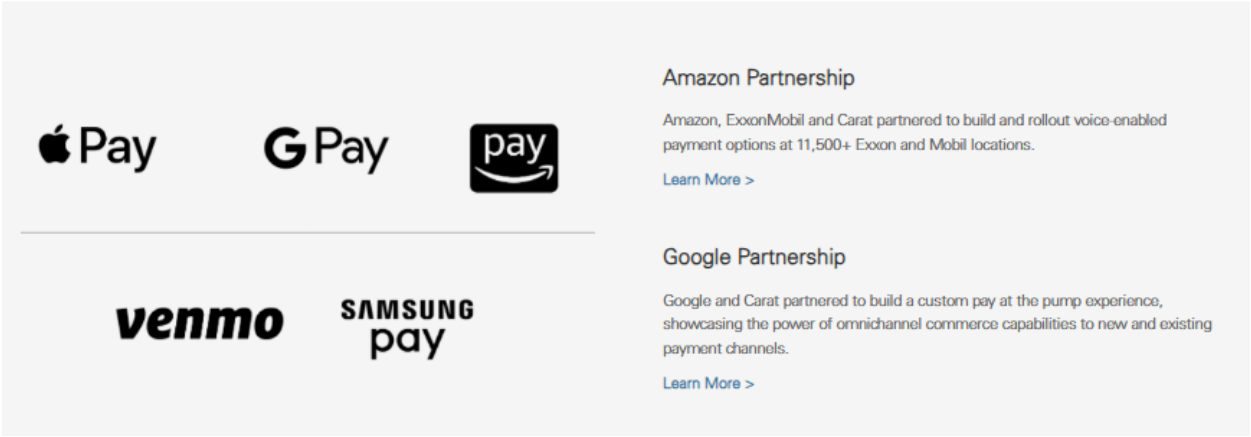




See Carat: Payment Acceptance, FISERV, https://www.carat.fiserv.com/en-us/solutions/ecommerce/ (last visited Oct. 12, 2023).







See Carat: Payment Methods, FISERV, https://www.carat.fiserv.com/en-us/solutions/payment-methods/ (last visited Oct. 20, 2023).

16. Such services associated with Fiserv's transaction instruments (e.g., Mastercard Cards) include systems and methods for processing digital transactions via online transactions and mobile payment solutions. *See, e.g., 2022 Annual Report*, at 5-11. Defendants, on their own and/or via related entities, their parent, alter egos, agents, subsidiaries, partners and/or affiliates, maintain at least one office in this District, for example, located at 6160 Warren Pkwy, Frisco, Texas 75034, United States. On information and belief, this office is a location where Defendants, on their own and/or via related entities, their parent, alter egos, agents, subsidiaries, partners and/or affiliates, maintain employees, including, for example, employees who develop Fiserv's payment products, methods, and/or services, which include without limitation systems used for payment via

Mastercard Cards, Fiserv's VisionPLUS account processing platform, Fiserv's FirstVision payment processing solution, Fiserv's Carat payment processing product, Fiserv's Clover payment processing product, Fiserv's CardHub platform, Fiserv's provision of EMV 3D-Secure Authentication, and/or other products, methods, and/or services that infringe the Asserted Patents. *See, e.g.*, *Office Locations Frisco*, https://www.careers.fiserv.com/location-frisco (last visited Oct. 31, 2023) (showing Fiserv Office Location at 6160 Warren Pkwy, Frisco, TX 75034); *Find Your Forward!: Join our team*, FISERV, https://www.careers.fiserv.com/search-jobs/Texas%2C%20US/1758/3/6252001-4736286/31x25044/-99x25061/50/2 (last visited Oct. 12, 2023) (showing job posting for "VisionPLUS Solution Architect" in "Frisco, Texas"); *Fiserv: Issuing Solutions*, FISERV, https://www.fiserv.com/en-ap/who-we-serve/financial-institutions/issuing-solutions.html (last visited Oct. 12, 2023); *Jason Wilkins*, LINKEDIN, https://www.linkedin.com/in/Jason-wilkins-22105b96 (last visited Oct. 12, 2023) (showing a "Jason Wilkins" profile that lists job title as "Director of Software Engineering at Fiserv" from "Mar 2020 – Present," showing a total of "20 years 5 months" at Fiserv, and listing location as "Frisco, Texas, United States"). Accordingly, Defendants do business, including committing infringing acts, in the U.S., the state of Texas, and in this District.

JURISDICTION AND VENUE

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

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

A. Defendant FSI

19. On information and belief, Defendant FSI 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 related entities, alter egos, intermediaries, agents, distributors, partners, subsidiaries, clients, customers, affiliates, and/or consumers.

20. For example, FSI owns and/or controls multiple subsidiaries and affiliates, and at least one, including, but not limited to, Defendant FSS, has a significant business presence in the U.S. and in Texas. FSI, via its own activities and via at least wholly owned subsidiary FSS, has at least one office in Frisco, Texas, in this District, at 6160 Warren Pkwy, Frisco, Texas 75034, United States. *See Join our team*, FISERV, https://www.careers.fiserv.com/location-frisco (last visited Oct. 31, 2023) (showing job postings available in Frisco, TX); *Join our team: Frisco, TX*, FISERV, https://www.careers.fiserv.com/ (last visited Oct. 12, 2023) ("Associates in Frisco enable client success through a wide range of functions – from IT and finance to sales, customer support and management."). Travis County CAD search results show that Defendant FSI's subsidiary FSS is listed as the owner of the property at Fiserv's office 6160 Warren Pkwy, Frisco, Texas 75034, United States. *See Property Search*, COLLIN CENTRAL APPRAISAL DISTRICT, https://www.collincad.org/propertysearch?owner_name=9iserv&situs_street_suffix=&isd%5B%5D=any&city%5B%5D=any&prop_type%5B%5D=R&prop_type%5B%5D=P&prop_type%5B%5D=MH&active%5B%5D=1&year=2023&sort=G (last visited Oct. 12, 2022) (search for

"Fiserv"). FSS is registered to do business in Texas and is 100% owned by Fiserv, Inc. On information and belief, Fiserv's at least one office employs around 600 or more residents of the state of Texas and/or this District. *See, e.g., Exclusive: Fiserv to Consolidate 600 Employees, Multiple Offices in North Texas*, CoStar, https://product.costar.com/home/news/shared/195802 (Sep. 25, 2018) (last visited Oct. 12, 2023) (stating "Fiserv, a provider of online banking and mobile payment services, plans a major consolidation in the Dallas area by funneling about 600 employees from multiple offices into what the federal government says is the fastest-growing U.S. city: Frisco, Texas" and "The Brookfield, Wisconsin-based company said it plans to lease about 75,000 square feet that will span multiple floors in The Offices One building at 6160 Warren Parkway at Frisco Station").

21. Such a corporate and commercial presence in Texas, including in this District, by Defendant FSI furthers the development, design, manufacture, distribution, sale, and use of FSI's and Fiserv's infringing products, methods, and/or services, including without limitation those in connection with Defendants' offering gateway, payment processor, and/or transaction processor products, methods, and/or services; Defendants' tokenization products, methods, and/or services; EMV compliant POS products and services, for example, products, methods, and/or services for securing RFID transactions involving a PIC transaction device and/or mobile wallets using host card emulation; Defendants' provisioning EMV compliant payment applications to mobile wallets on behalf of card issuers; Defendants' providing processing, authorization, clearing and settlement services to its card issuer customers; Defendants' providing card issuance solutions for banks and financial institutions; and Defendants' offering, providing, issuing, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing, controlling and/or deriving substantial revenue from financial transactions, including without

limitation those associated with payment transaction instruments (e.g., Fiserv Transaction Instruments, Mastercard Transaction Instruments, and/or Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, acquirers, merchants, partners, customers, consumers, and clients, including Defendants' payment processing, authentication, authorization, validation, and fraud detection products, methods and/or services. Through direction and control of its related entities, alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and/or consumers, FSI 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 FSI would not offend traditional notions of fair play and substantial justice.

22. On information and belief, FSI directs and controls and/or otherwise directs and authorizes all activities of its related entities, alter egos, intermediaries, agents, subsidiaries, and affiliates, including, but not limited to Defendant FSS; Clover Network, LLC; Clover Network, Inc; First Data Corporation; First Data Services LLC; and/or First Data Merchant Services LLC. *See, e.g., 2022 Annual Report* at 2, 24-25 ("In this report, all references to 'we,' 'us,' 'our' and 'Fiserv' refer to Fiserv, Inc. ('Fiserv'), and, unless the context otherwise requires, its consolidated subsidiaries. . . . We have grown our business organically and through acquisitions, by signing new clients, expanding the products and services we provide to existing clients, offering new and enhanced products and services developed through innovation and acquisition, and extending our capabilities geographically, all of which have enabled us to deliver a wide range of integrated products and services and created new opportunities for growth."). Via its own activities and via at least these entities, FSI has substantial business operations in Texas, which include without

limitation the provision of products and/or services, for example, payment processing services, to various entities including without limitation partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers. FSI has placed and continues to place infringing products and/or services for offering, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from commercial transactions via Fiserv Transaction Instruments (e.g., Mastercard Cards) and associated accounts, including without limitation related mobile, contactless, and online payment systems, into the U.S. stream of commerce. FSI has placed such products, methods, and/or services into the stream of commerce with the knowledge and understanding that such products, methods, and/or services are, will be, and continue to be sold, offered for sale, and/or used in this District and the State of 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.").

23. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391 and/or 1400(b). As alleged herein, Defendant FSI has committed acts of infringement in this District. As further alleged herein, Defendant FSI, via its own operations and employees located there and via ratification of Defendant FSS's presence and/or the presence of other subsidiaries as agents and/or alter egos of FSI, has a regular and established place of business, in this District at least at an office located at 6160 Warren Pkwy, Frisco, Texas 75034, United States. Accordingly, FSI may be sued in this district under 28 U.S.C. § 1400(b).

B. Defendant FSS

24. On information and belief, Defendant FSS 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, FSS, including as an agent and alter ego of parent company FSI, is listed as the owner of the property at Fiserv's office 6160 Warren Pkwy, Frisco, Texas 75034, United States. *See Property Search, COLLIN CENTRAL APPRAISAL DISTRICT, https://www.collincad.org/propertysearch?owner_name=13iserv&situs_street_suffix=&isd%5B%5D=any&city%5B%5D=any&prop_type%5B%5D=R&prop_type%5B%5D=P&prop_type%5B%5D=MH&active%5B%5D=1&year=2023&sort=G (last visited Oct. 12, 2022) (search for "Fiserv").* The at least one office in Frisco, Texas, employs around 600 or more employees that develop and/or provide products, methods, and/or services that include FSI and/or FSS offering, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from services related to Fiserv Transaction Instruments (e.g., Mastercard Cards), via Fiserv Transaction Instruments and associated accounts, including without limitation related mobile, contactless, and online payment systems, for Fiserv's customers, consumers, and clients in Texas and this District. *See, e.g., Exclusive: Fiserv to Consolidate 600 Employees, Multiple Offices in North Texas*, CoStar, https://product.costar.com/home/news/shared/195802 (Sep. 25, 2018) (last visited Oct. 12, 2023) (stating "Fiserv, a provider of online banking and mobile payment services, plans a major

consolidation in the Dallas area by funneling about 600 employees from multiple offices into what the federal government says is the fastest-growing U.S. city: Frisco, Texas" and "The Brookfield, Wisconsin-based company said it plans to lease about 75,000 square feet that will span multiple floors in The Offices One building at 6160 Warren Parkway at Frisco Station"). Additionally, on information and belief, Fiserv payment applications are stored on mobile devices, smart phones, tablets and/or computer chips embedded on Fiserv Transaction Instruments (e.g., Mastercard Cards) used in transactions in Texas and in this District. Fiserv payment applications utilize tokenization processes for facilitating transactions, including, for example, payments.

25. On information and belief, FSI and FSS conform to applicable standards (e.g., EMV standards) and/or require any entity that accesses or uses a Fiserv product and/or service, for example, all issuer and/or merchant systems interfacing with FSI and FSS systems, to conform to the applicable standards (e.g., EMV standards) when effecting payment transactions. Through direction and control of its alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers, FSS 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 FSI would not offend traditional notions of fair play and substantial justice.

26. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391 and/or 1400(b). Defendant FSS has committed acts of infringement in this District. As further alleged herein, Defendant FSS, via its own operations and employees located there and/or via ratification of its subsidiaries as agents and/or via alter egos of FSS, has a regular and established place of business,

in this District at least at an office located at 6160 Warren Pkwy, Frisco, Texas 75034, United States. Accordingly, FSS may be sued in this district under 28 U.S.C. § 1400(b).

27. Upon information and belief, Defendants FSI and FSS 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

28. The Asserted Patents cover various aspects of products (e.g., systems, networks, devices, technology, and/or applications), methods (e.g., processes), and services that include: Defendants' offering gateway, payment processor, and/or transaction processor products, methods, and/or services (including without limitation EMV 3-D Secure services for eCommerce websites, hosted payment forms and/or mobile apps); Defendants' tokenization products, methods, and/or services (e.g., Multi-pay Token service and/or Clover tokenization services that can replace card numbers with tokens); EMV compliant POS products (e.g., Clover and/or Carat RFID reader systems and devices) and services, for example, products, methods, and/or services for securing RFID transactions involving a PIC transaction device and/or mobile wallets using host card emulation (e.g., in connection with Google Pay and Samsung Pay mobile wallets); Defendants' provisioning EMV compliant payment applications to mobile wallets on behalf of card issuers; Defendants' providing processing, authorization, clearing and settlement services to its card issuer customers; Defendants' providing card issuance solutions for banks and financial institutions (e.g., making and selling EMV contactless cards to financial institutions and provisioning EMV compliant payment applications for consumers' cards onto mobile wallets); and Defendants' offering, providing, issuing, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing, controlling and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction

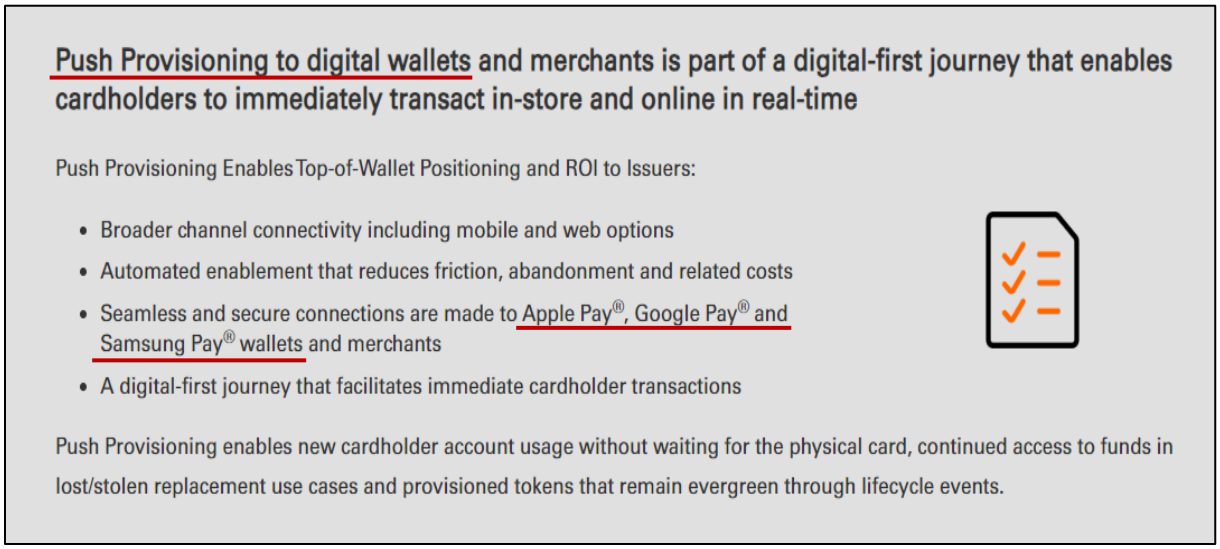
instruments (e.g., Fiserv Transaction Instruments, Fiserv Cards, Mastercard Transaction Instruments, and/or Mastercard Cards), associated accounts, and related products, methods, and/or services for Defendants' licensees, acquirers, merchants, partners, customers, consumers, and clients, including Defendants' payment processing, authentication, authorization, validation, and fraud detection products, methods and/or services (e.g., Fiserv's products used for payment transactions involving Mastercard Cards, Fiserv's VisionPLUS account processing platform, Fiserv's FirstVision payment processing solution, Fiserv's Carat payment processing solution, Fiserv's Clover payment processing solutions, and/or Fiserv's CardHub platform), referred to herein collectively as the "Accused Instrumentalities."

29. The Asserted Patents cover Accused Instrumentalities of Defendants that provide, facilitate, maintain, transact, authenticate, validate, authorize, clear, settle, and/or process financial data, financial transactions, mobile payments, contactless payments, and/or online payments using Fiserv Transaction Instruments (e.g., Mastercard Cards) and related access to Fiserv's payment products, methods, and/or services (e.g., solutions, systems, devices, networks, APIs, software development kits, and/or other product solutions) licensed by Defendants to their licensees, issuers, acquirers, partners, consumers, customers, and/or clients. Defendants use the Accused Instrumentalities to process financial data and transactions. Additionally, Defendants use the Accused Instrumentalities to issue or to facilitate the issuance of accounts (e.g., for cardholders of Mastercard Cards) by, for, and/or to Defendants' licensees and partners, consumers, 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 solutions (e.g., products, methods, and/or services) to process such payments. Defendants use the Accused Instrumentalities to provision EMV compliant payment applications

to mobile wallets on behalf of card issuers. Defendants use the Accused Instrumentalities to provide processing, authorization, clearing and settlement services to their card issuer customers. Defendants use the Accused Instrumentalities to provide card issuance solutions for banks and financial institutions, for example, by making and selling EMV contactless cards to financial institutions and provisioning EMV compliant payment applications for consumers' cards onto mobile wallets. Defendants use the Accused Instrumentalities to provide EMV 3-D Secure services for eCommerce websites, hosted payment forms and/or mobile apps. Defendants use the Accused Instrumentalities to provide tokenization products, methods, and/or services, for example, Multi-pay Token service and/or Clover tokenization services that can replace card numbers with tokens. At the point of purchase, Defendants use the Accused Instrumentalities to provide EMV compliant POS products, methods, and/or services, for example, Clover and/or Carat RFID reader systems and devices, which can be used for securing RFID transactions involving a PIC transaction device and/or mobile wallets using host card emulation in connection with Google Pay and Samsung Pay mobile wallets. Defendants also use the Accused Instrumentalities to provide digital solutions, including offering mobile wallets for contactless payments to cardholders (directly and/or via Defendants' issuers, licensees, partners, consumers, customers and/or clients) which are installed onto a mobile device of a cardholder. Such mobile wallets include an appropriate smartcard (e.g., Mastercard smartcard), API, and/or app installed on the mobile device (and in some cases, the software is native to the device). Defendants use the Accused Instrumentalities to provide to cardholders (directly and/or via Defendants' issuers, licensees, partners, consumers, customers and/or clients) embedded chip or smartcard technology that is integrated into a physical card, with Defendants' payment application software, API, or firmware installed. In other instances, the Accused Instrumentalities may be utilized in online purchases conducted over a network (e.g., the

Internet) and/or when the user of the payment card account is registering, activating, or maintaining an account.

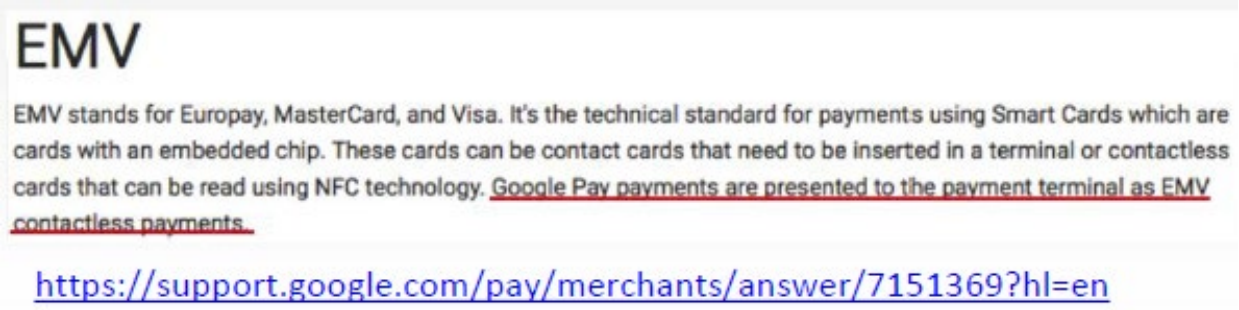
30. On information and belief, Defendants' services in connection with Fiserv Transaction Instruments (e.g., Mastercard Cards) utilize the Europay, Mastercard, and Visa (EMV) standards in processing, securing, and authenticating financial transactions. For example, Defendants provide, or direct and control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

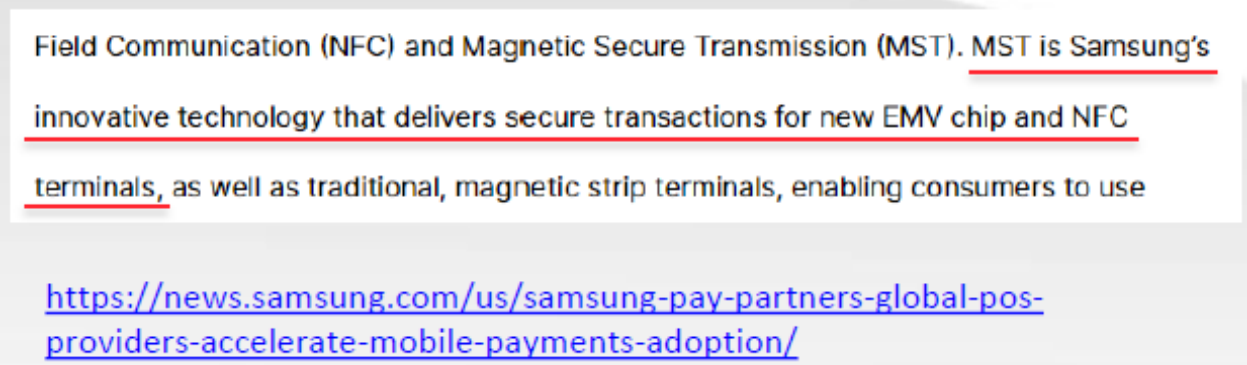


Real-Time Provisioning Drives Issuer Cards to Top of Wallet, FISERV, https://www.fiserv.com/en/solutions/payments/credit-and-debit-solutions/real-time-

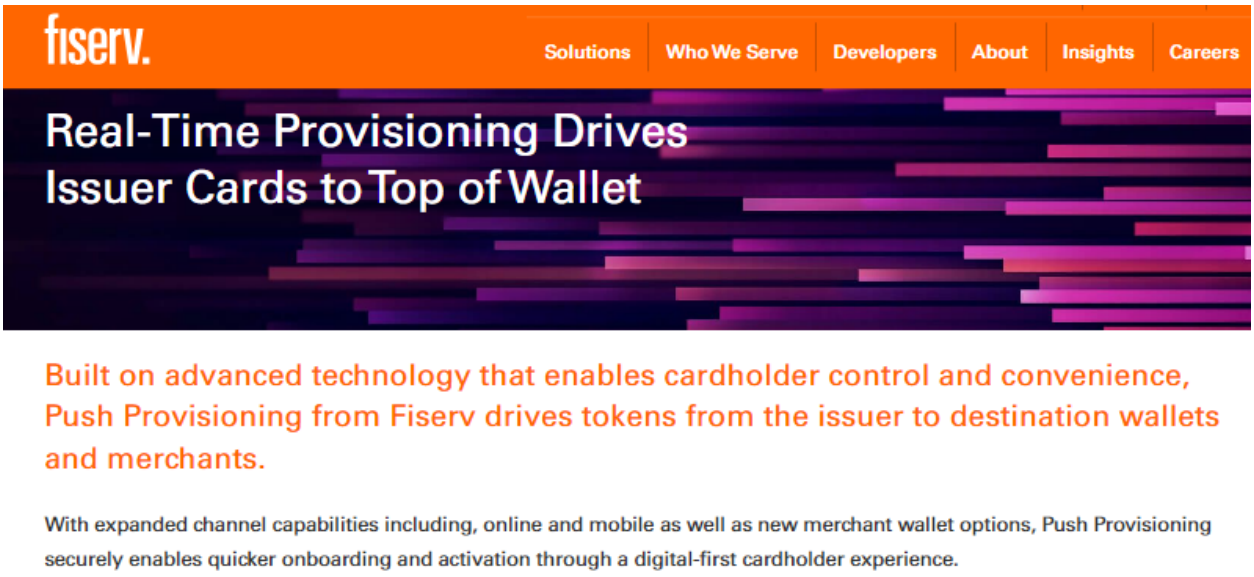
provisioning.html (last visited Oct. 12, 2023) (describing "Push Provisioning from Fiserv" that "drives tokens from the issuer to destination wallets and merchants").

31. 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.





32. On information and belief, as indicated below, Defendants directly and/or indirectly provide their payment technology to their licensees, issuers, acquirers, partners, merchants, clients, consumers, customers, cardholders, and/or other users at least for utilization in transactions involving Fiserv Transaction Instruments (e.g., Mastercard Cards). These payment products utilize Fiserv's provisioning services 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.



Real-Time Provisioning Drives Issuer Cards to Top of Wallet, FISERV, https://www.fiserv.com/en/solutions/payments/credit-and-debit-solutions/real-time-provisioning.html (last visited Oct. 23, 2023) (describing "Push Provisioning from Fiserv" that "drives tokens from the issuer to destination wallets and merchants").

33. The Accused Instrumentalities also include at least Mastercard Cards made, sold, provided and/or issued by Fiserv on behalf of or via direction and control of third parties; related products, methods, and/or services for card payments using a physical banking, payment, credit,

debit, or prepaid card having an embedded chip or smartcard; mobile payment systems (e.g., mobile wallets) and methods using Mastercard 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 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 "Mastercard Transaction Instruments").

34. The Accused Instrumentalities also include at least Fiserv Cards (e.g., Mastercard Cards) and Mastercard Transaction Instruments that are made, sold, provided and/or issued by Fiserv, including for example, on behalf of or via direction and control of third parties; related products, methods, and/or services for card payments using a physical banking, payment, credit, debit, or prepaid card having an embedded chip or smartcard, and systems operative to implement such methods and/or services; mobile payment systems (e.g., mobile wallets) and methods using Fiserv Cards and Mastercard Transaction Instruments 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 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 "Fiserv Transaction Instruments").

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

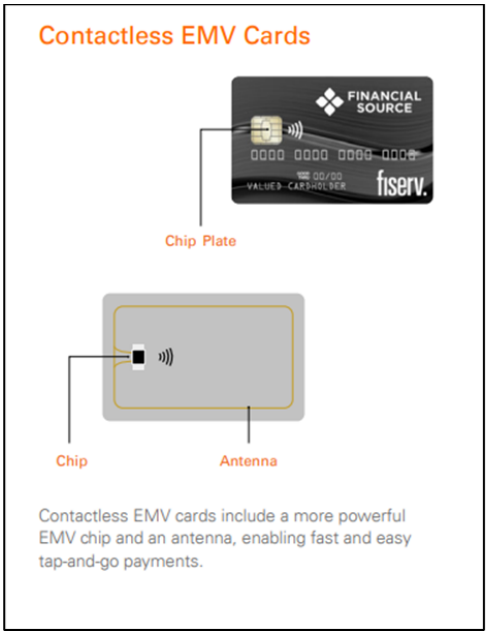
fiserv.

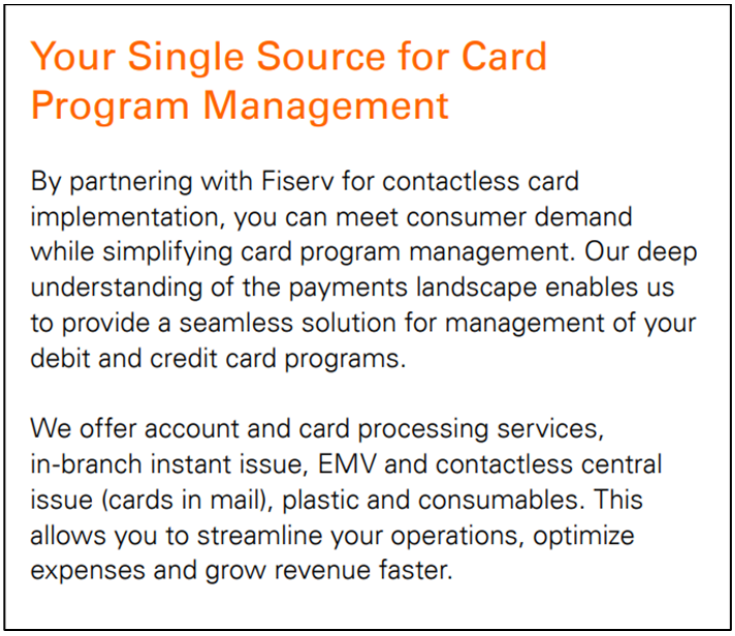
BEST-IN-CLASS CAPABILITIES

Credit Solutions

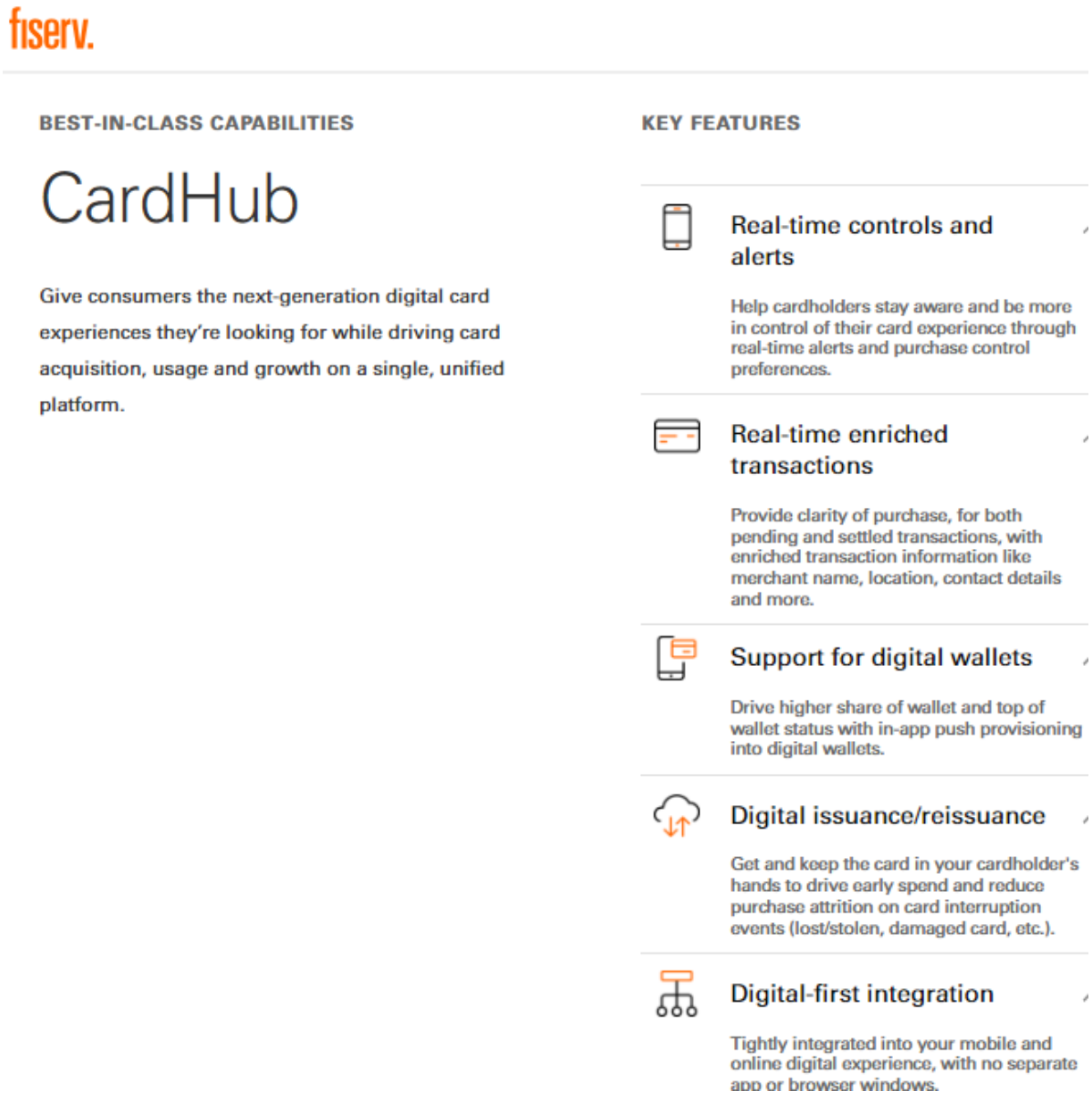
Deliver a complete credit card program that gives consumers control and meets their expectations.

See Credit Solutions, FISERV, https://www.fiserv.com/en/solutions/card-services/credit-solutions.html (last visited Oct. 13, 2023).

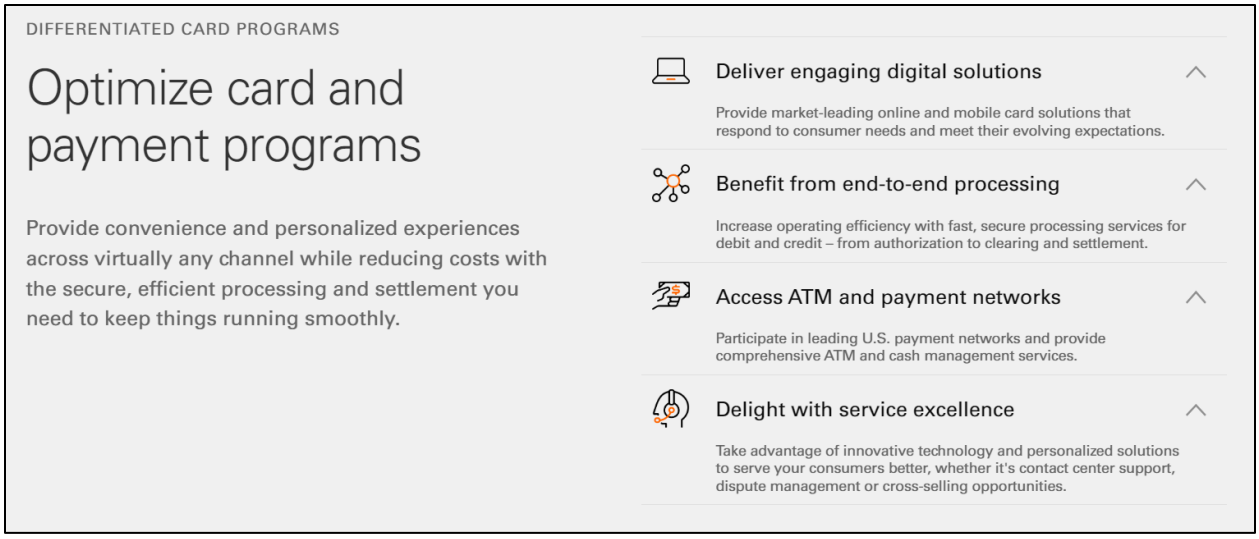




Solution: Contactless EMV® Cards, FISERV, https://www.fiserv.com/content/dam/fiserv-ent/final-files/marketing-collateral/sales-sheets/Contactless_EMV_Cards_Sales_Sheet_0221.pdf (last visited Oct. 13, 2023).

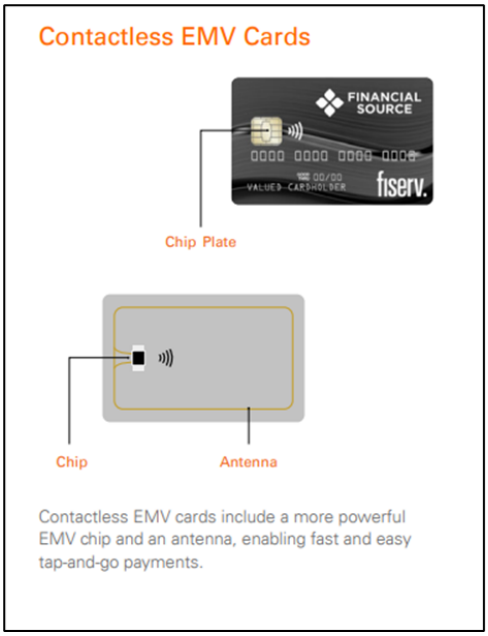


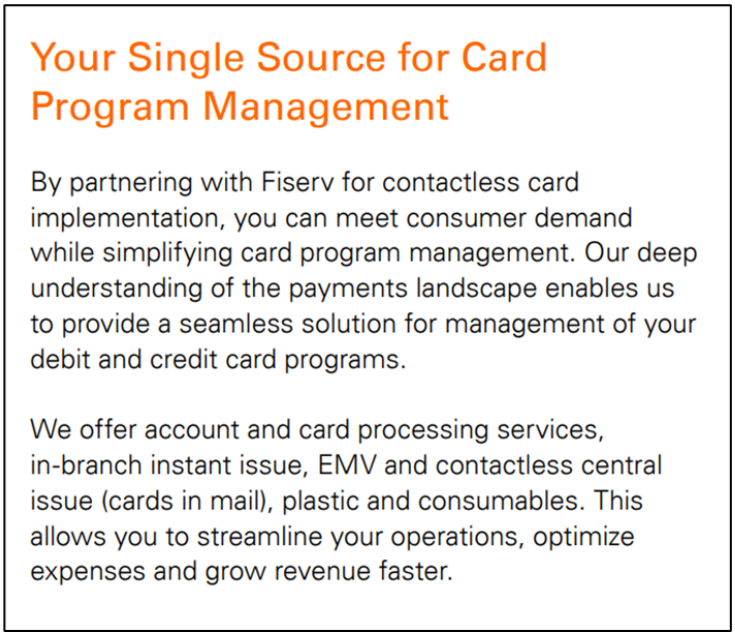
See CardHub, FISERV, https://www.fiserv.com/en/solutions/card-services/cardhub.html (last visited Oct. 13, 2023).



Optimize card and payment programs, FISERV, https://www.fiserv.com/en/solutions/card-services.html (last visited Oct. 12, 2023) ("Benefit from end-to-end processing . . . from authorization to clearing and settlement).

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

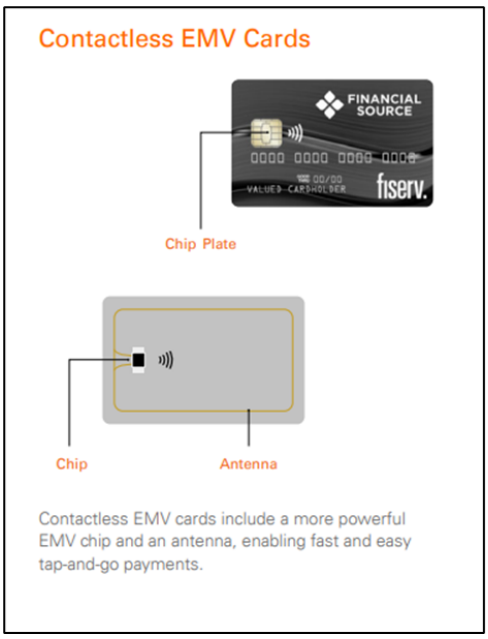


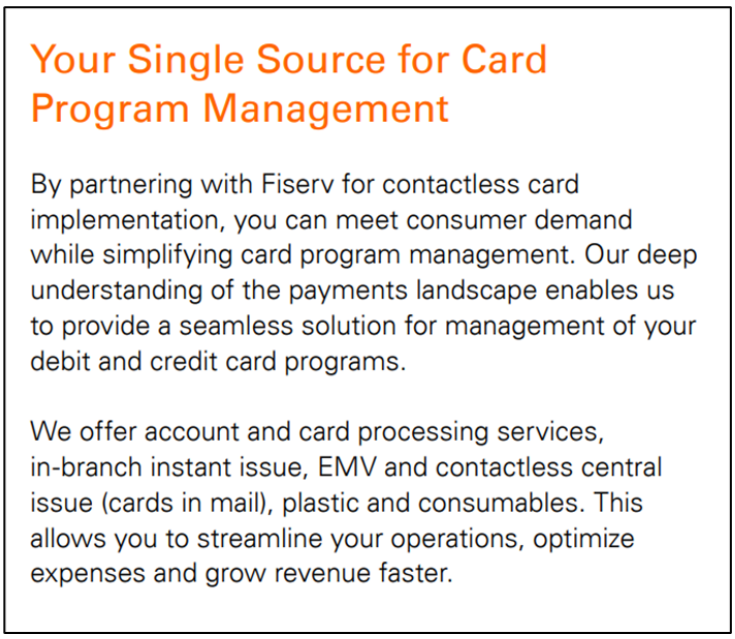


Solution: Contactless EMV® Cards, FISERV, https://www.fiserv.com/content/dam/fiserv-ent/final-files/marketing-collateral/sales-sheets/Contactless_EMV_Cards_Sales_Sheet_0221.pdf (last visited Oct. 13, 2023).

37. On information and belief, the Accused Instrumentalities include at least Defendants' payment card (e.g., banking, credit, debit, and prepaid card) related products, methods, and/or services for contactless payments that utilize EMV standards for contactless payment. *See, e.g., Secure Payment Cards*, FISERV, https://www.fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards.html (last visited Oct. 20, 2023) ("Fiserv offers high-quality, cost-effective manufacturing, personalization and delivery services for a wide variety of cards including debit, credit, ATM, prepaid and gift cards; EMV® and contactless cards; photo cards; membership; and healthcare ID cards. Fulfillment options include central and in-branch issuance to meet immediate needs."); *EMV and Contactless EMV Cards*, FISERV, https://www.fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards/central-issuance/emv-chip-cards.html (last visited Oct. 20, 2023) (noting "Fiserv offers the industry's most complete, comprehensive and integrated EMV solution" including "processing EMV transactions on the Visa®, Mastercard® and Accel® debit networks" and "[c]ontactless EMV cards").

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





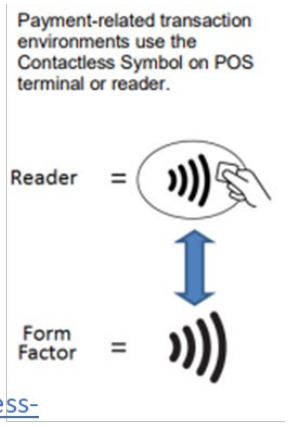
Solution: Contactless EMV® Cards, FISERV, https://www.fiserv.com/content/dam/fiserv-ent/final-files/marketing-collateral/sales-sheets/Contactless_EMV_Cards_Sales_Sheet_0221.pdf (last visited Oct. 13, 2023).

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

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

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

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



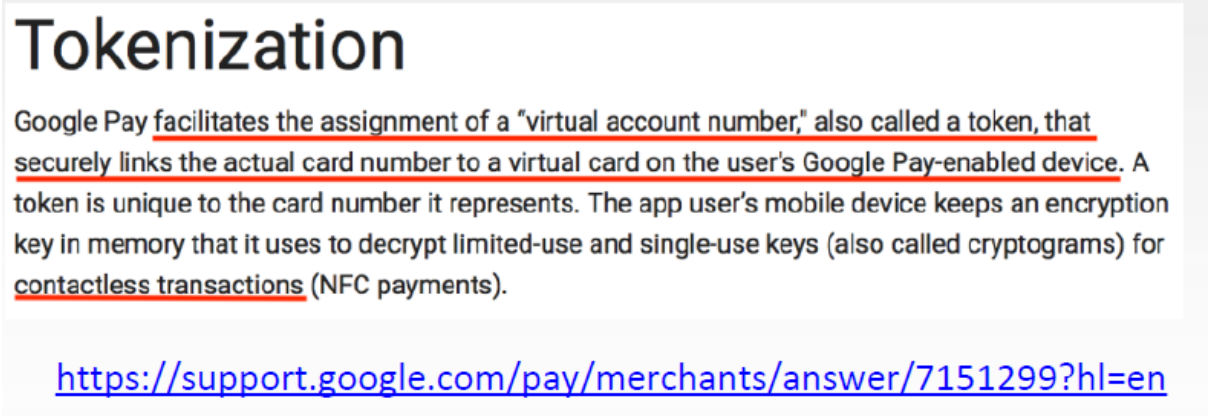
https://www.emvco.com/wp-content/uploads/2020/02/EMVCo-Contactless-Indicator-Reproduction-Requirements-Nov-2019.pdf

40. On information and belief, a process referred to as "tokenization," which is also part of the EMV standards, is also utilized by Defendants in authorizing transactions for Fiserv Transaction Instruments (e.g., Mastercard Cards), via online payments, in-app payments, and mobile payments. As explained below, a "payment token" is a "surrogate value for a PAN" (a primary account number). In tokenization, "Payment Tokens are requested, generated, issued, provisioned, and processed as a surrogate for PANs."

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

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

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



Tokenization

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

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

42. Defendants, as providers and/or licensors of solutions (e.g., products, methods, and/or services) to account issuers for Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments), merchants involved in transactions associated with Fiserv Transaction Instruments, and/or merchant acquirers involved in transactions associated with Fiserv Transaction Instruments, act on behalf of and/or 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/or cardholders, in the operation of the Fiserv Transaction Instruments using Fiserv's payment solutions (e.g., products, methods, and/or services). Defendants act on behalf of and/or direct and control the infringing activities of third parties by conditioning and permitting the use of Fiserv Transaction Instruments (and the benefits derived therefrom) upon performance by one or more of those third parties of a step or steps or by use by those third parties of certain claimed apparatuses or systems of the Asserted Patents. *See Akamai Techs. V. Limelight Networks*, 797 F.3d 1020, 1023-24. Moreover, by establishing and maintaining their payment products, methods, and/or services, Defendants further act on behalf of and/or direct and control the activities of third parties in infringing the Asserted Patents. For example, Defendants directly employ or require that third parties conform to EMV contactless standards in performing various EMV contactless transactions. *See, e.g., EMV and Contactless EMV Cards*, FISERV,

https://www.fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards/central-issuance/emv-chip-cards.html (last visited Oct. 20, 2023) (noting "Fiserv offers the industry's most complete, comprehensive and integrated EMV solution" including "processing EMV transactions on the Visa®, Mastercard® and Accel® debit networks" and "[c]ontactless EMV cards").

43. Additionally, Defendants, as providers and/or licensors of solutions, products, methods, and/or services to account issuers for Fiserv Transaction Instruments (e.g., Mastercard Cards), merchants involved in transactions associated with Fiserv Transaction Instruments, and/or merchant acquirers involved in transactions associated with Fiserv Transaction Instruments, act on behalf of and/or direct and control the activities of third parties in connection with the operation of mobile wallets. This is described below with respect to the mobile wallet Google Pay.

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

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

44. As an example of how Defendants act on behalf of and/or direct and control third parties in connection with mobile wallets, Defendants provision third-party mobile wallets with

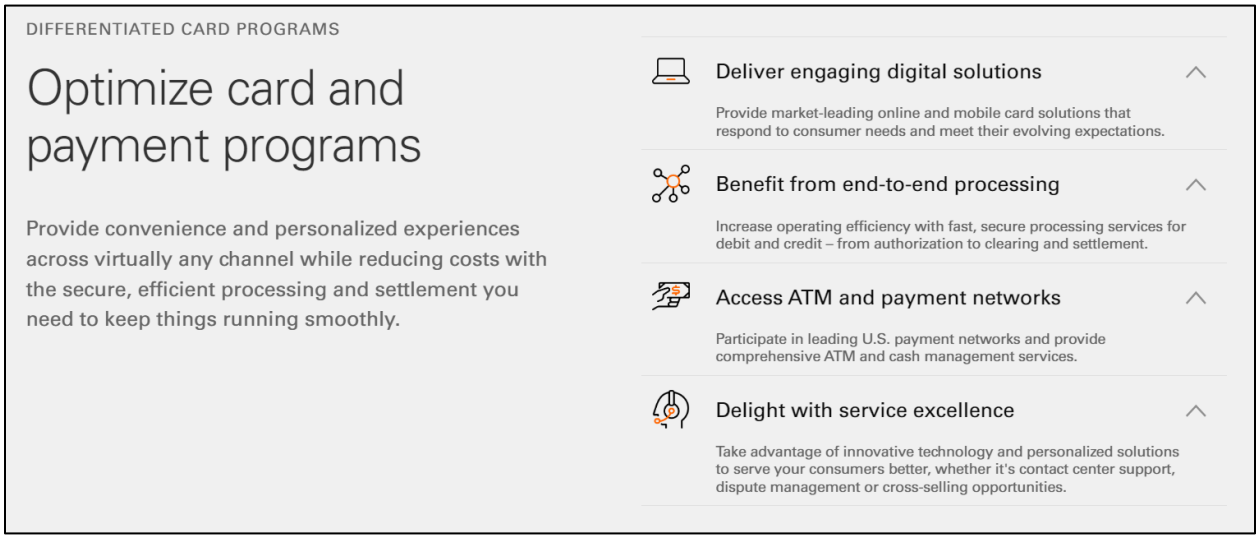
Defendants' own credentials and EMV payment applications, e.g., via Fiserv's push provisioning digital wallets. *See, e.g., Real-Time Provisioning Drives Issuer Cards to Top of Wallet*, FISERV, https://www.fiserv.com/en/solutions/payments/credit-and-debit-solutions/real-time-provisioning.html (last visited Oct. 12, 2023) (describing "Push Provisioning from Fiserv" that "drives tokens from the issuer to destination wallets and merchants").

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

46. 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 Fiserv Transaction Instruments (e.g., Mastercard Cards) to secure direct and safe transactions between consumers and merchants.

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



Optimize card and payment programs, FISERV, https://www.fiserv.com/en/solutions/card-services.html (last visited Oct. 12, 2023) ("Benefit from end-to-end processing . . . from authorization to clearing and settlement). Defendants also infringe the '671 patent via Defendants' computer-based systems that conduct user enrollment processes for mobile wallet payments associated with Fiserv Transaction Instruments (e.g., Mastercard Cards); and/or via direction and control of third parties in connection with these systems.

Push Provisioning to digital wallets and merchants is part of a digital-first journey that enables cardholders to immediately transact in-store and online in real-time

Push Provisioning Enables Top-of-Wallet Positioning and ROI to Issuers:

- Broader channel connectivity including mobile and web options
- Automated enablement that reduces friction, abandonment and related costs
- Seamless and secure connections are made to Apple Pay®, Google Pay® and Samsung Pay® wallets and merchants
- A digital-first journey that facilitates immediate cardholder transactions

Push Provisioning enables new cardholder account usage without waiting for the physical card, continued access to funds in lost/stolen replacement use cases and provisioned tokens that remain evergreen through lifecycle events.

Real-Time Provisioning Drives Issuer Cards to Top of Wallet, FISERV, https://www.fiserv.com/en/solutions/payments/credit-and-debit-solutions/real-time-provisioning.html (last visited Oct. 12, 2023) (describing "Push Provisioning from Fiserv" that "drives tokens from the issuer to destination wallets and merchants").

EMV

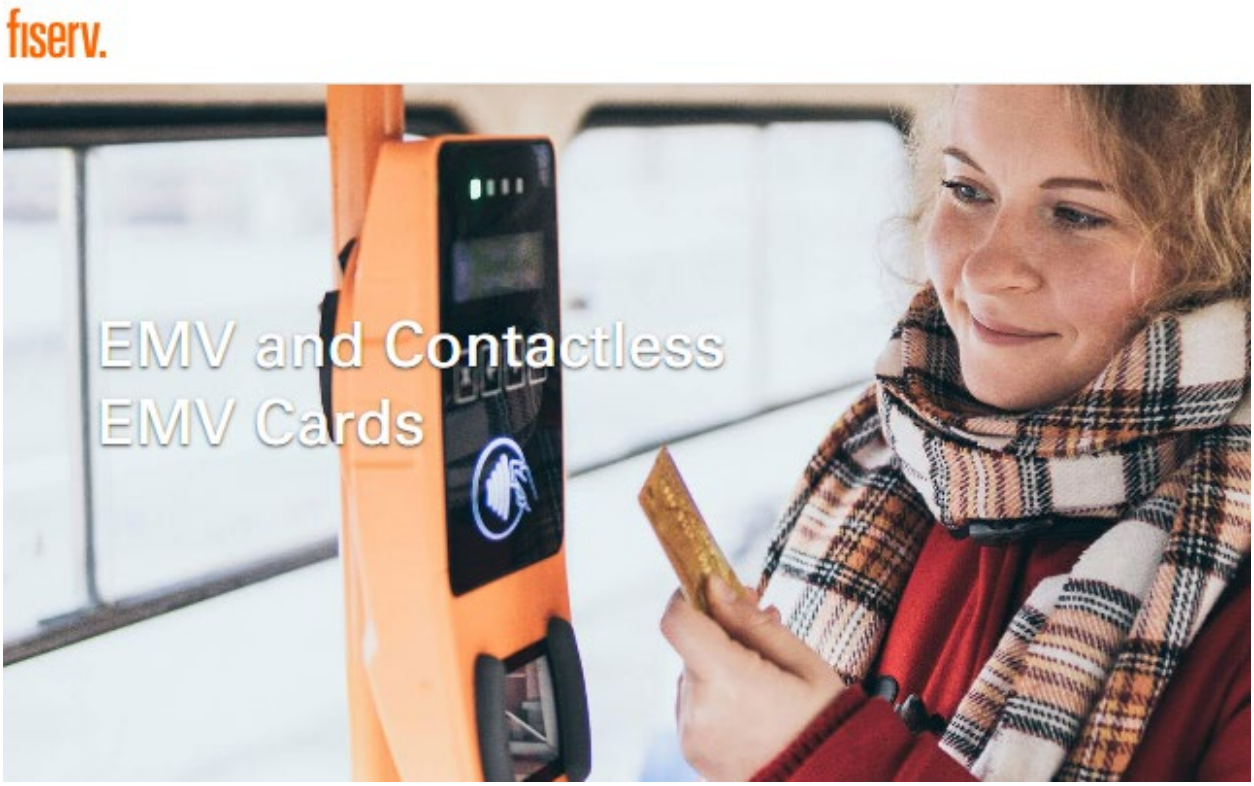
EMV stands for Europay, MasterCard, and Visa. It's the technical standard for payments using Smart Cards which are cards with an embedded chip. These cards can be contact cards that need to be inserted in a terminal or contactless cards that can be read using NFC technology. Google Pay payments are presented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

Google Pay Merchant Help: EMV, GOOGLE, https://support.google.com/pay/merchants/answer/7151369?hl=en (last visited Oct. 12, 2023).

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

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

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



Fiserv is ready to support your migration to EMV and contactless EMV cards. We help our clients make decisions on the critical elements of their card programs including chip configurations, card design, plastic procurement, key management, card personalization, project implementation and consumer education.

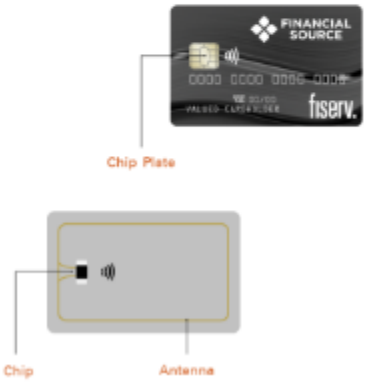
EMV Cards

Fiserv offers the industry's most complete, comprehensive and integrated EMV solution. That includes processing EMV transactions on the Visa®, Mastercard® and Accel® debit networks, EMV card personalization, and fraud and EMV risk management tools to detect, measure and defend against financial crime. Our standard EMV chip configurations are pre-certified to significantly reduce the time and expense associated with migration.

Contactless EMV Cards

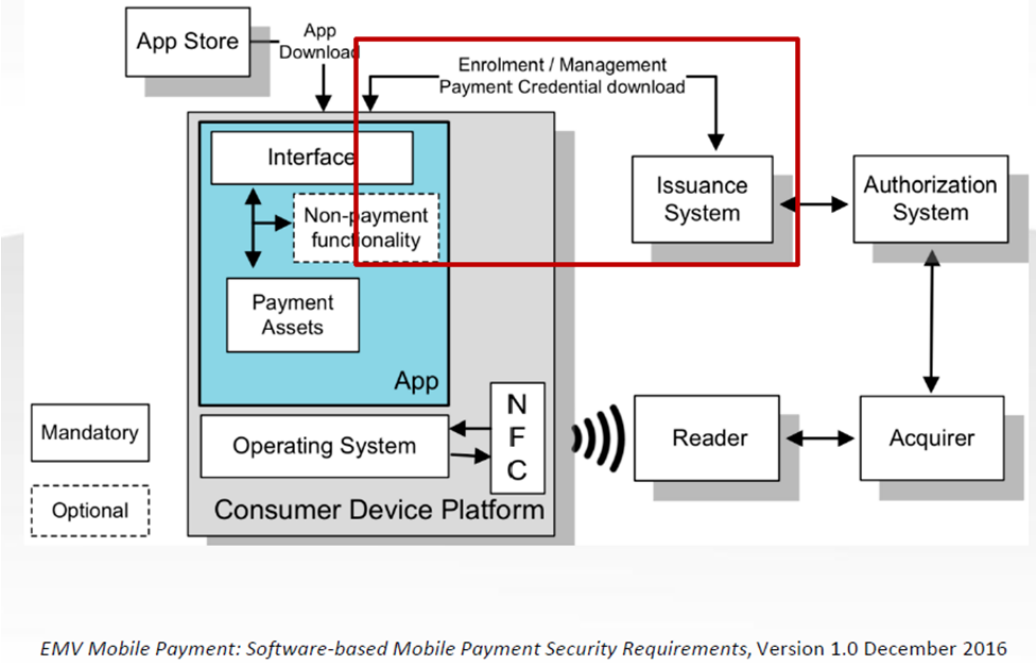
Contactless EMV cards from Fiserv include a more powerful EMV chip and an antenna, enabling fast and easy tap-and-go payments. Consumers like contactless cards because they are convenient, secure and innovative – yet they can be used anywhere conventional cards are accepted. With all of these advantages, contactless EMV cards can help you secure top-of-wallet positioning and grow transaction revenue.

- Antenna + more powerful EMV chip
- Transact when held within an inch of the POS terminal
- Can be inserted or swiped if contactless is not supported
- Contactless cards have the same high level of security as EMV cards; they just transmit the necessary data via antenna rather than a chip reader



EMV and Contactless EMV Cards, FISERV, https://www.fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards/central-issuance/emv-chip-cards.html (last visited Oct. 12, 2023).

Figure 2.2: Basic Mobile Payment System Overview (Example)



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

49. 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

50. Defendants further assemble credentials, including encryption keys, to be used when effecting transactions, referred to as "provisioning" below.

3.4 Provisioning and Credential Issuance

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

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

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

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

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

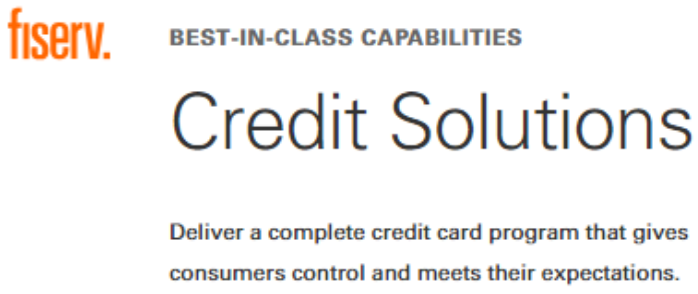
be useful for clarity. The ARQC is a cryptogram generated by the card from transaction data using an issuer key stored in the card and known at the issuer authorisation system. The issuer uses this key to authenticate the ARQC and thereby authenticate the card. This process is termed 'online card authentication'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

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

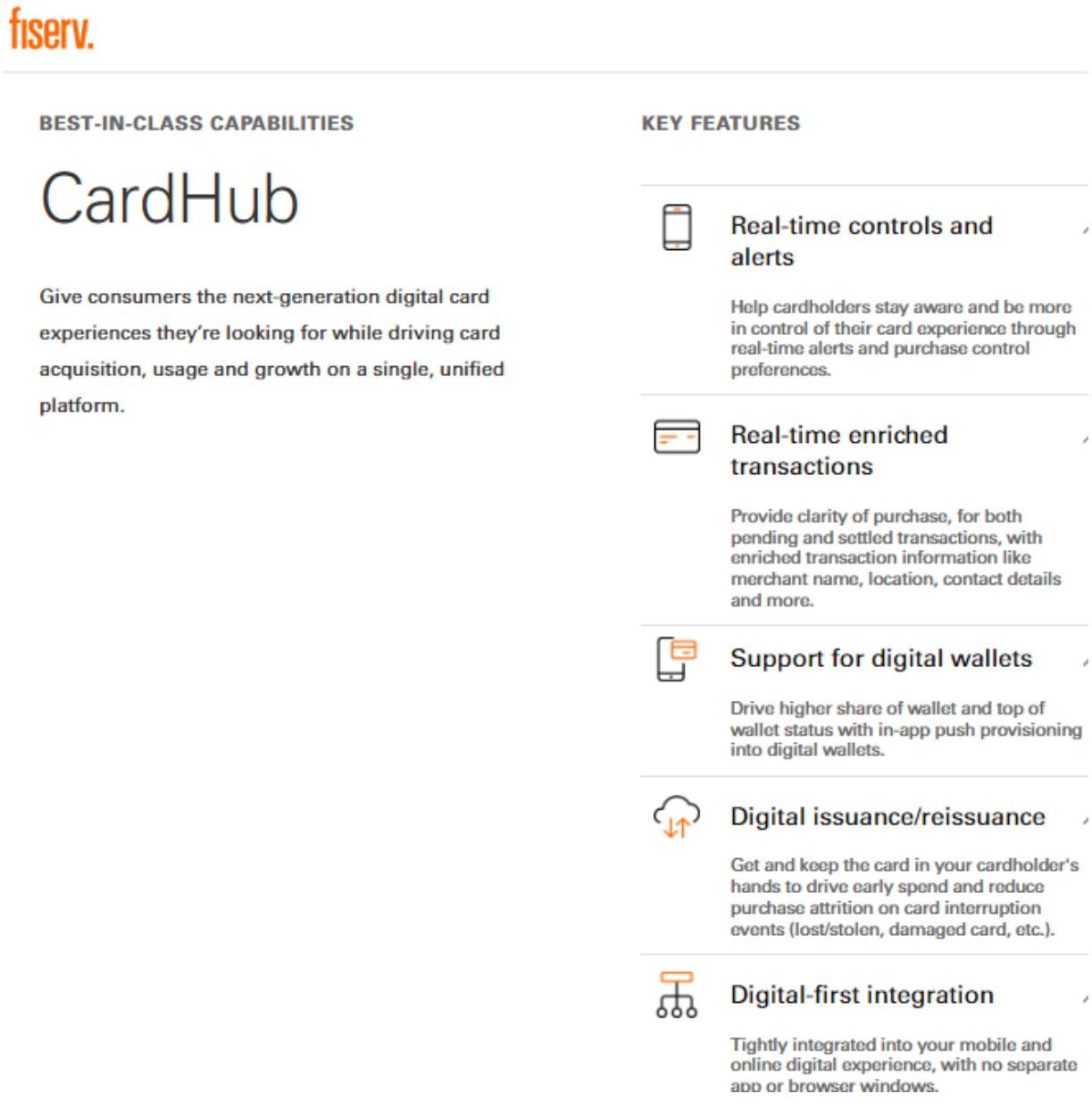
53. The Accused Instrumentalities of Defendants infringe one or more claims of the '985 patent, which provide methods and systems for authorizing payment transactions for customers with more than one transaction instrument representing a single transaction account. In the '985 patent, customer-level transaction data may be determined to be common to more than one instrument, and such data may be analyzed in order to authorize a payment transaction. Data

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

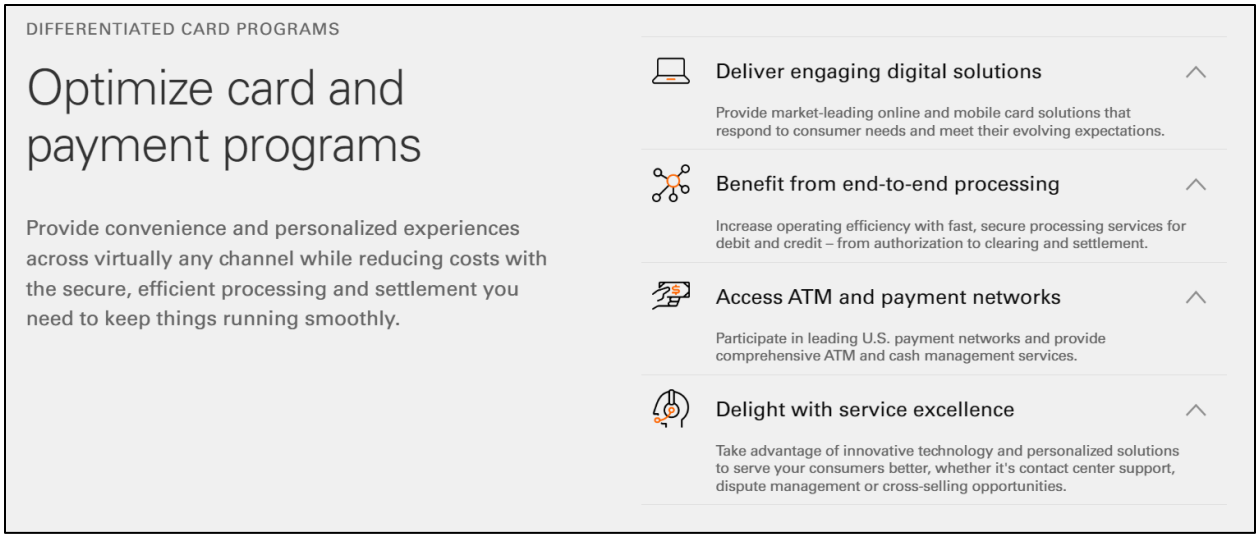
54. Defendants infringe the '985 patent via Defendants' set of card issuance solutions for banks and financial institutions, including without limitation processing and support for mobile wallets, and EMV-compliant payment applications used in conjunction with mobile wallets, including Google Pay and Samsung Pay and/or via direction and control of third parties in connection with these payment applications. As an example, Fiserv provides a complete set of card issuance solutions for banks and financial institutions as illustrated in screenshots from Fiserv's website as shown below.



See Credit Solutions, FISERV, https://www.fiserv.com/en/solutions/card-services/credit-solutions.html (last visited Oct. 13, 2023).

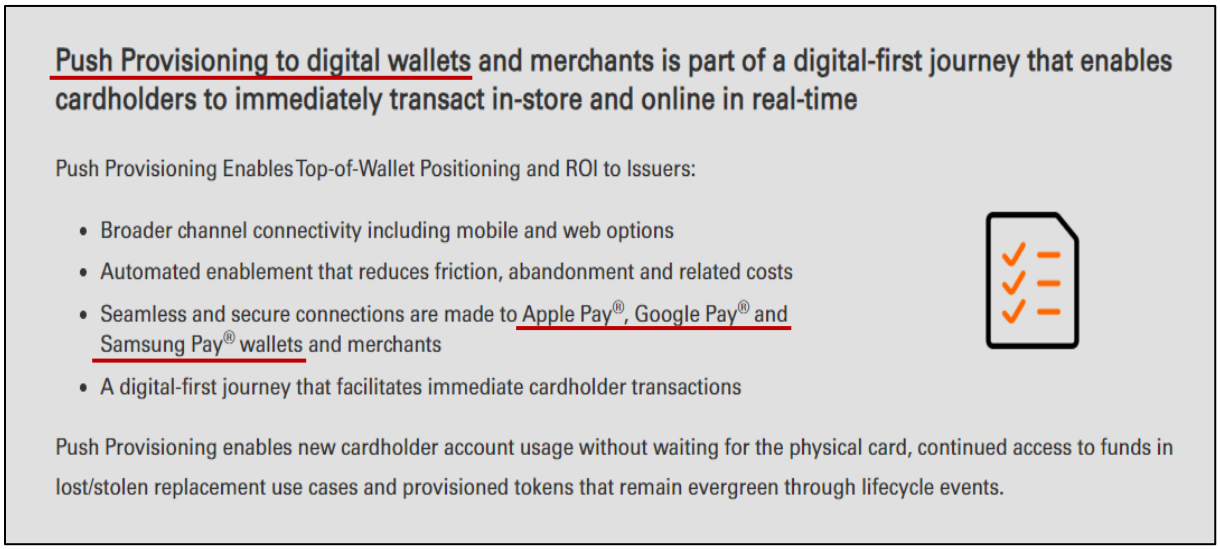


See CardHub, FISERV, https://www.fiserv.com/en/solutions/card-services/cardhub.html (last visited Oct. 13, 2023).

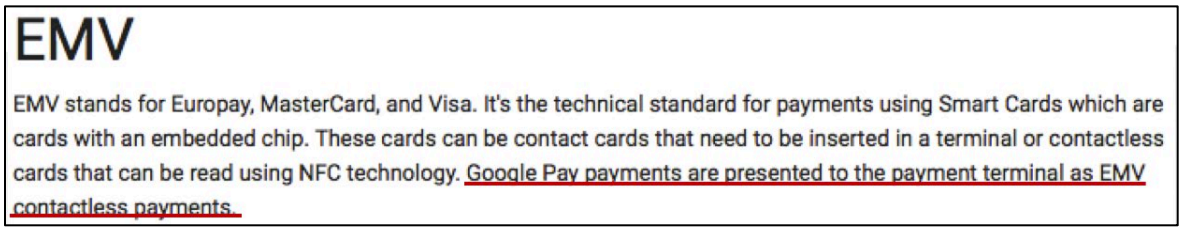


Optimize card and payment programs, FISERV, https://www.fiserv.com/en/solutions/card-services.html (last visited Oct. 12, 2023) ("Benefit from end-to-end processing . . . from authorization to clearing and settlement).

55. Fiserv also provisions EMV compliant payment applications for consumers' cards onto mobile wallets, including Google Pay and Samsung Pay. In connection with transaction instruments and/or the mobile wallets that Fiserv provisions, at least one Fiserv computer system performs the steps of claim 1 of the '985 patent.



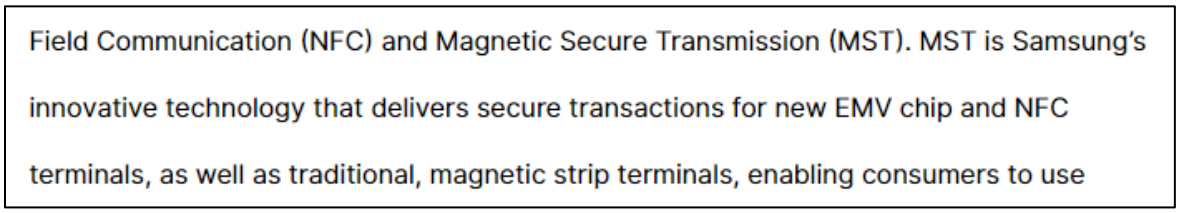
Real-Time Provisioning Drives Issuer Cards to Top of Wallet, FISERV, https://www.fiserv.com/en/solutions/payments/credit-and-debit-solutions/real-time-provisioning.html (last visited Oct. 12, 2023) (describing "Push Provisioning from Fiserv" that "drives tokens from the issuer to destination wallets and merchants").



EMV

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

Google Pay Merchant Help: EMV, GOOGLE, https://support.google.com/pay/merchants/answer/7151369?hl=en (last visited Oct. 12, 2023).



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

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

56. As required by mobile wallets, Fiserv offers tokenization to all its card issuer customers.

Fiserv Financial Institution Clients Can Keep their Cards at the Top of the Mobile Wallet with New Tokenization Capabilities

September 10, 2014 PDF Version

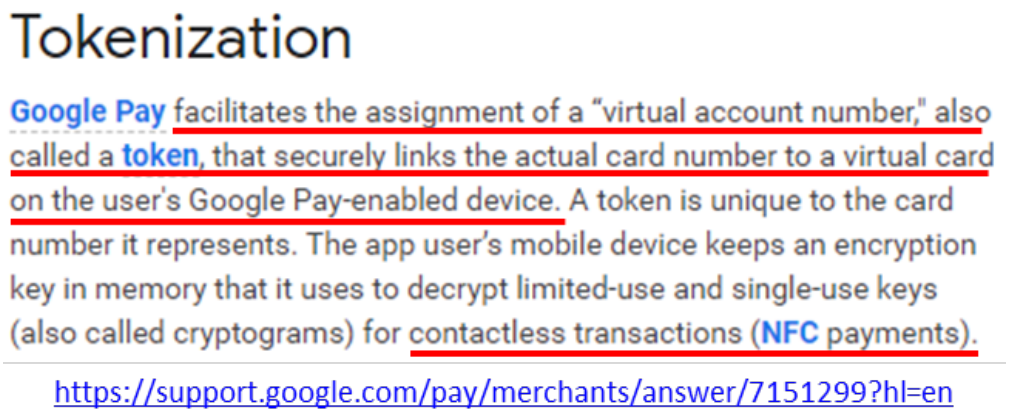
- Fiserv will offer tokenization via Visa Token Service (VTS) and MasterCard Digital Enablement Service (MDES) and will support tokenization through its own Accel network
- Tokenization enhances security for a variety of mobile and online payment types
- Tokenization capabilities are required for cards to be used through the newly announced Apple Pay service

BROOKFIELD, Wis.--(BUSINESS WIRE)-- Fiserv, Inc. (NASDAQ: FISV), a leading global provider of financial services technology solutions, announced today that it has expanded its mobile payments solution portfolio to include tokenization capabilities via Visa Token Service (VTS) and MasterCard Digital Enablement Service (MDES). These capabilities will be available to all Fiserv-processed debit and credit issuers. Fiserv will also enable its Accel™ debit payments network to support tokenization for its participants.

By supporting tokenization capabilities, Fiserv ensures that its financial institution clients can play an integral role in the mobile payments ecosystem. For example, tokenization capabilities are required for cards to be used through the newly announced Apple Pay™ service, which will enable mobile payments at a variety of physical and online merchants and service providers.

Fiserv Financial Institution Clients Can Keep their Cards at the Top of the Mobile Wallet with New Tokenization Capabilities, FISERV, https://newsroom.fiserv.com/news-releases/news-release-details/fiserv-financial-institution-clients-can-keep-their-cards-top (Sep. 10, 2014) (last visited Oct. 16, 2023).

57. 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 Fiserv Transaction Instruments (e.g., Mastercard Cards). Transactions associated with Fiserv Transaction Instruments made online by consumers may also utilize virtual account numbers via "tokenization," as shown below in relation to Google Pay.

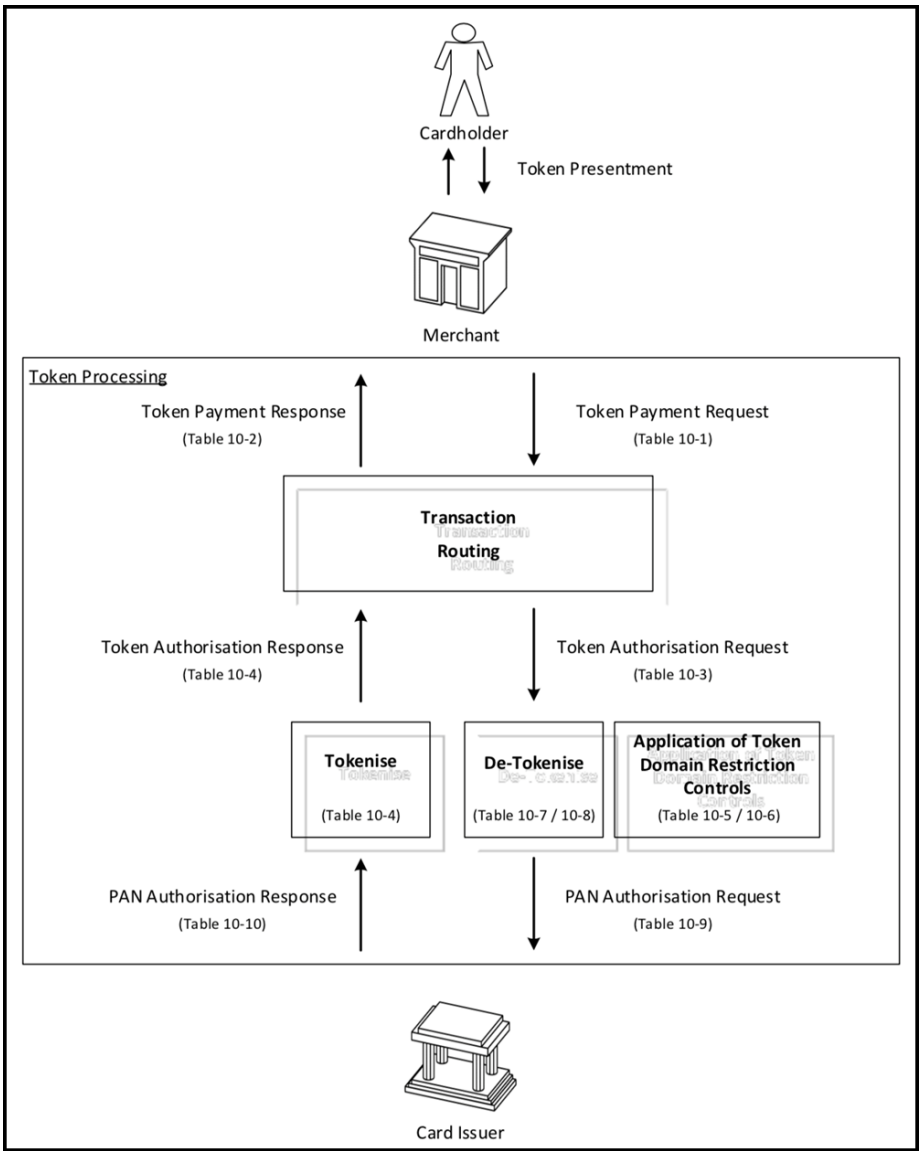


Tokenization

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

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

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



Token Payment Request: includes the request that originates from the point of interaction with the Merchant (such 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

59. 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.

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

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

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

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

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

8.1.2 Application Cryptogram Algorithm

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

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

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

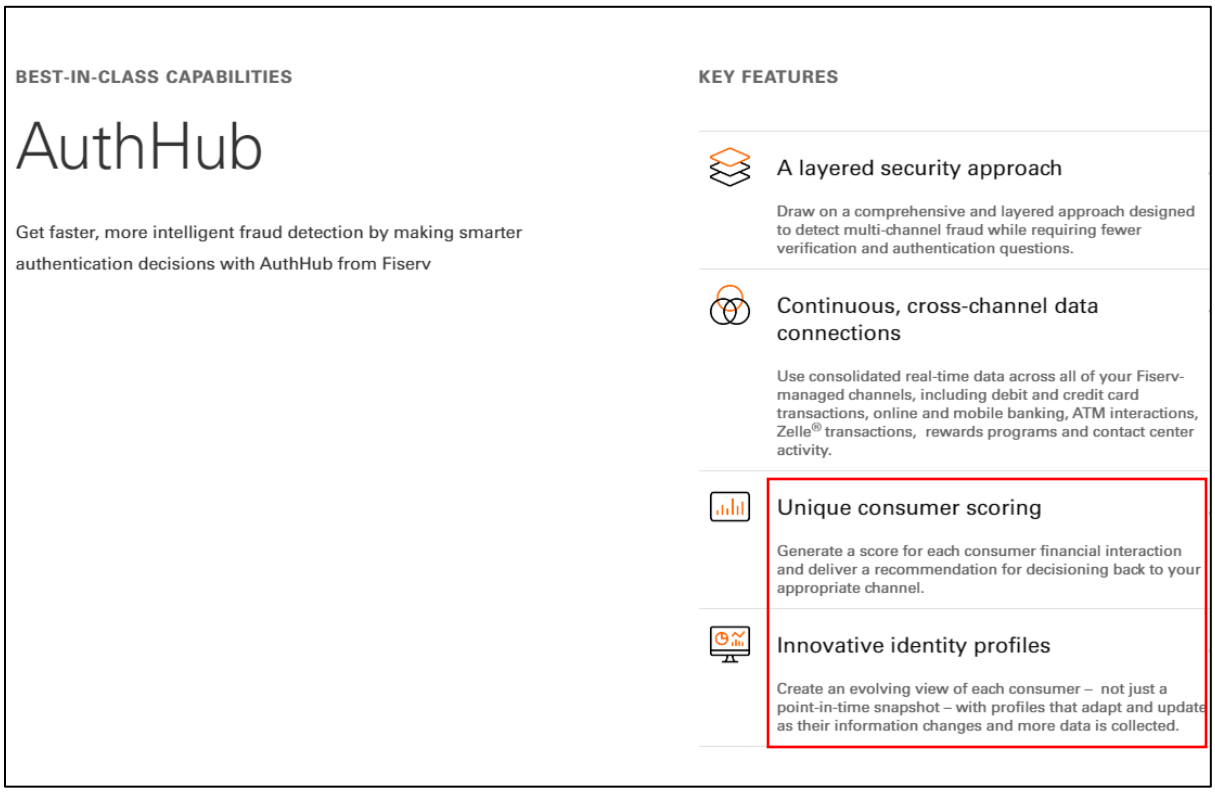
EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3, November 2011

61. 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

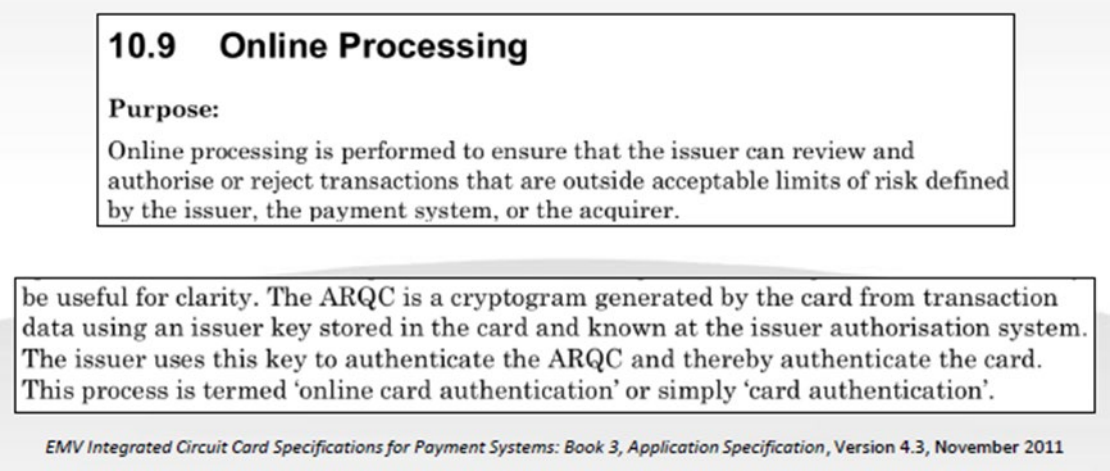
62. As an additional example of part of the analyzing conducted by Fiserv, Fiserv compares the transaction data to past transaction history for the underlying account (second transaction instrument) to identify fraudulent transactions.



See AuthHub, FISERV, https://www.fiserv.com/en/solutions/card-services/authhub.html (last visited Oct. 16, 2023).

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

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



10.9 Online Processing

Purpose:

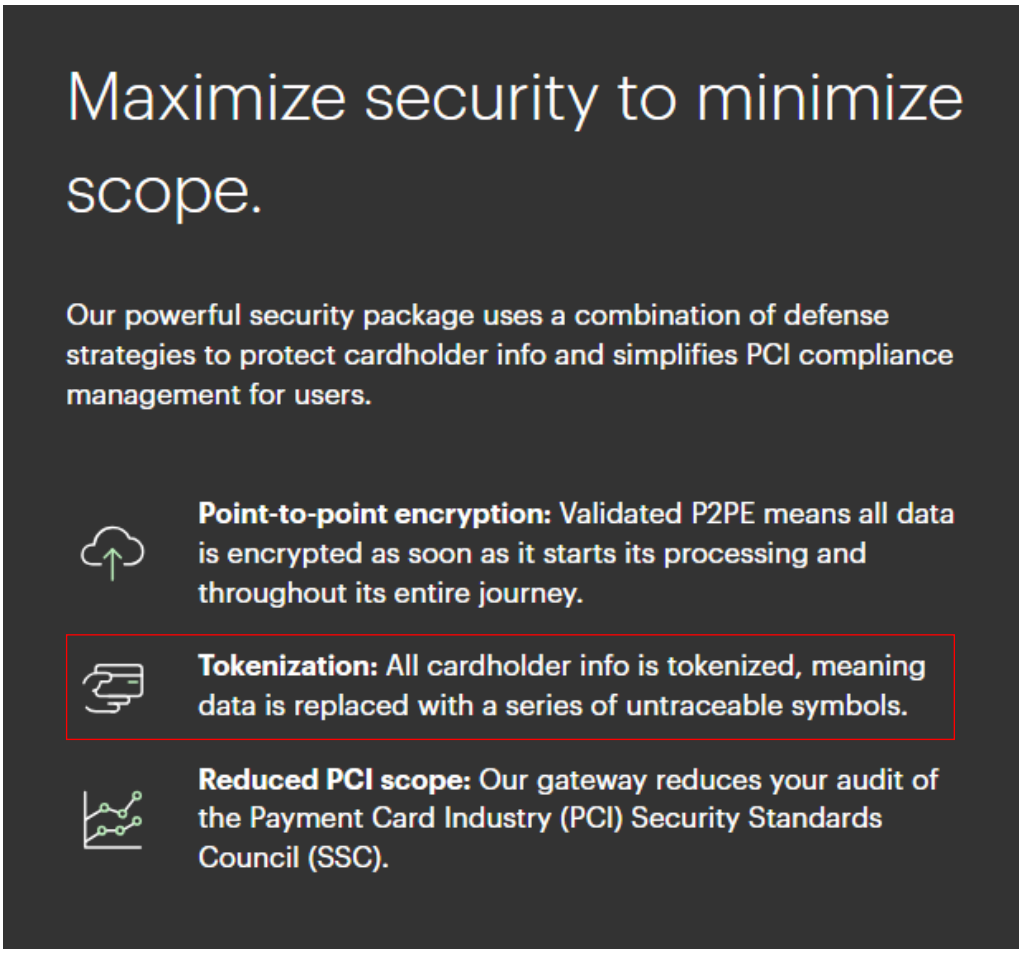
Online processing is performed to ensure that the issuer can review and authorise or reject transactions that are outside acceptable limits of risk defined by the issuer, the payment system, or the acquirer.

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

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

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

64. As a further example of how Defendants infringe the '985 patent, Fiserv, at least through one or more of its Clover subsidiaries and/or brands, allows merchants to use and store a token in place of customer credit card information. Accordingly, at least some of the card numbers stored by Fiserv's customers (merchants) are tokens, rather than actual card numbers.



Plug into a secure payment gateway, CLOVER CONNECT, https://integrate.clover.com/ecommerce/ (last visited Oct. 17, 2023) (emphasis added).

What Is tokenization?

Simply put — tokenization is a fraud-prevention measure designed to protect sensitive payment credentials, such as:

- Credit card numbers
- Cardholder names
- Expiration dates
- CVV codes
- Bank account numbers

Tokenization accomplishes this by substituting all of a user's payment details with non-specific IDs known as "tokens." Each of these tokens is randomly generated when a customer supplies his or her payment information at the point of sale (POS). By design, there is no clear relationship between the user's payment details and the resulting tokens.

https://blog.clover.com/how-does-tokenization-work/ (emphasis added)

The first step in the Ecommerce API flow is encrypting a customer card as a `source` token. Apps using an `iframe` and `API integration` receive and send `source` tokens that represent encrypted customer card data. See Using the Clover-hosted iframe and iFrame and API Integration.

Clover uses this token to process secure payments. Complete an Ecommerce API flow by using the `source` token, along with an OAuth token.

https://docs.clover.com/docs/ecommerce-generating-a-card-token (emphasis added)

65. Fiserv allows merchants to use Card-on-File (COF) transactions in which a multi-pay card token (a tokenized card number—that is, a first transaction instrument) associated with a user can be used as the source value in a payment request (i.e., an authorization request).

What is card-on-file (COF)?

Card-on-file (COF) transactions are payments in which the cardholders have authorized merchants to store their credit or debit card information to use for future purchases or recurring payments. You can use sandbox test cards to build and test the COF feature. A COF payment

Make subsequent payments with saved cards

To make a payment and then subsequent payments with a saved customer card, you can use either the customer `id` or the multi-pay card token as the `source` value in your payment request.

Save a card for future transactions, CLOVER, https://docs.clover.com/docs/ecommerce-saving-card (last visited Oct. 17, 2023) (emphasis added).

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

Only the merchant's payment gateway can match this token against the customer's original credit card number. It is unreadable by anyone else (including the merchant). Even if a token is intercepted mid-transit across an unsecured network, criminals cannot reverse-engineer the customer's payment information. The token is useless to them and cannot be used to make purchases.

Anatomy of a tokenized credit card transaction

- When a customer provides his or her payment details (either at a POS terminal or through an online checkout form), each data point is substituted with a randomly generated token.
- In most cases, the merchant's payment gateway is responsible for creating these random IDs.
- Next, the tokenized information is encrypted before being sent across the networks to the merchant's payment processor. The original credit card information is securely stored in the payment gateway's "token" vault. It is the ***only*** component that can map this token back to the underlying payment data.
- The merchant's provider encrypts the information again before sending these payment details across the card or ACH networks for verification.
- If authorization goes through, confirmation of the sale is sent across the card or ACH networks to all relevant parties – including the payment processor, payment gateway, merchant, and the customer.

How does tokenization work, CLOVER, https://blog.clover.com/how-does-tokenization-work/ (last visited Oct. 17, 2023) (emphasis added).

67. Fiserv analyzes the transaction data by checking some of the submitted data against the issuer's cardholder information.

Overview

When you create a card token or charge a customer's card, Clover checks some of the submitted data against the issuer's cardholder information to verify the card is being used legitimately. These checks include three possible values that correspond to fields in the response:

- The CVC/CVV provided by the customer - `cvc_check`
- The first line of the customer's address - `address_line1_check`
- The postal code provided by the customer - `address_zip_check`

The CVC and address information is not checked when the card is tokenized. For the fraud checks to occur, your app must use the token as the `source` for a charge or order payment request. If you examine the response in either case, you will see the fraud check fields in the `source` object.

Confirm customer information with fraud tools, CLOVER, https://docs.clover.com/docs/confirming-customer-information-with-ecommerce-fraud-tools (last visited Oct. 17, 2023) (emphasis added).

68. Based on checking some of the submitted data against the issuer's cardholder information, a response indicating if the transaction has been authorized or declined. For example, a response will include a cvc_check that either passed or failed depending on the entered PIN number.

Anatomy of a tokenized credit card transaction

- When a customer provides his or her payment details (either at a POS terminal or through an online checkout form), each data point is substituted with a randomly generated token.
- In most cases, the merchant's payment gateway is responsible for creating these random IDs.
- Next, the tokenized information is encrypted before being sent across the networks to the merchant's payment processor. The original credit card information is securely stored in the payment gateway's "token" vault. It is the ***only*** component that can map this token back to the underlying payment data.
- The merchant's provider encrypts the information again before sending these payment details across the card or ACH networks for verification.
- If authorization goes through, confirmation of the sale is sent across the card or ACH networks to all relevant parties – including the payment processor, payment gateway, merchant, and the customer.

How does tokenization work, CLOVER, https://blog.clover.com/how-does-tokenization-work/ (last visited Oct. 17, 2023) (emphasis added).

Recommendations for CVC checks

If the customer's PIN does not match the PIN stored with the issue, the response includes `"cvc_check": "failed". Your app should automatically refund the payment in this case using the Create a refund or Return an order endpoint.


```
{
  "id": "KYZ5X18N6ZX7P",
  "amount": 563,
  "paid": true,
  "status": "succeeded",
  "source": {
    "id": "clv_1TSTSC9WX8G52NFGikM9YWuW",
    "address_city": "Colorado Springs",
    "address_country": "US",
    "address_line1": "2424 Garden of the Gods Rd",
    "address_line1_check": "pass",
    "address_line2": "Ste 1400",
    "address_state": "CO",
    "address_zip": "80919",
    "address_zip_check": "pass",
    "brand": "DISCOVER",
    "cvc_check": "pass",
    "exp_month": "12",
    "exp_year": "2021",
    "first6": "601136",
    "last4": "6668"
  }
}
```

Confirm customer information with fraud tools, CLOVER, https://docs.clover.com/docs/confirming-customer-information-with-ecommerce-fraud-tools (last visited Oct. 17, 2023) (emphasis added).

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

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

Clover accepts all major types of payments

Although some contactless payment companies lock you into their technology, Clover POS systems accept all of the most popular types of traditional and contactless payments.

Clover devices accept numerous methods of payment, including:

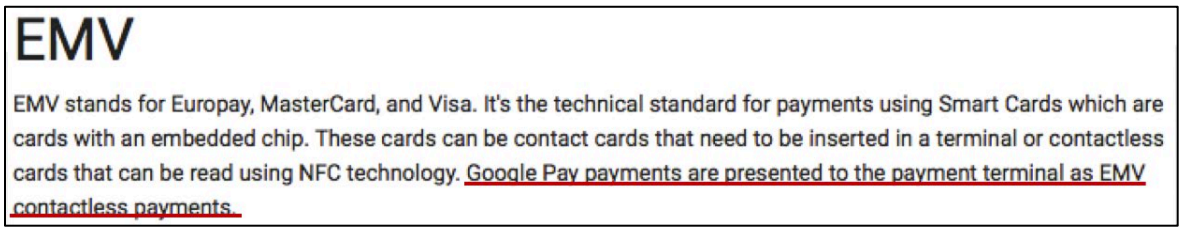
- Cash
- Checks
- Credit cards
- Debit cards
- Prepaid cards
- Gift cards
- EBT cards
- Custom tenders
- Alipay®

Credit and debit cards are the most popular payment methods. Many cards are already contactless-enabled and many more are being issued with contactless payments capabilities so that they can be simply waved over a Clover device for payment. In addition, almost all cards can be added to a mobile wallet, including:

- Apple Pay®
- Google Pay™
- Samsung Pay®

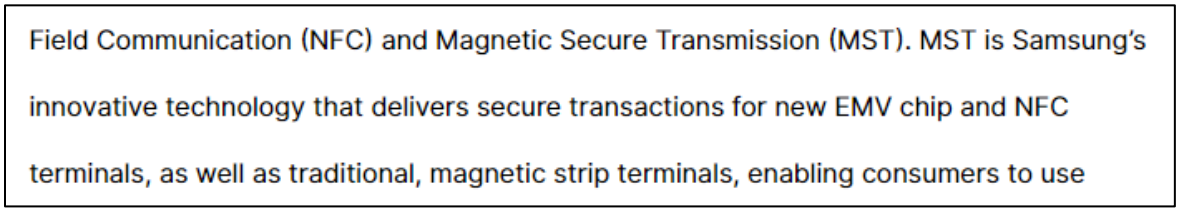
Contactless Payments, CLOVER, https://www.clover.com/small-business-resources/contactless-payments (last visited Oct. 17, 2023).

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


EMV

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

Google Pay Merchant Help: EMV, GOOGLE, https://support.google.com/pay/merchants/answer/7151369?hl=en (last visited Oct. 12, 2023) (emphasis added).


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

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

72. Examples of Fiserv's EMV compliant POS systems and devices include the following Clover systems and devices:

Handheld card reader to take payments wherever you do business

$49

SHOP GO

Peak performance at your fingertips on a large 14" touchscreen

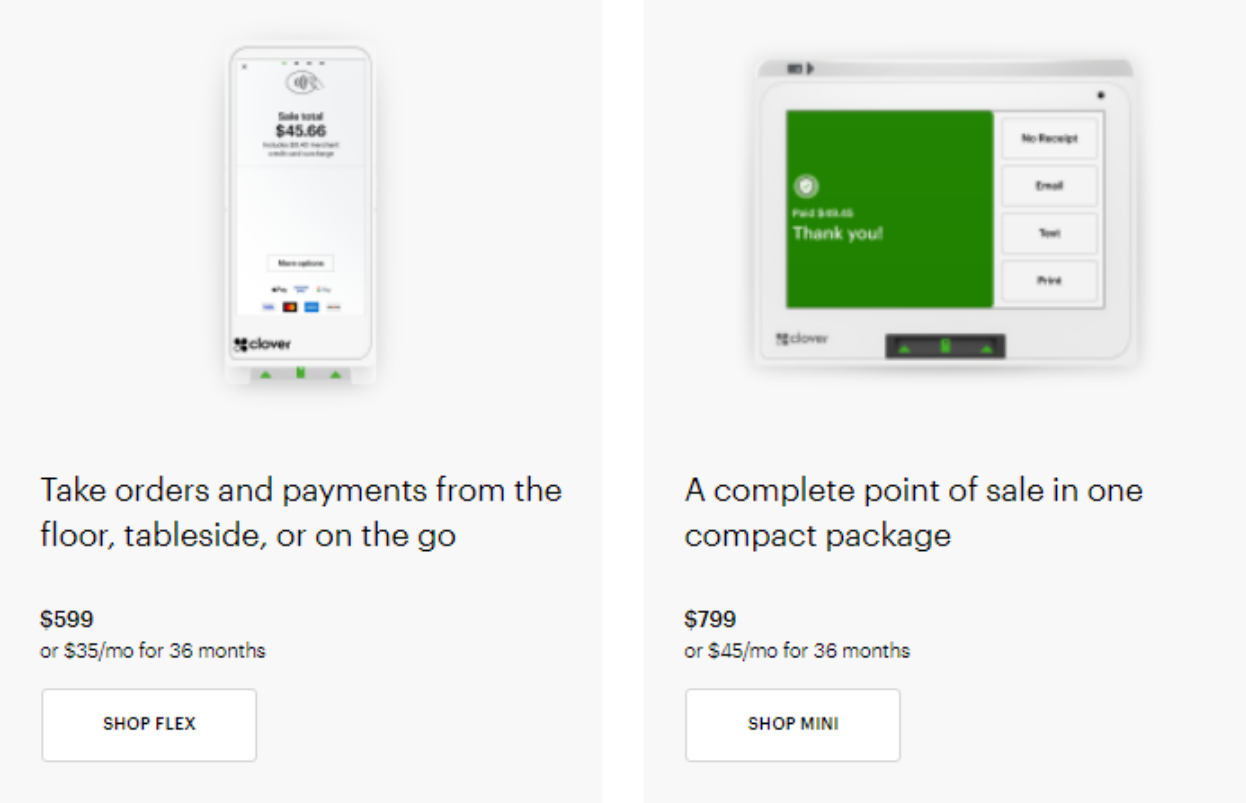
$1,699
or $125/mo for 36 months

SHOP STATION SOLO

A powerful point of sale for both sides of the counter

$1,799
or $135/mo for 36 months

SHOP STATION DUO



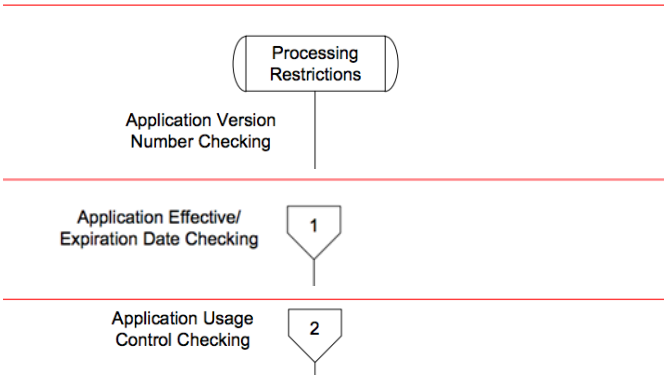
Flexible POS systems tailored to your business, CLOVER, https://www.clover.com/shop (last visited Oct. 17, 2023).

73. Fiserv's Clover EMV-compliant merchant systems and devices (e.g., payment terminals) determine a first action analysis result based at least in part on one of an Offline Data Authentication, a risk management factor and a process restriction analysis. For example, this occurs as part of an EMV mode transaction after a "GET PROCESSING OPTIONS" command, as exemplified by Kernel 2 applicable to MasterCard.

3.4.3 EMV Mode

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

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



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

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

74. As explained below, the EMV-compliant merchant systems and devices request an application cryptogram from a transaction device (e.g., using the GENERATE AC Command),

which may be for approving/denying the transaction, or for online approval, as exemplified by Kernel 2 applicable to Mastercard.

3.4.3 EMV Mode

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

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

5.4 Generate AC

5.4.1 Definition and Scope

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

Table 5.10—Generate AC Reference Control Parameter

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

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

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

76. The transaction device, at the direction of the terminal, transmits the card action analysis result, as exemplified by Kernel 2 applicable to Mastercard.

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

A.1.117 Outcome Parameter Set

Tag: 'DF8129'

Template: —

Length: 8

Format: b

Update: K

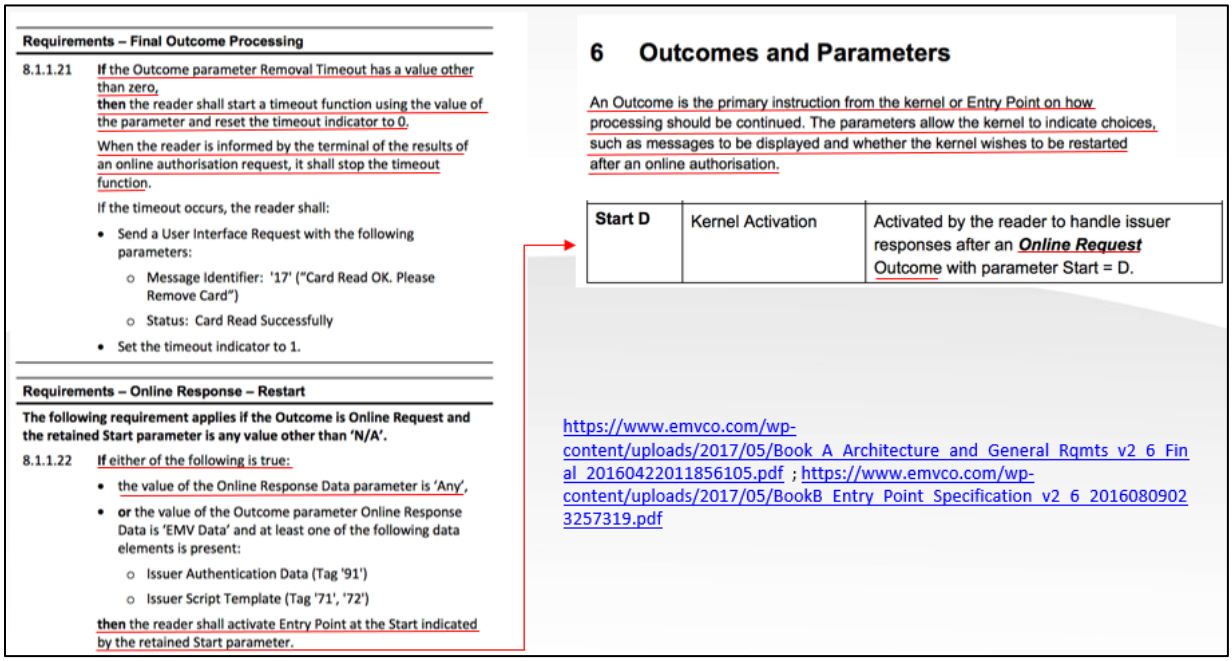
Description: This data object is used to indicate to the Terminal the outcome of the transaction processing by the Kernel. Its value is an accumulation of results about applicable parts of the transaction.

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

Online authorization and transaction logging	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. The authorization request and clearing record include different data depending on whether the transaction was completed in mag-stripe mode or EMV mode.

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

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



Requirements – Final Outcome Processing

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

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

If the timeout occurs, the reader shall:

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

Requirements – Online Response – Restart

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

8.1.1.22 If either of the following is true:

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

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

6 Outcomes and Parameters

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

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

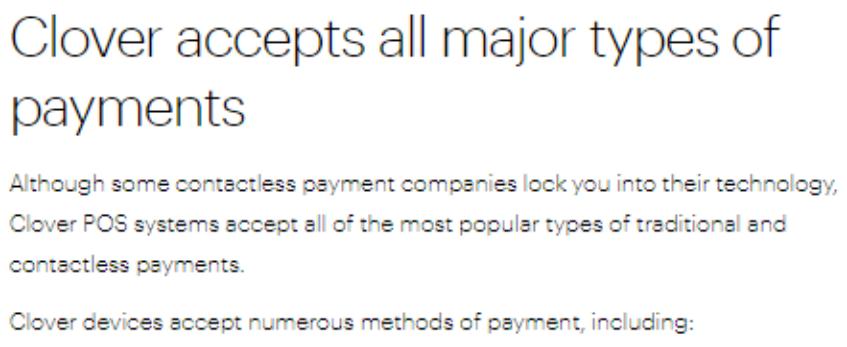
https://www.emvco.com/wp-content/uploads/2017/05/Book_A_Architecture_and_General_Rqmts_v2_6_Final_20160422011856105.pdf ; https://www.emvco.com/wp-content/uploads/2017/05/BookB_Entry_Point_Specification_v2_6_20160809023257319.pdf

Outcome	Description	Kernel	Entry Point	Reader/ Terminal
Approved	The kernel is satisfied that the transaction is acceptable with the selected contactless card application and wants the transaction to be approved. This is the expected Outcome for a successful offline transaction. This might also occur following reactivation of a kernel after an online response.	Creates Outcome, passes to Entry Point	• Processes selected Outcome parameters • Passes Outcome to reader as a Final Outcome	Processes the Final Outcome
Declined	The kernel has found that the transaction is not acceptable with the selected contactless card application and wants the transaction to be declined. This might also occur following reactivation of a kernel after an online response.			
Online Request	The transaction requires an online authorisation to determine the approved or declined status. If the kernel wishes to be restarted when the response has been received (e.g. to receive issuer update data), then this is indicated in the parameters.			

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

79. 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.

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



Clover accepts all major types of payments

Although some contactless payment companies lock you into their technology, Clover POS systems accept all of the most popular types of traditional and contactless payments.

Clover devices accept numerous methods of payment, including:

- Cash
- Checks
- Credit cards
- Debit cards
- Prepaid cards
- Gift cards
- EBT cards
- Custom tenders
- Alipay®

Credit and debit cards are the most popular payment methods. Many cards are already contactless-enabled and many more are being issued with contactless payments capabilities so that they can be simply waved over a Clover device for payment. In addition, almost all cards can be added to a mobile wallet, including:

- Apple Pay®
- Google Pay™
- Samsung Pay®

Contactless Payments, CLOVER, https://www.clover.com/small-business-resources/contactless-payments (last visited Oct. 17, 2023) (emphasis added).

EMV

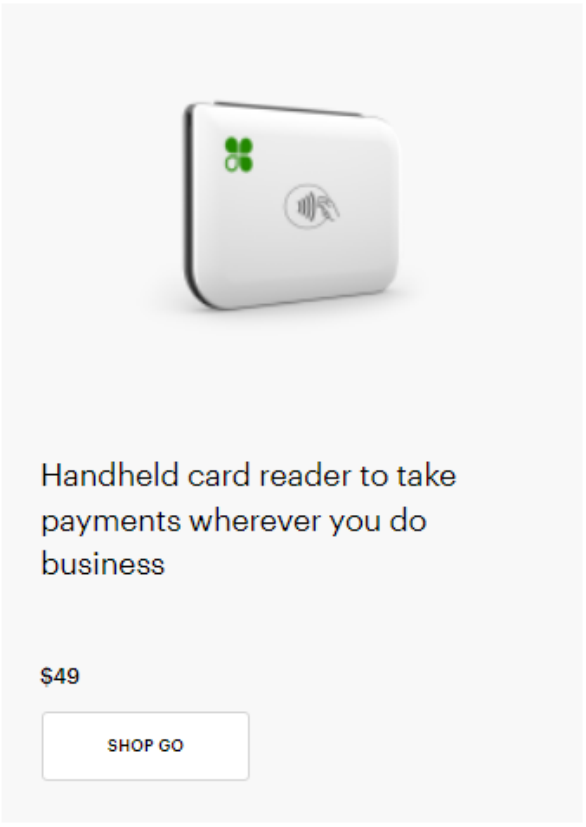
EMV stands for Europay, MasterCard, and Visa. It's the technical standard for payments using Smart Cards which are cards with an embedded chip. These cards can be contact cards that need to be inserted in a terminal or contactless cards that can be read using NFC technology. Google Pay payments are presented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

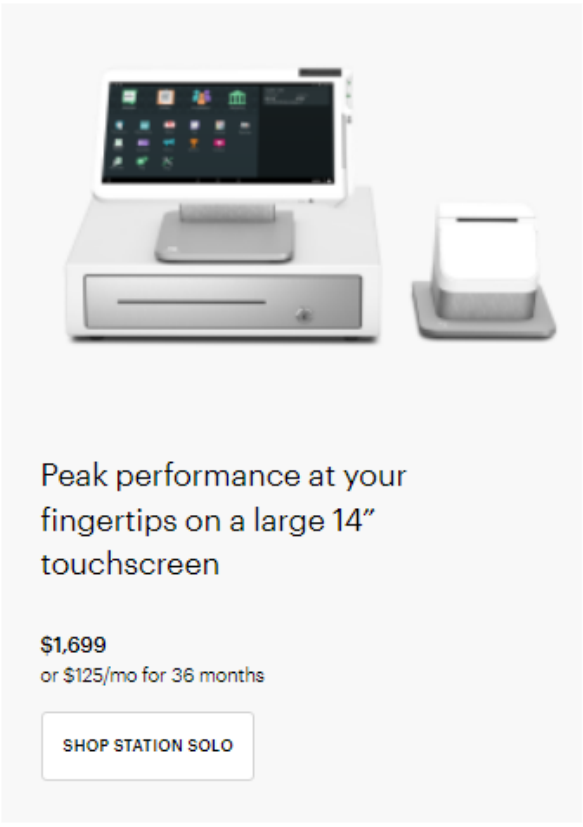
Google Pay Merchant Help: EMV, GOOGLE, https://support.google.com/pay/merchants/answer/7151369?hl=en (last visited Oct. 12, 2023) (emphasis added).

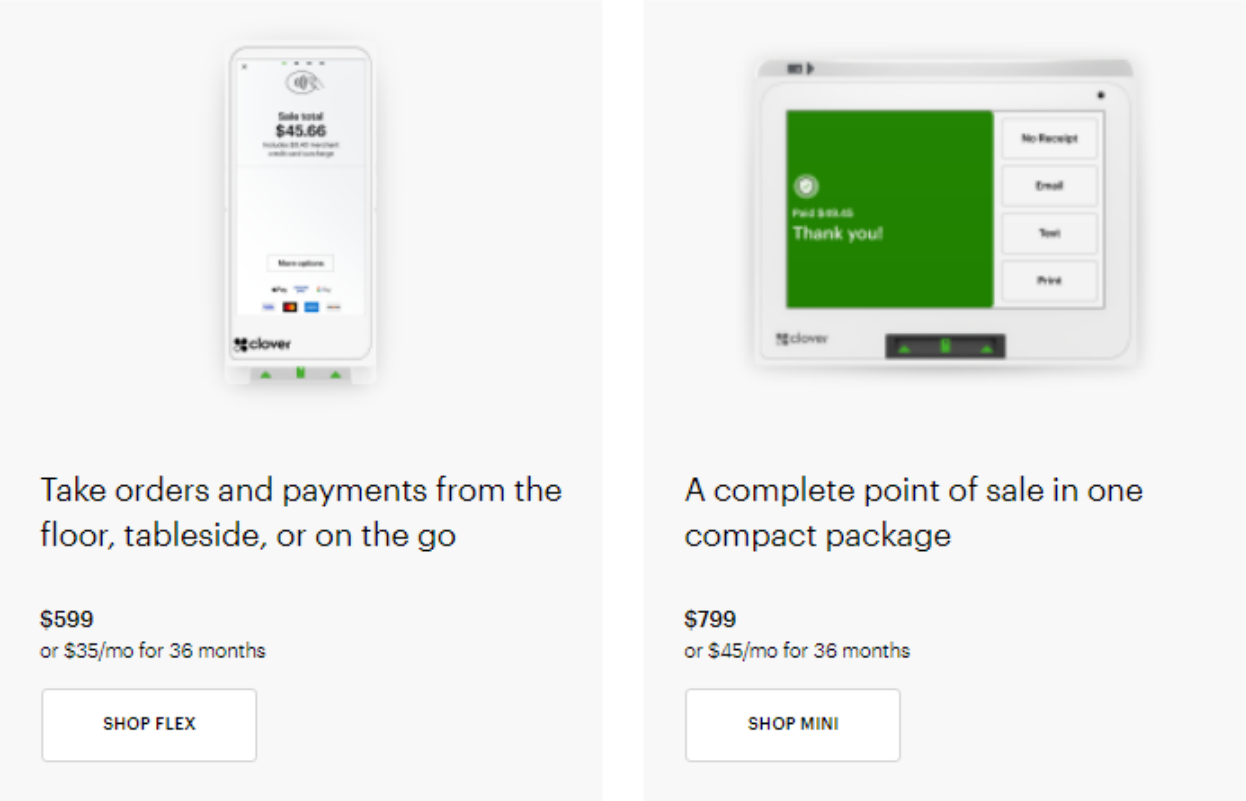
Field Communication (NFC) and Magnetic Secure Transmission (MST). MST is Samsung's innovative technology that delivers secure transactions for new EMV chip and NFC terminals, as well as traditional, magnetic strip terminals, enabling consumers to use

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

81. Examples of Fiserv's EMV compliant POS systems and devices include the following Clover systems and devices:







Flexible POS systems tailored to your business, CLOVER, https://www.clover.com/shop (last visited Oct. 17, 2023).

82. Fiserv's Clover EMV readers receive a financial transaction request comprising an Application Cryptogram for an online authorization (ARQC) and the Primary Account Number (PAN). This is exemplified by Kernel 2 applicable to Mastercard.

83. 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.

84. The point-of-sale terminal (e.g., Clover reader) transmits the Application Cryptogram for online authorization (ARQC) and the Primary Account Number (PAN) to the issuer. This is exemplified by Kernel 2 applicable to Mastercard.

85. The point-of-sale terminal (e.g., Clover reader) receives a response to the transaction request from the issuer. The response may indicate that the issuer has declined the transaction due to thresholds of the LUK being exceeded, e.g., number of transactions indicated by ATC being more than 1 for Mastercard or more than 15 for another brand card.

limited-use key

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

limited-use key, GOOGLE, https://support.google.com/pay/merchants/answer/7151225?hl=en (last visited Oct. 18, 2023) (emphasis added)

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

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

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

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

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

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

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

Madhu Vasu, Senior Director, Innovation and Strategic Partnerships, Visa Inc, available at: https://www.kansascityfed.org/~/media/files/publicat/pscp/2015/sessions/2015-psr-conf-session4-paneldiscussion.pdf?la=en (emphasis added)

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

First Final Outcome	POS System Processing

Online Request	• The POS System advises the cardholder that an online transaction is in progress. An initial message to the cardholder might have been displayed as a result of the kernel including a User Interface Request with the Outcome. If a PIN CVM is required, then the message directs the cardholder to enter the PIN.
	• The terminal initiates an online authorisation request, using the data record provided with the Outcome. If the CVM is online PIN, then the terminal processes and submits the encrypted online PIN.
	• The terminal receives the online response or might determine that the request was unable to go online.
	• If the Start parameter was any value other than 'N/A', then:
	  • The terminal makes available the transaction disposition in the online response together with all of the EMV TLV data elements present.
	  • The reader reactivates Entry Point by continuing with 'Requirements – Online Response – Restart' on page 69.
	• The terminal determines the transaction disposition, based on the online response indication (with Unable To Go Online a decline).
	• The terminal advises the cardholder of the transaction outcome.
	• If a cardholder receipt is required, the terminal prints it or provides it electronically (e.g. email).
	• The terminal captures CVM signature or online PIN if requested.
	• The terminal prepares a clearing record if transaction disposition is "approved".
	• Once complete, continue with 'Requirements – New Transaction Preparation and Start' on page 64.

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

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

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

87. 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

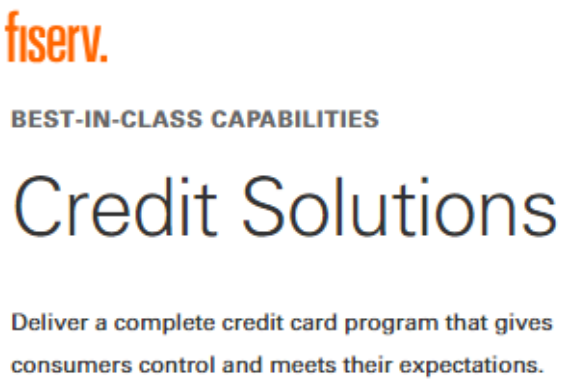
transaction instrument at the time of sale of goods or services and then would request authorization at a later time, including after the customer or merchant had already left the point of sale. Merchants were also required to pay "card not present" fees, because of the higher risks associated with such transactions, which included fraudulent use of the customer's account number.

88. 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.

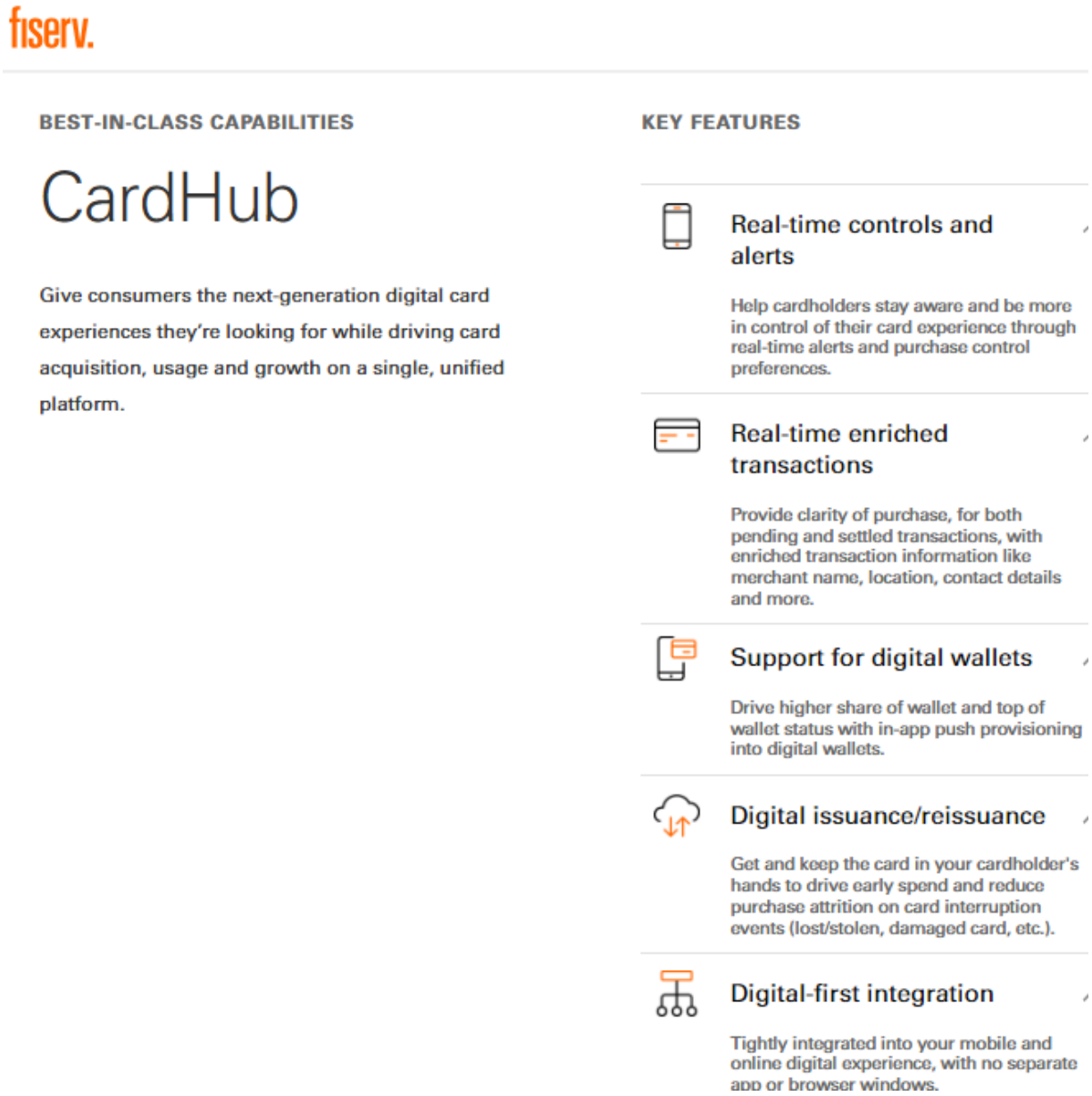
89. The Accused Instrumentalities of Defendants infringe one or more claims of the '509 patent, which provide technological solutions and improvements for facilitating payment transactions. Conventional methods for payment transactions, particularly RFID transactions, had problems supporting multiple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

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

90. Defendants infringe one or more claims of each of the '039 patent and '509 patent by providing services and/or their computer-based systems (e.g., Fiserv contactless EMV cards, Fiserv's payment network, including without limitation products, methods, and/or services offered under various subsidiary and brand names) for transaction processing associated with Fiserv Transaction Instruments (e.g., Mastercard Cards), including, for example, via transactions conducted using an EMV payment application issued to a user and stored in a mobile wallet. Defendants also infringe one or more claims of each of the '039 patent and '509 patent via Defendants' action on behalf of and/or direction and control of third parties in connection with their activities including processing transactions associated with Fiserv Transaction Instruments (e.g., Mastercard Cards) using Fiserv's computer-based systems. Fiserv's services and computer-based systems include, without limitation, those advertised on Fiserv's website. As an example, Fiserv provides a complete set of card issuance solutions for banks and financial institutions as illustrated in screenshots from Fiserv's website as shown below.



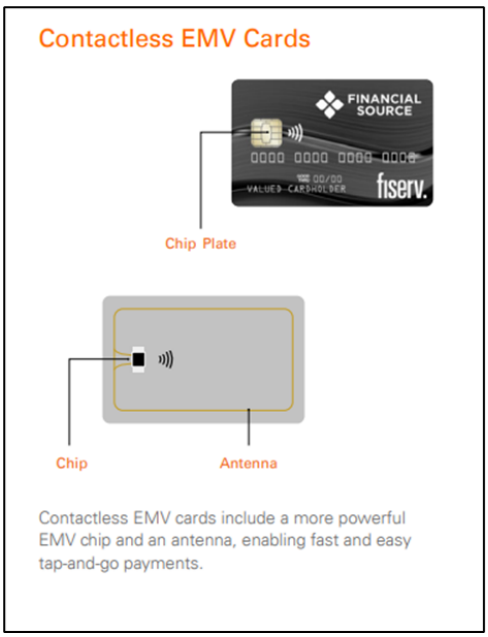
See Credit Solutions, FISERV, https://www.fiserv.com/en/solutions/card-services/credit-solutions.html (last visited Oct. 13, 2023).

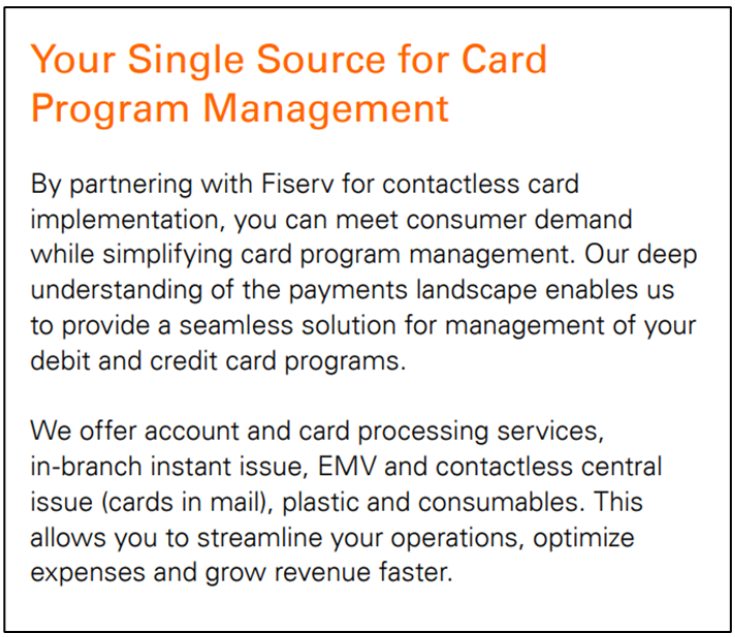


See CardHub, FISERV, https://www.fiserv.com/en/solutions/card-services/cardhub.html (last visited Oct. 13, 2023).

91. Fiserv also makes, sells, provides, issues and/or provisions EMV contactless cards (e.g., to and/or for financial institutions and/or in connection with mobile wallets). These EMV contactless cards comprise claimed systems and perform claimed methods of the '039 patent and

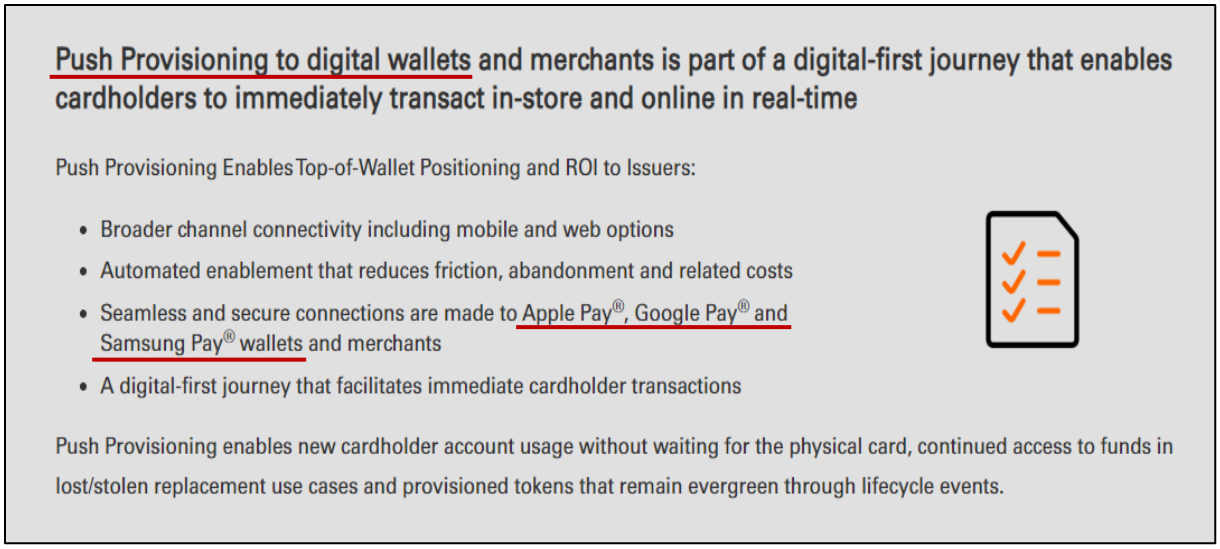
'509 patent. For example, the EMV contactless cards perform the steps of claim 1 of the '039 patent and claim 1 of the '509 patent.



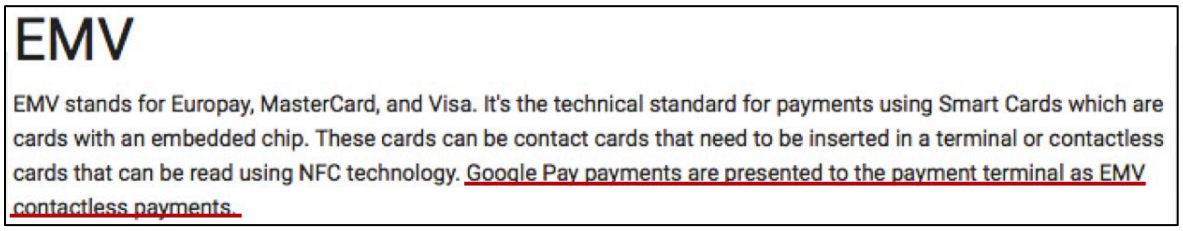


Solution: Contactless EMV® Cards, FISERV, https://www.fiserv.com/content/dam/fiserv-ent/final-files/marketing-collateral/sales-sheets/Contactless_EMV_Cards_Sales_Sheet_0221.pdf (last visited Oct. 13, 2023).

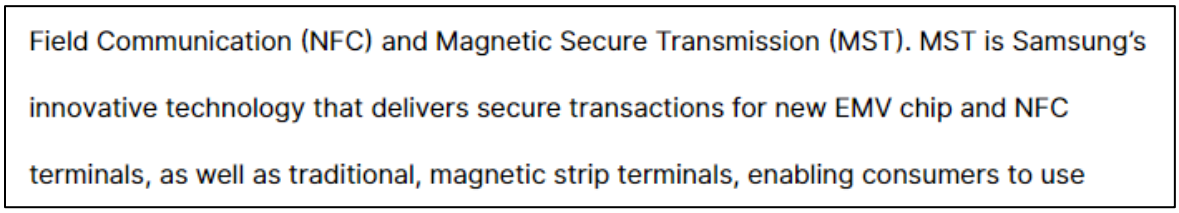
92. Fiserv also provisions EMV compliant payment applications for consumers' cards onto mobile wallets, including without limitation Google Pay and Samsung Pay. The mobile wallets perform the steps of claim 1 of the '039 patent and claim 1 of the '509 patent.



Real-Time Provisioning Drives Issuer Cards to Top of Wallet, FISERV, https://www.fiserv.com/en/solutions/payments/credit-and-debit-solutions/real-time-provisioning.html (last visited Oct. 12, 2023) (describing "Push Provisioning from Fiserv" that "drives tokens from the issuer to destination wallets and merchants").



Google Pay Merchant Help: EMV, GOOGLE, https://support.google.com/pay/merchants/answer/7151369?hl=en (last visited Oct. 12, 2023).



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

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

> The basic functions of the POS System include:
>
> - communication with contactless cards
> - application selection and kernel activation

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

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

COMPLETE LIST OF APPLICATION IDENTIFIERS (AID)

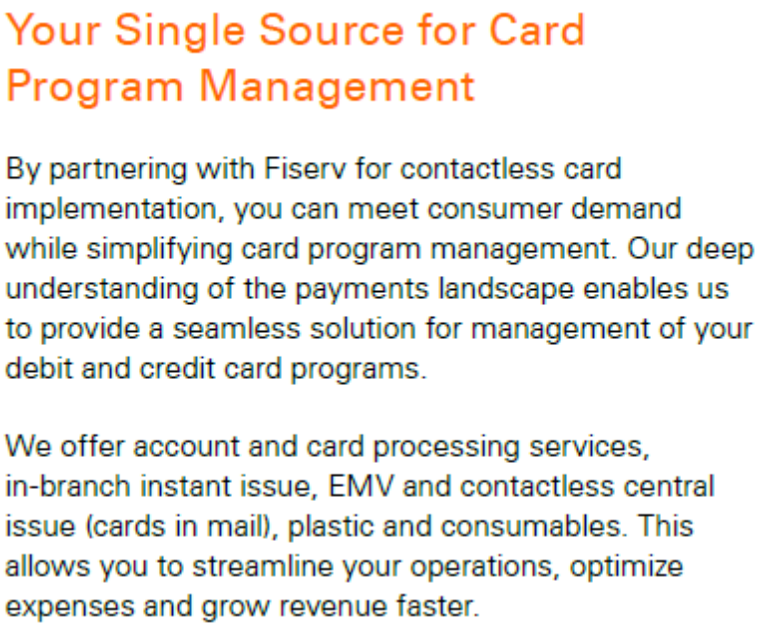
List of AID's with their description.

AID (Application Identifier)	Vendor	Country	Name	Description	Type
A00000000401	Mastercard International	United States	MasterCard PayPass	AEPM (Association Européenne Payez Mobile)	EMV
A0000000041010	Mastercard International	United States	MasterCard Credit/Debit (Global)	Standard MasterCard	EMV
A00000000410101213	Mastercard International	United States	MasterCard Credit	Standard MasterCard	EMV
A00000000410101215	Mastercard International	United States	MasterCard Credit	Standard MasterCard	EMV

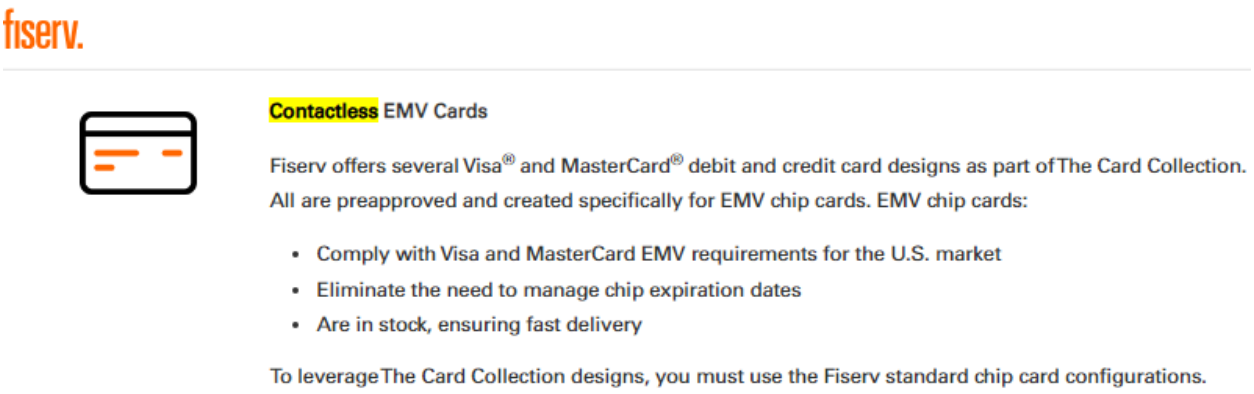
https://www.eftlab.com/knowledge-base/211-emv-aid-rid-pix/

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

Mastercard Cards) and to acquirers involved in transactions associated with Fiserv Transaction Instruments.



Solution: Contactless EMV® Cards, FISERV, https://www.fiserv.com/content/dam/fiserv-ent/final-files/marketing-collateral/sales-sheets/Contactless_EMV_Cards_Sales_Sheet_0221.pdf (last visited Oct. 13, 2023).



Card Designs Made Cost-Effective, Fiserv, https://www.fiserv.com/en/lp/the-card-collection-exclusive-designs.html (last visited Oct. 13, 2023).

96. Fiserv Transaction Instruments transmit a payment authorization request through the payment system for online processing, as exemplified by Kernel 2 applicable to Mastercard.

5.4 Generate AC

5.4.1 Definition and Scope

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

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

97. Fiserv Transaction Instruments receive authorization through the candidate payment system.

5.5.6 Transaction Disposition

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

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

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

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

98. Fiserv Transaction Instruments send the authorization (Transaction Certificate) to the POS terminal, as exemplified by Kernel 2 applicable to MasterCard.

5.4 Generate AC

5.4.1 Definition and Scope

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

Table 5.10—Generate AC Reference Control Parameter

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

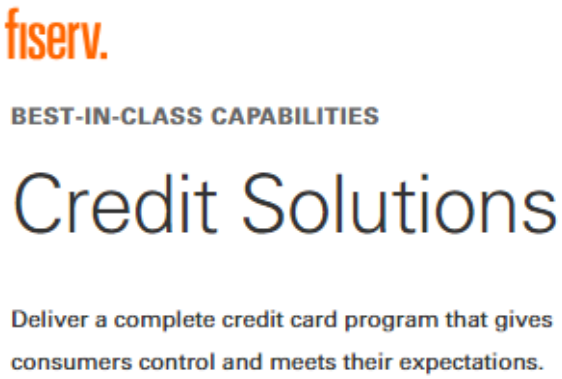
EMV® Contactless Specifications for Payment Systems, Book C-2, Kernel 2 Specification, Version 2.7, April 2018

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

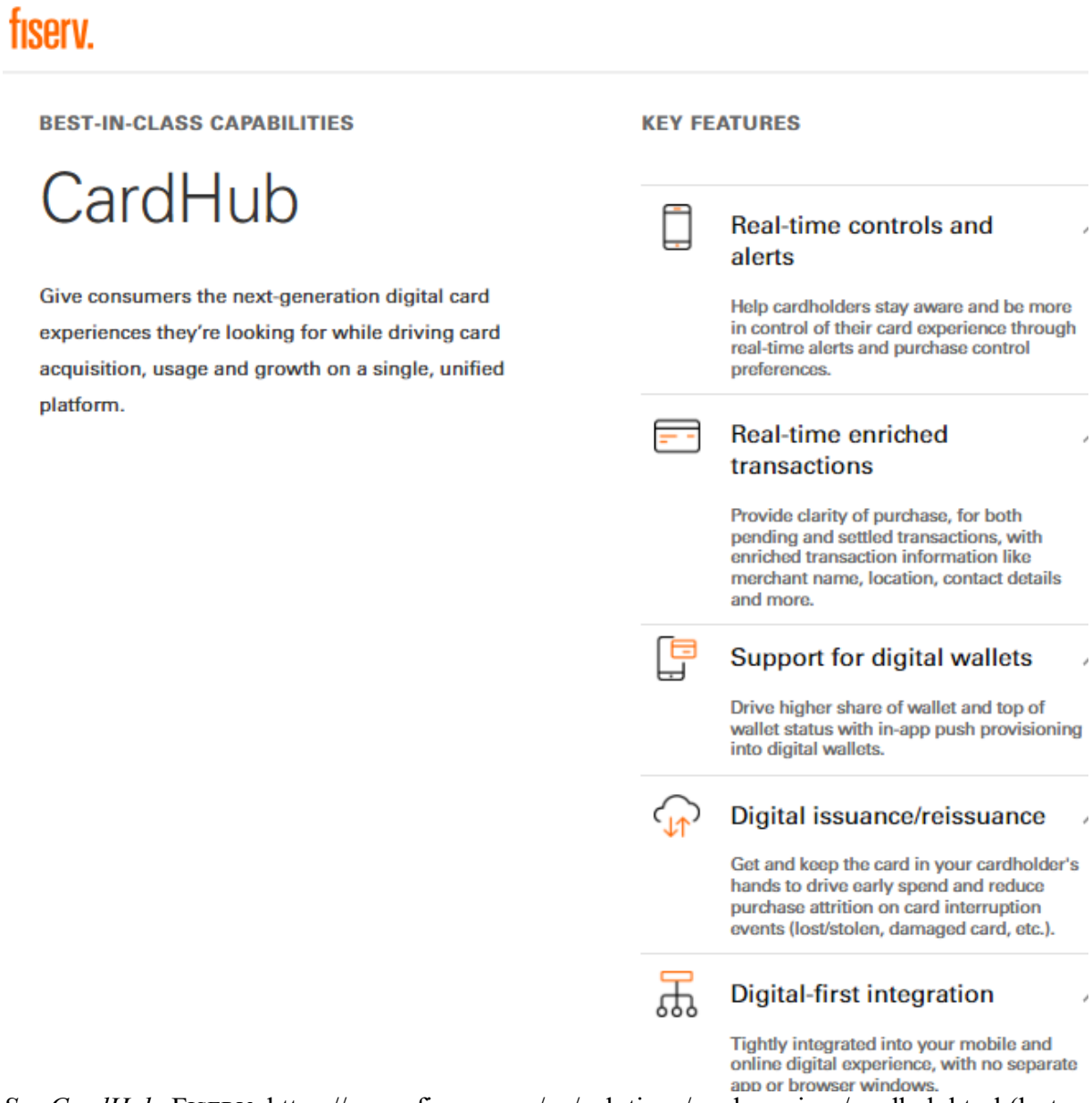
directory to identify a payment system that is mutually supported and appropriate for a particular transaction.

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

101. As an example, Fiserv provides a complete set of card issuance solutions for banks and financial institutions as illustrated in screenshots from Fiserv's website as shown below.

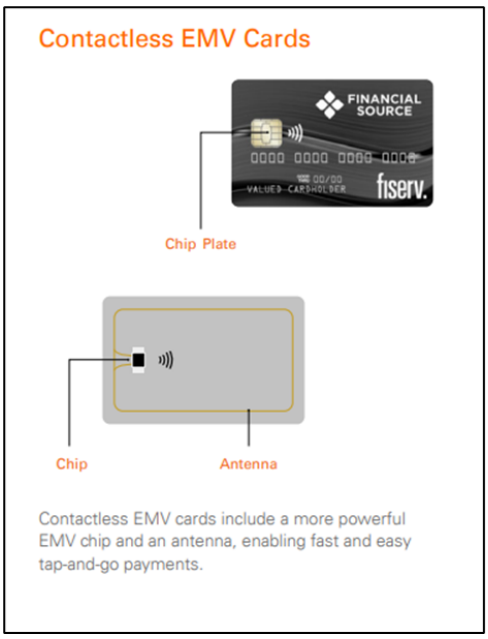


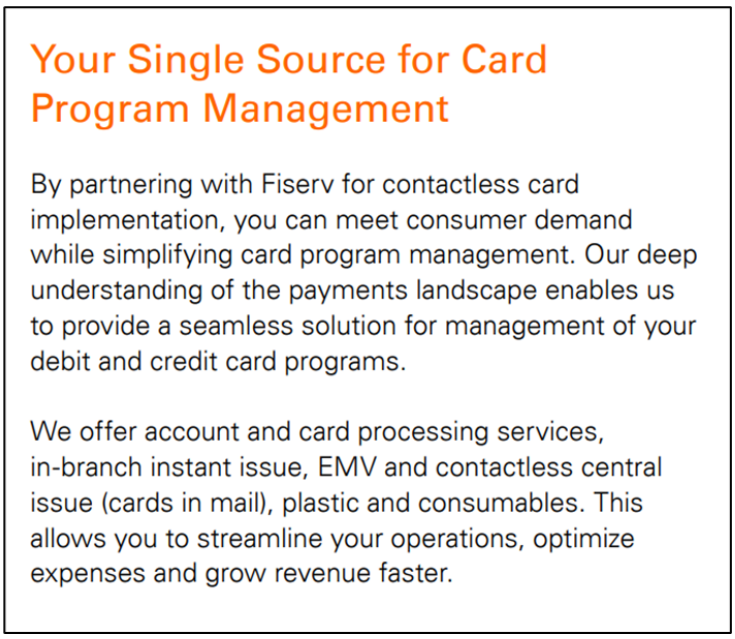
See Credit Solutions, FISERV, https://www.fiserv.com/en/solutions/card-services/credit-solutions.html (last visited Oct. 13, 2023).



See CardHub, FISERV, https://www.fiserv.com/en/solutions/card-services/cardhub.html (last visited Oct. 13, 2023).

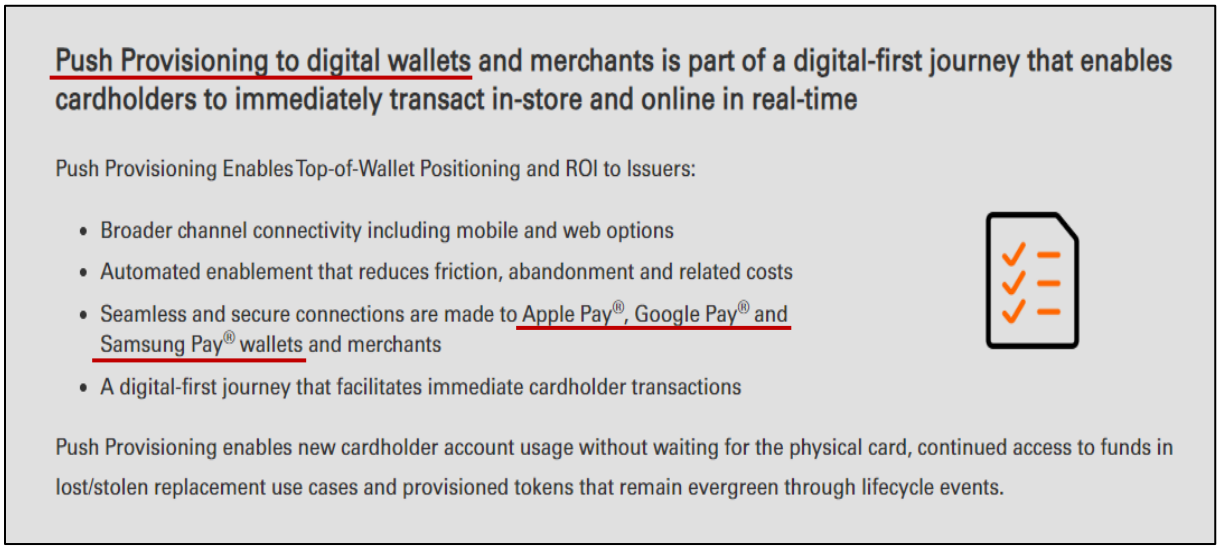
102. By their own actions, on behalf of third parties, and/or via direction and control of third parties, Defendants make, sell, provide, issue, and/or provision smartcards and also act on behalf of and/or direct and control the activities of third parties in connection with smartcards.





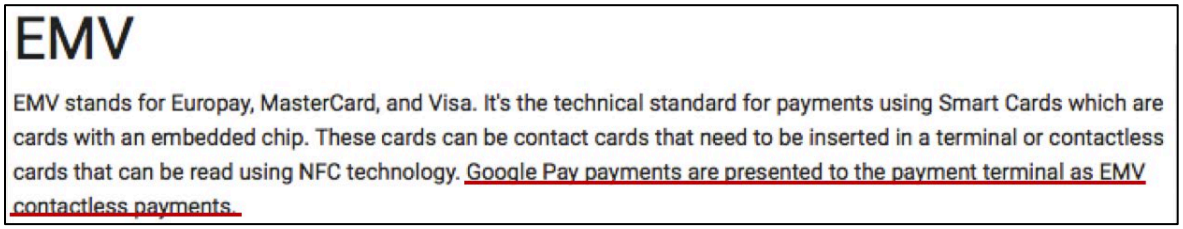
Solution: Contactless EMV® Cards, FISERV, https://www.fiserv.com/content/dam/fiserv-ent/final-files/marketing-collateral/sales-sheets/Contactless_EMV_Cards_Sales_Sheet_0221.pdf (last visited Oct. 13, 2023).

103. As an example, Fiserv provisions EMV compliant payment applications for consumers' cards onto mobile wallets, including without limitation Google Pay and Samsung Pay.



Real-Time Provisioning Drives Issuer Cards to Top of Wallet, FISERV, https://www.fiserv.com/en/solutions/payments/credit-and-debit-solutions/real-time-

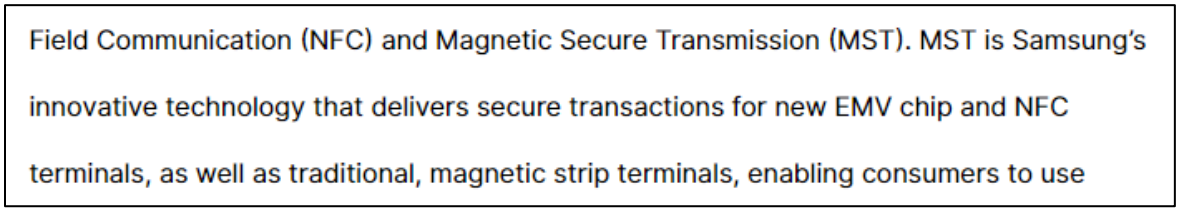
provisioning.html (last visited Oct. 12, 2023) (describing "Push Provisioning from Fiserv" that "drives tokens from the issuer to destination wallets and merchants").



EMV

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

Google Pay Merchant Help: EMV, GOOGLE, https://support.google.com/pay/merchants/answer/7151369?hl=en (last visited Oct. 12, 2023).



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

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

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

3.4.3 EMV Mode

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

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

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

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

The basic functions of the POS System include:

- communication with contactless cards
- application selection and kernel activation

5.8.2 Application Selection and Kernel Activation

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

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

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

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

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

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

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

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

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

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

108. The Accused Instrumentalities of Defendants infringe one or more claims of the '707 patent, which provide technological solutions and improvements for securing a Radio Frequency (RF) transaction using a Radio Frequency Identification (RFID) transaction device.

109. Conventional methods for payment transactions aimed at minimizing fraudulent RFID transactions were problematic due to increased transaction times. For example, one conventional method for securing RFID transactions required the device user to provide a secondary form of identification such as a personal Identification Number (PIN), which delayed the transaction. Increased transaction times, in turn, were an impediment to RFID transactions, especially given that one of the advantages of RFID transaction instruments (e.g., RFID transaction devices) is providing expedient transactions. Advantageously, the '707 patent provides systems and methods that can be used to secure RFID transactions. For example, the '707 patent addresses transactions involving an RFID reader (e.g., Fiserv, Clover and/or Carat reader) and an RFID transaction device (e.g., a contactless Mastercard Card and/or a mobile wallet). As described in exemplary embodiments of the '707 patent, a random number is transmitted from an RFID reader to an RFID transaction device. In the RFID transaction device, an RFID transaction device authentication tag is created using at least (a) the random number, (b) a routing number associated with a transaction account, and (c) a stored counter value. Next, the RFID transaction device authentication tag is transmitted to the RFID reader, and the stored counter value in the RFID transaction device is incremented. A transaction request for verification is formed from at least the RFID transaction device authentication tag and the stored counter value. The transaction request for verification is transmitted, the transaction request is processed, and at least one of the RFID transaction device authentication tags and the stored counter value is verified. Systems and methods

of the ’707 patent, such as these, advantageously address problems found in conventional methods for securing RFID transactions.

110. Defendants infringe one or more claims of the ‘707 patent via Fiserv’s directly and/or indirectly making, providing, and/or selling EMV compliant POS systems and devices (e.g., via at least one or more Clover subsidiaries and/or brands), including acting on behalf of and/or directing and controlling third parties in connection with the use of those systems and/or devices. These POS systems and devices perform a method of securing RFID transactions with mobile wallets using host card emulation (e.g., Google Pay and Samsung Pay).

Clover accepts all major types of payments

Although some contactless payment companies lock you into their technology, Clover POS systems accept all of the most popular types of traditional and contactless payments.

Clover devices accept numerous methods of payment, including:

- Cash
- Checks
- Credit cards
- Debit cards
- Prepaid cards
- Gift cards
- EBT cards
- Custom tenders
- Alipay[9]

> Credit and debit cards are the most popular payment methods. Many cards are already contactless-enabled and many more are being issued with contactless payments capabilities so that they can be simply waved over a Clover device for payment. In addition, almost all cards can be added to a mobile wallet, including:
>
> - Apple Pay®
> - Google Pay™
> - Samsung Pay®

Contactless Payments, CLOVER, https://www.clover.com/small-business-resources/contactless-payments (last visited Oct. 17, 2023) (emphasis added).

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

Google Pay Merchant Help: EMV, GOOGLE, https://support.google.com/pay/merchants/answer/7151369?hl=en (last visited Oct. 12, 2023) (emphasis added).

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

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

111. Examples of Fiserv's EMV compliant POS systems and devices include the following Clover systems and devices:

Handheld card reader to take payments wherever you do business

$49

SHOP GO

Peak performance at your fingertips on a large 14" touchscreen

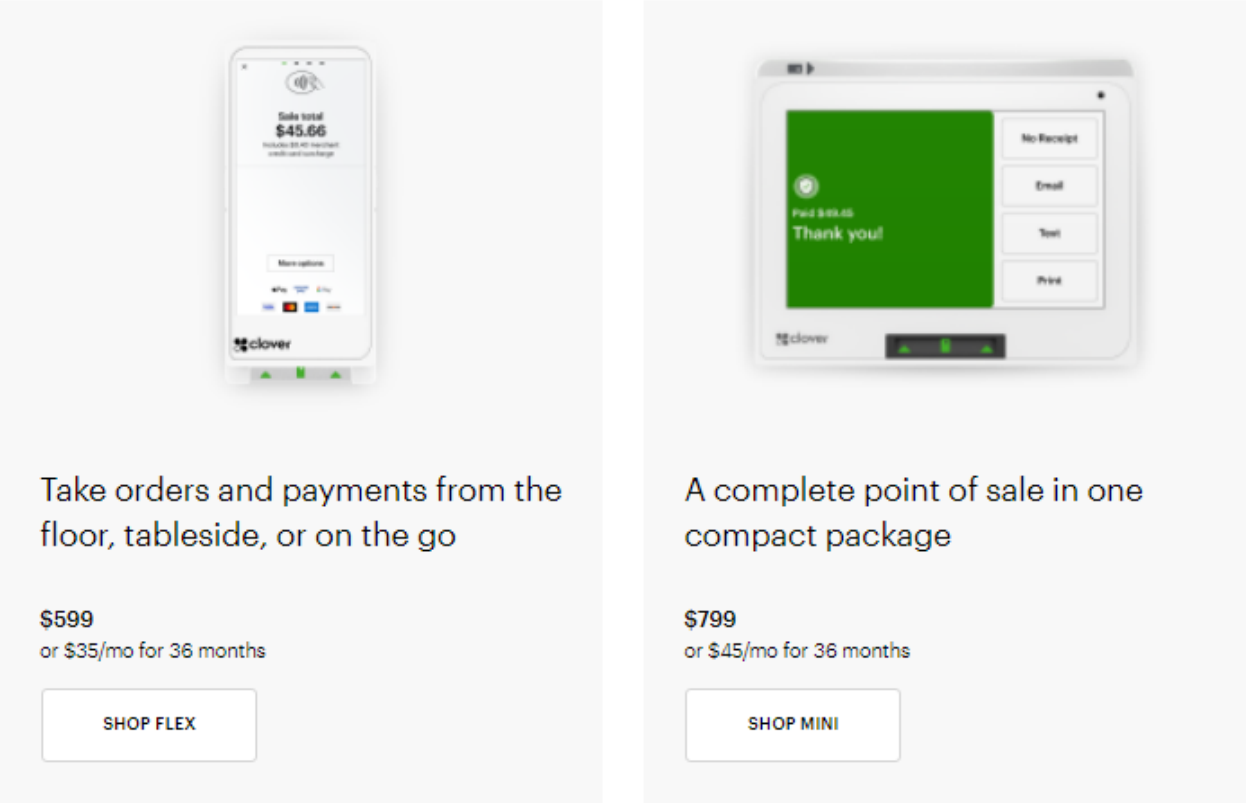
$1,699
or $125/mo for 36 months

SHOP STATION SOLO

A powerful point of sale for both sides of the counter

$1,799
or $135/mo for 36 months

SHOP STATION DUO



Flexible POS systems tailored to your business, CLOVER, https://www.clover.com/shop (last visited Oct. 17, 2023).

112. Fiserv's Clover EMV readers transmit an unpredictable (random) number to an RFID transaction device as part of a Generate AC command, commanding the RFID transaction device to compute and return an Application Cryptogram. This is exemplified by Kernel 2 applicable to Mastercard.

> **5.4 Generate AC**
>
> **5.4.1 Definition and Scope**
>
> The GENERATE AC command sends transaction-related data to the Card, which then computes and returns an *Application Cryptogram*. Depending on the risk management in the Card, the cryptogram returned by the Card may differ from that requested in the command message. The Card may return an AAC (transaction declined), an ARQC (online authorization request), or a TC (transaction approved).

A.1.187 Unpredictable Number

Tag:	'9F37'
Template:	—
Length:	4
Format:	b
Update:	K
Description:	Contains a Kernel challenge (random) to be used by the Card to ensure the variability and uniqueness to the generation of a cryptogram during an EMV mode transaction.

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

113. The transaction device authentication tag comprises of an Application Cryptogram for Online Authorization (ARQC) which is encrypted using a Limited use Key (LUK) from the device. The LUK is generated using an Application Transaction Counter (ATC) value at the time the LUK was generated, and a Primary Account Number (PAN).

8.1.2 Application Cryptogram Algorithm

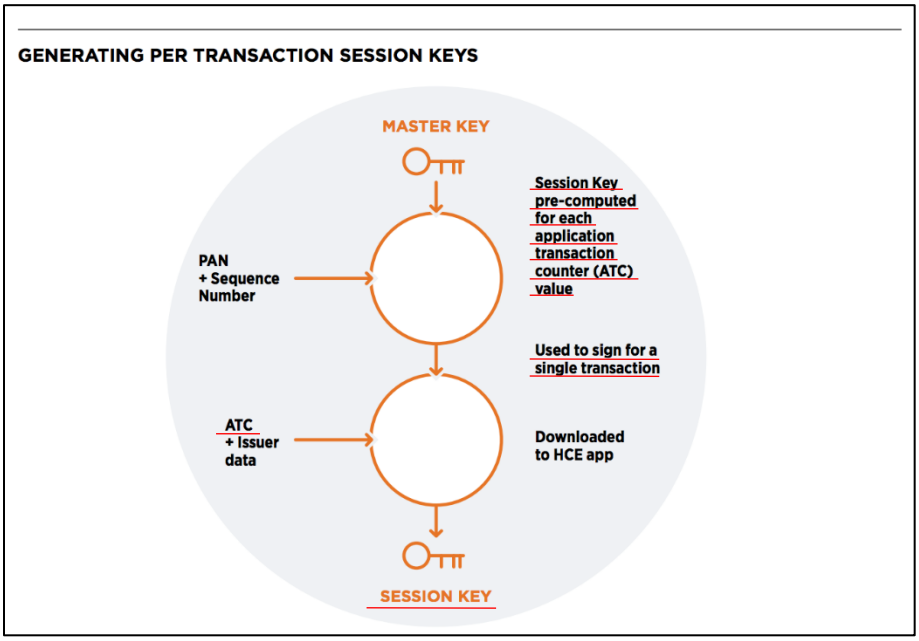
The method for Application Cryptogram generation takes as input a unique ICC Application Cryptogram Master Key MK_{AC} and the data selected as described in section 8.1.1, and computes the 8-byte Application Cryptogram in the following two steps:

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.

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

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

https://www.gsma.com/digitalcommerce/wp-content/uploads/2014/11/GSMA-HCE-and-Tokenisation-for-Payment-Services-paper_WEB.pdf



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

limited-use key

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

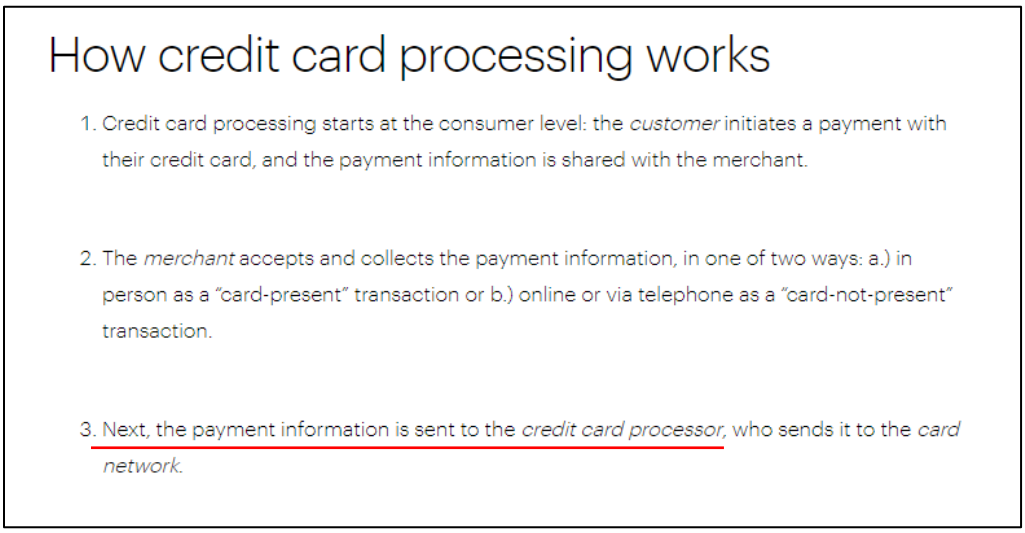
limited-use key, GOOGLE, https://support.google.com/pay/merchants/answer/7151225?hl=en (last visited Oct. 18, 2023) (emphasis added)

114. The RFID transaction device transmits the Application Cryptogram in response to the Generate AC command from the point-of-sale terminal (e.g., Clover reader). This is exemplified by Kernel 2 applicable to Mastercard.

115. The Application Transaction Counter (ATC) in the transaction device is incremented each time a transaction is performed.

116. The point-of-sale terminal (e.g., Clover terminal) transmits a transaction request for authorization, which includes the ARQC and the ATC, as exemplified by Kernel 2, applicable to Mastercard.

117. Fiserv (e.g., via a Clover device and/or system) then processes the transaction request, wherein the LUK is validated by the issuer, by e.g., verifying that the number of transactions indicated by ATC is not more than 1, and by validating the ARQC.



How credit card processing works

1. Credit card processing starts at the consumer level: the *customer* initiates a payment with their credit card, and the payment information is shared with the merchant.

2. The *merchant* accepts and collects the payment information, in one of two ways: a.) in person as a "card-present" transaction or b.) online or via telephone as a "card-not-present" transaction.

3. Next, the payment information is sent to the *credit card processor*, who sends it to the *card network*.

Credit card processor. Also known more generally as a "payment processor." The entity that facilitates communication between the merchant, the credit card network, and the cardholder's bank. Processors, along with merchants, are responsible for maintaining compliance with the Payment Card Industry Data Security Standards (PCI DSS). Some payment processors provide their own payment gateways, while others, typically the larger processors, have reseller agreements with payment gateways.

Credit Card Processing: The All-You-Need-to-Know Guide, CLOVER, https://www.clover.com/small-business-resources/credit-card-processing (last visited Oct. 18, 2023) (emphasis added).

> **Step 5: Authorization response**
> The issuing bank authorizes the transaction and routes the response back to the merchant.

How the payment process works, MASTERCARD, https://sea.mastercard.com/en-region-sea/business/merchants/start-accepting/payment-process.html (last visited Oct. 18, 2023).

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

Madhu Vasu, Senior Director, Innovation and Strategic Partnerships, Visa Inc, available at: https://www.kansascityfed.org/~/media/files/publicat/pscp/2015/sessions/2015-psr-conf-session4-paneldiscussion.pdf?la=en (emphasis added)

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

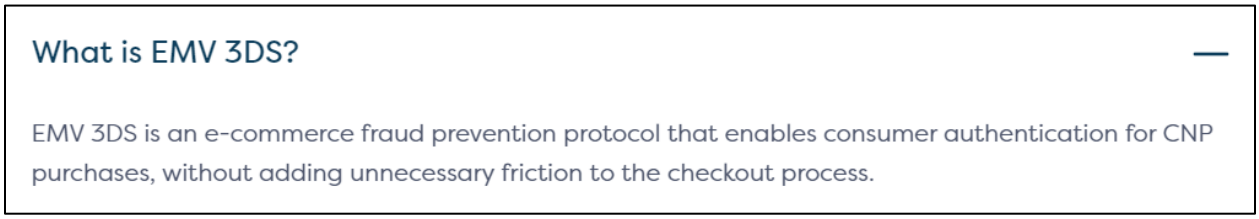
Payment Strategies, FEDERAL RESERVE BANK OF BOSTON, https://www.bostonfed.org/-/media/Documents/PaymentStrategies/understanding-the-role-of-host-card-emulation-in-mobile-wallets-brief-rmay-2016.pdf (last visited Oct. 18, 2023)

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

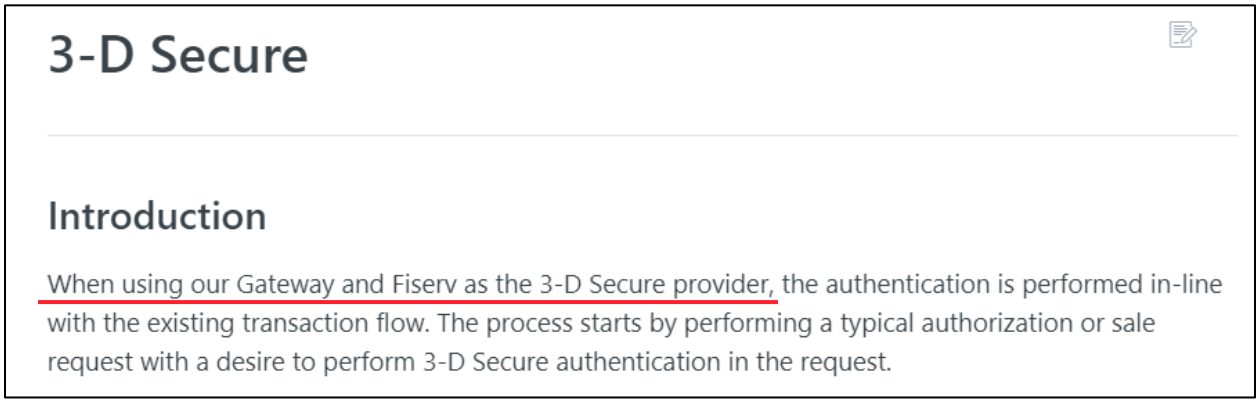
119. Conventional methods for payment transactions aimed at card transaction fraud were unsatisfactory, especially for online commerce (e.g., e-commerce). The increased risk of fraud with online and "card not present" transactions means that payment processors or providers historically may charge significantly higher rates for merchants engaging in online commerce, in some cases almost twice as much as the rates charged to "brick and mortar" merchants. Advantageously, the '207 patent provides systems and methods that can be used to authenticate the identity of a customer as the true cardholder, even when a card is not presented for payment. Among other benefits, to cardholders, merchants, and payment processors, this can reduce the risk of a card being used improperly. As described in exemplary embodiments of the '207 patent, a card payment request is submitted to a merchant. A communication is initiated between a cardholder submitting the card payment request and an authorization computer of an issuer. An authorization request is received from the merchant in response to said card payment request, and an identity of the cardholder is authenticated using information received from the cardholder. The authentication includes matching the information received from the cardholder with a corresponding predetermined stored value and generating an authentication score representing a relative reliability of the identity of the cardholder based on the information from the cardholder. The authorization request is matched to the cardholder, the authorization request is authorized and, if the authorization request is approved, a private payment number is generated. Upon authorizing the authorization request, an authorization confirmation including the authorization score and the private payment

number is issued to the merchant. Systems and methods of the '207 patent, such as these, advantageously address inadequacies found in conventional methods for securing e-commerce transactions.

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



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



3-D Secure, FISERV, https://docs.fiserv.dev/public/docs/payments-3ds (last visited Oct. 18, 2023) (emphasis added).

121. Fiserv also acts as the gateway and payment processor for its merchant customers.

The Role of a Payment Processor

Payment processors transmit the payment data among the four parties listed above (i.e., you, the customer, the customer's bank, and your bank). In many cases, payment processors also provide merchants with the physical equipment needed to accept card-based transactions. In addition, they often help businesses create a merchant account – in-house or with a third-party merchant services provider.

It's technically possible to obtain your merchant account, payment gateway, and payment processing from different providers. However, this can create difficulties whenever issues or disputes arise. Who is responsible if your online store suddenly stops accepting credit cards in the middle of the night?

By securing all three from the same provider, however, you minimize interoperability issues. Whenever you face an issue, there is only one provider you need to call.

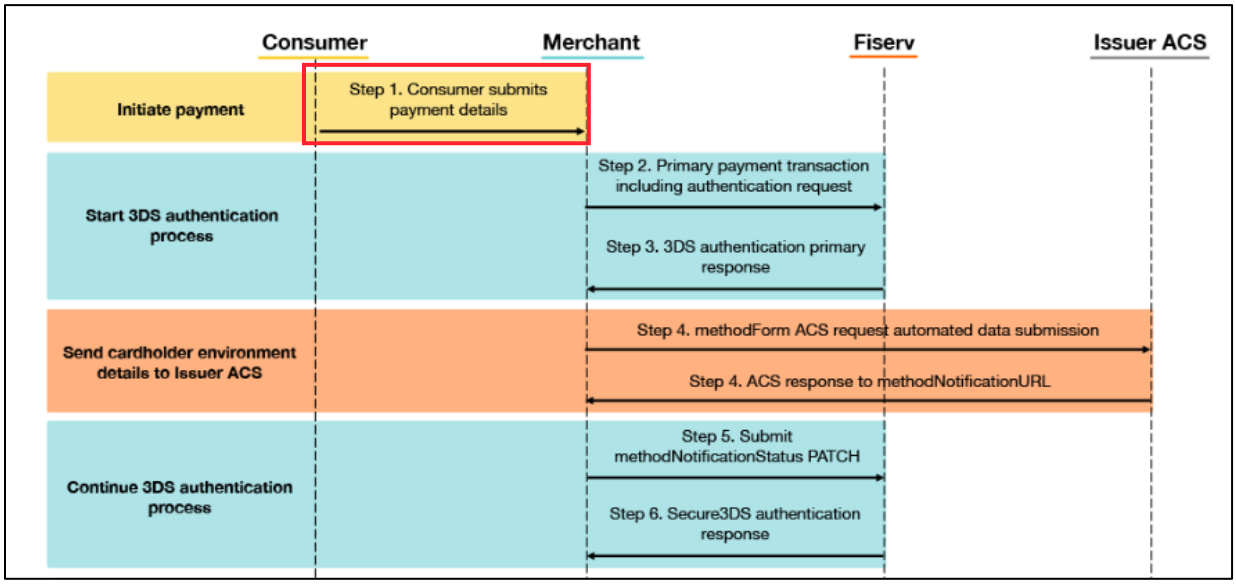
Payment Gateway vs. Payment Processor: What Is the Difference?, FISERV, https://merchants.fiserv.com/en-us/resources/payment-gateway-vs-payment-processor/ (last visited Oct. 18, 2023) (emphasis added).

122. As the merchant gateway, Fiserv receives a card payment request at the user's browser.

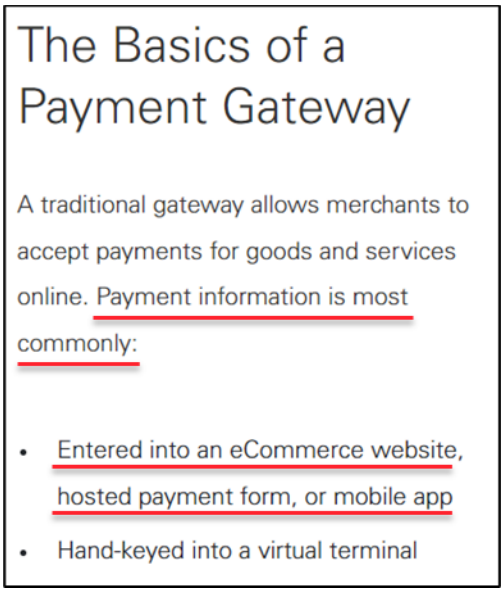
3-D Secure

Introduction

When using our Gateway and Fiserv as the 3-D Secure provider, the authentication is performed in-line with the existing transaction flow. The process starts by performing a typical authorization or sale request with a desire to perform 3-D Secure authentication in the request.



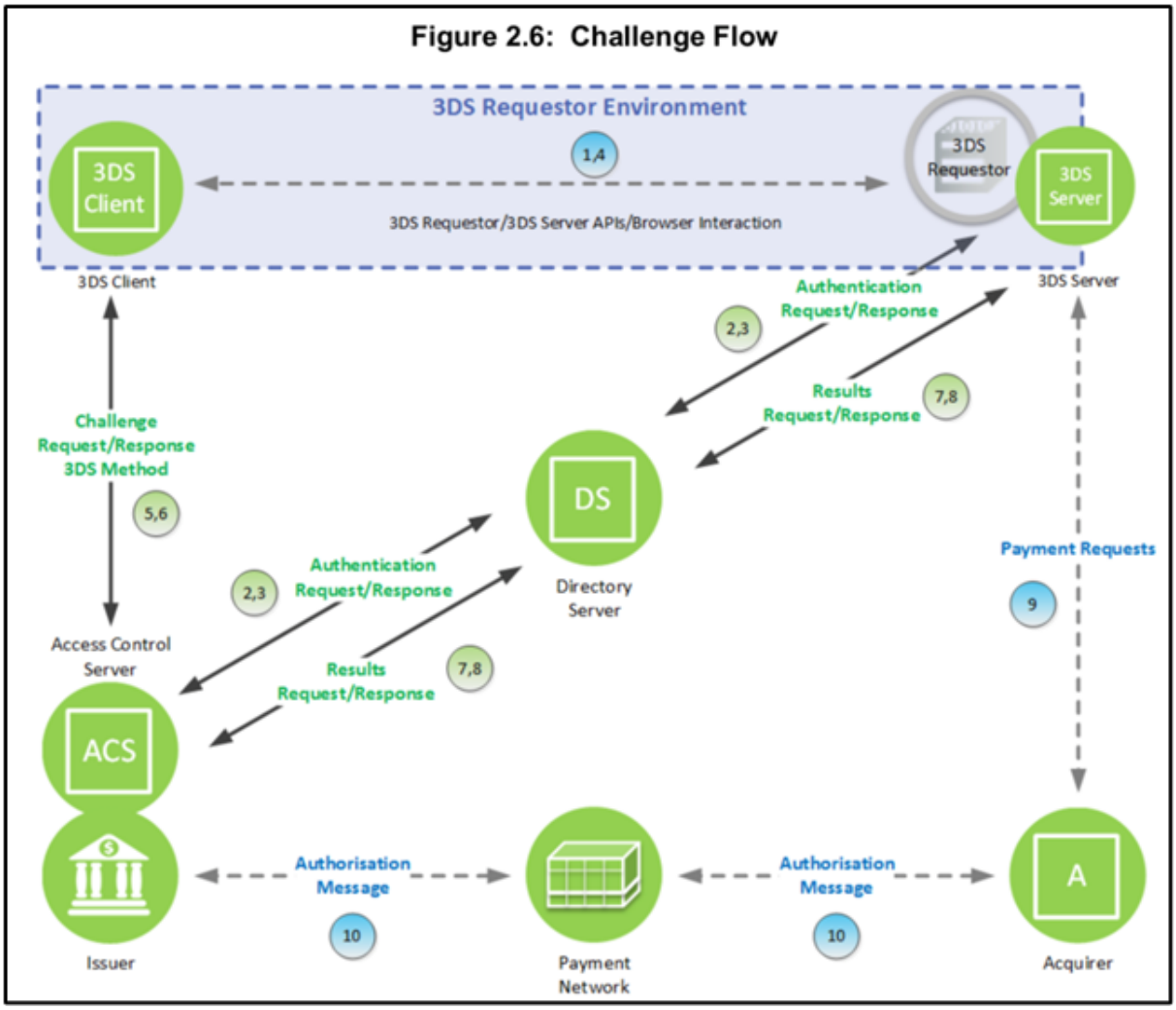
3-D Secure, FISERV, https://docs.fiserv.dev/public/docs/payments-3ds (last visited Oct. 18, 2023) (emphasis added).



What Is a Payment Gateway, FISERV, https://merchants.fiserv.com/en-us/resources/what-is-a-payment-gateway/ (last visited Oct. 18, 2023) (emphasis added).

123. If 3DS authentication is selected for the transaction, Fiserv initiates a communication between the cardholder and an ACS server of the issuing bank.

124. Fiserv receives a primary payment transaction request from the merchant gateway, sent in response to the card payment request from the cardholder. The primary payment transaction request includes a 3DS authentication request.



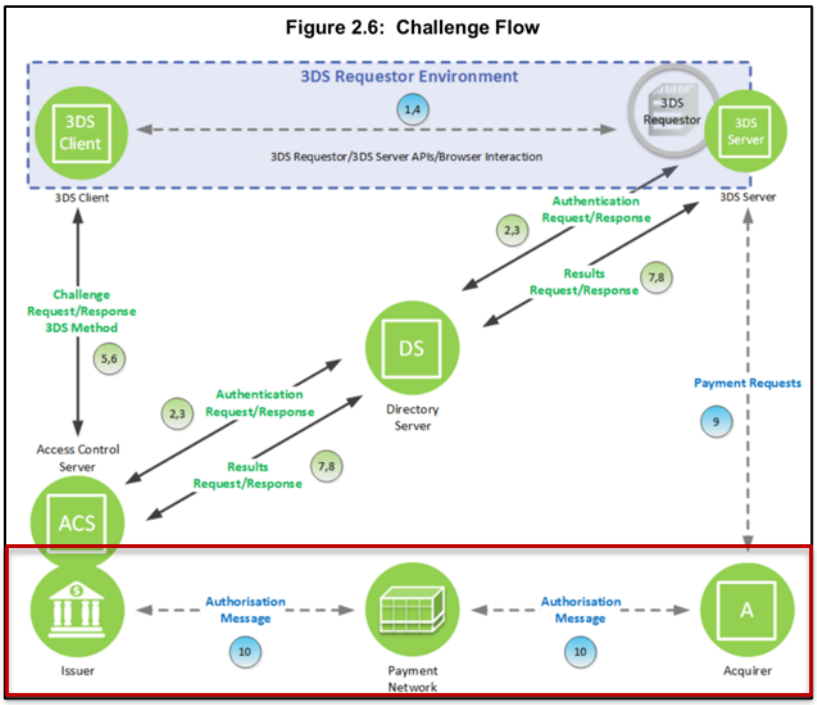
EMV 3-D Secure: Protocol and Core Functions Specification, EMVCo, Version 2.1.0, https://docs.3dsecure.io/3dsv2/_downloads/0b80f2e0693052852012f1151cde4f01/EMVCo_3DS_spec_v210.pdf (October 2017). The ACS Server authenticates the identity of the cardholder by matching the information, received from the user, with the information stored on the server. The information depends on a chosen authentication method.

125. The ACS generates an authentication score that it places in the transStatusReason field.

Data Element/Field Name	Description	Source	Length/Format/Values	Device Channel	Message Category	Message Inclusion	Conditional Inclusion
Transaction Status Reason Field Name: `transStatusReason`	Provides information on why the Transaction Status field has the specified value.	ACS DS	Length: 2 characters JSON Data Type: String Values accepted: • 01 = Card authentication failed • 02 = Unknown Device • 03 = Unsupported Device • 04 = Exceeds authentication frequency limit • 05 = Expired card • 06 = Invalid card number • 07 = Invalid transaction • 08 = No Card record • 09 = Security failure • 10 = Stolen card • 11 = Suspected fraud • 12 = Transaction not permitted to cardholder • 13 = Cardholder not enrolled in service • 14 = Transaction timed out at the ACS • 15 = Low confidence • 16 = Medium confidence • 17 = High confidence • 18 = Very High confidence • 19 = Exceeds ACS maximum challenges	01-APP 02-BRW 03-3RI	01-PA 02-NPA	ARes = C RReq = C	For 01-PA, required if the Transaction Status field = N, U, or R. For 02-NPA, Conditional as defined by the DS.

EMV 3-D Secure: Protocol and Core Functions Specification, EMVCo, Version 2.1.0, https://docs.3dsecure.io/3dsv2/_downloads/0b80f2e0693052852012f1151cde4f01/EMVCo_3DS_spec_v210.pdf (October 2017) (emphasis added).

126. If the authentication is successful and the Issuer does not otherwise decline the transaction, the issuer authorizes the transaction and sends. At the time of authorization, issuers generate a six-digit authorization code for every transaction.



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

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

EMV 3-D Secure: Protocol and Core Functions Specification, EMVCo, Version 2.1.0, https://docs.3dsecure.io/3dsv2/_downloads/0b80f2e0693052852012f1151cde4f01/EMVCo_3DS_spec_v210.pdf (October 2017) (emphasis added).

Electronic Commerce Transactions

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

Transaction Processing Rules, MASTERCARD, https://www.mastercard.us/content/dam/mccom/en-us/documents/TPR-manual-June2015.pdf (June 9, 2015) (last visited Oct. 18, 2023).

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

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

127. The ACS sends a final response to the merchant containing the authentication score as well as a Transaction Identifier.

Data Element/Field Name	Description	Source	Length/Format/Values	Device Channel	Message Category	Message Inclusion	Conditional Inclusion
Transaction Status Reason Field Name: transStatusReason	Provides information on why the Transaction Status field has the specified value.	ACS DS	Length: 2 characters JSON Data Type: String Values accepted: • 01 = Card authentication failed • 02 = Unknown Device • 03 = Unsupported Device	01-APP 02-BRW 03-3RI	01-PA 02-NPA	ARes = C RReq = C	For 01-PA, required if the Transaction Status field = N, U, or R. For 02-NPA, Conditional as defined by the DS.

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

EMV 3-D Secure: Protocol and Core Functions Specification, EMVCo, Version 2.1.0, https://docs.3dsecure.io/3dsv2/_downloads/0b80f2e0693052852012f1151cde4f01/EMVCo_3DS_spec_v210.pdf (October 2017) (emphasis added).

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

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

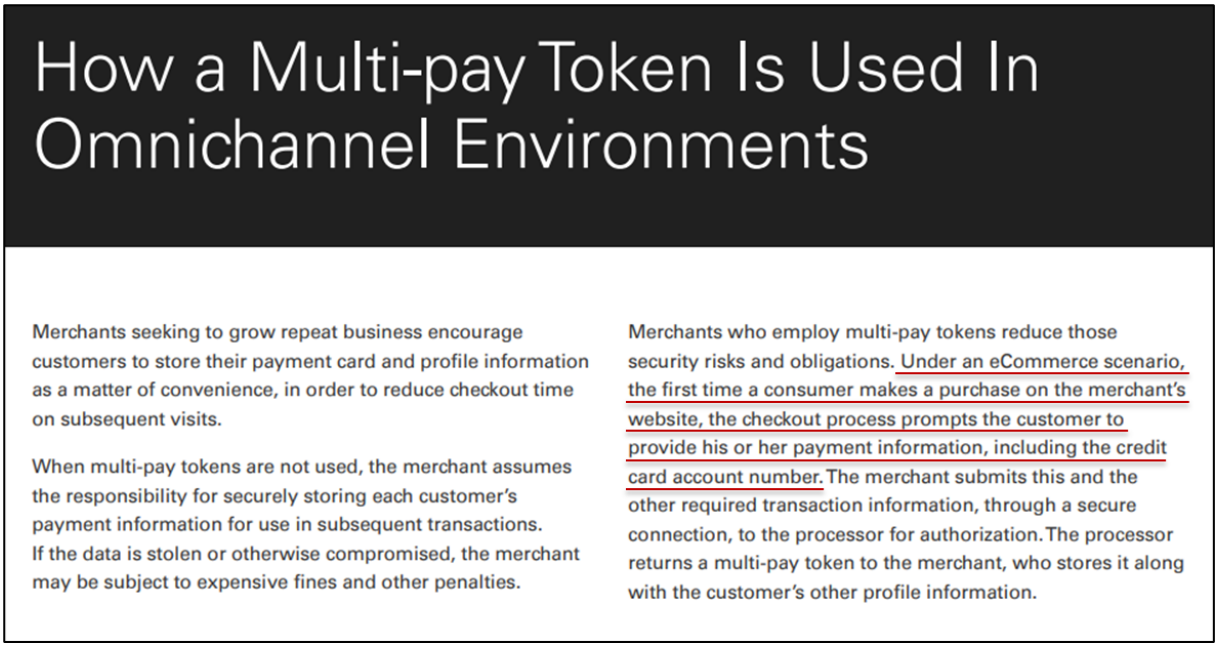
https://www.mastercard.us/en-us/merchants/get-support/merchant-learning-center/glossary.html

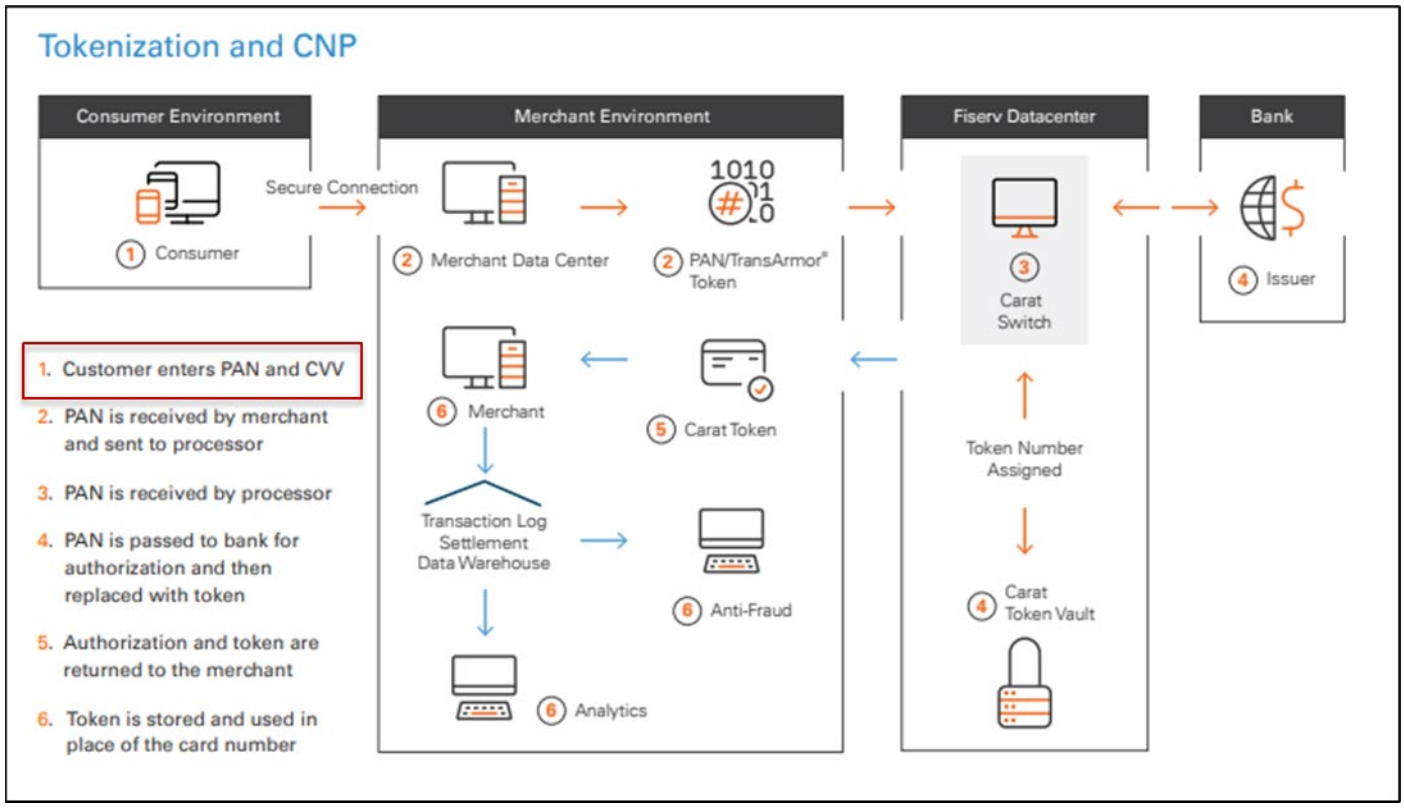
128. The Accused Instrumentalities of Defendants infringe one or more claims of the '960 patent, which provide technological solutions and improvements for facilitating a transaction using a secondary transaction number in lieu of an account number.

129. Conventional methods for payment transactions have been beset by several undesirable attributes. For example, simply using and recording a customer's actual account number for a transaction can increase the risk that the account number is obtained and improperly used by a third party.

130. Advantageously, the '960 patent provides systems and methods that can be used to facilitate a transaction using a secondary transaction number in lieu of an account number, for example, as occurs via Fiserv's Multi-pay Token service. As described in exemplary embodiments of the '960 patent, an account number of a user is received by a merchant and via a processor. The account number is submitted, by the merchant and via the processor, to a provider of the account number, and authorization of the transaction is requested. The provider is requested, by the merchant and via the processor, to return a secondary transaction number (STN) in lieu of returning the account number. An authorization record referencing the STN is received from the provider and via the processor. A settlement request associated with the transaction is issued, via the processor, and the settlement request includes the STN and does not include the account number. A record of the transaction is maintained, by the merchant and via the processor. The account number is replaced with the STN, and the record of the transaction includes the STN, and the record of the transaction does not include the account number. Systems and methods of the '960 patent, such as these, advantageously address problems found in conventional methods for processing transactions using an account number.

131. Defendants infringe one or more claims of the ’960 patent via directly and/or indirectly providing and/or selling Fiserv’s Multi-pay Token service. Fiserv’s Multi-pay Token service allows merchants to use and store a token in place of customer credit card information. The first time a customer uses a card to make a purchase (and saves for future use), they are prompted to enter a credit card account number. Fiserv receives the account number at a merchant portal and via a processor.

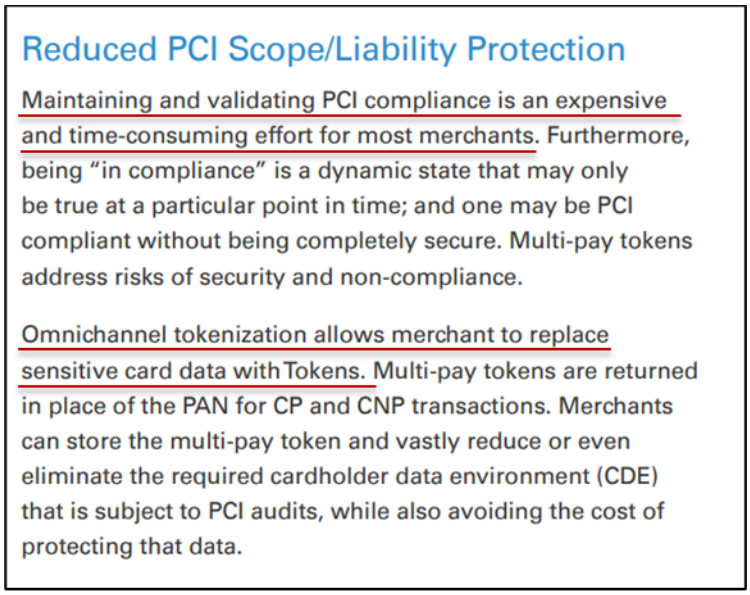




Reducing PCI Scope With Omnichannel Tokens, CARAT, https://www.carat.fiserv.com/content/dam/carat/us/en/pdf/multi-pay-token-whitepaper.pdf (2021) (last visited Oct. 18, 2023).

132. The merchant submits an authorization request, including the credit card account number, to the issuer, via a processor, for authorization.

133. Fiserv is PCI compliant, as such, Fiserv stores account numbers on behalf of merchants, and uses tokenization to return a token ("secondary transaction number") in lieu of the account number.

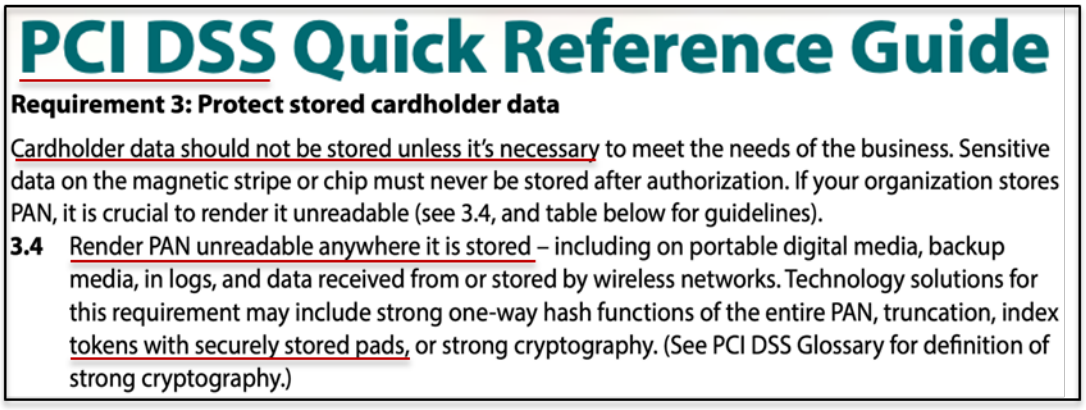


Reduced PCI Scope/Liability Protection

Maintaining and validating PCI compliance is an expensive and time-consuming effort for most merchants. Furthermore, being "in compliance" is a dynamic state that may only be true at a particular point in time; and one may be PCI compliant without being completely secure. Multi-pay tokens address risks of security and non-compliance.

Omnichannel tokenization allows merchant to replace sensitive card data with Tokens. Multi-pay tokens are returned in place of the PAN for CP and CNP transactions. Merchants can store the multi-pay token and vastly reduce or even eliminate the required cardholder data environment (CDE) that is subject to PCI audits, while also avoiding the cost of protecting that data.

Reducing PCI Scope With Omnichannel Tokens, CARAT, https://www.carat.fiserv.com/content/dam/carat/us/en/pdf/multi-pay-token-whitepaper.pdf (2021) (last visited Oct. 18, 2023).



PCI DSS Quick Reference Guide

Requirement 3: Protect stored cardholder data

Cardholder data should not be stored unless it's necessary to meet the needs of the business. Sensitive data on the magnetic stripe or chip must never be stored after authorization. If your organization stores PAN, it is crucial to render it unreadable (see 3.4, and table below for guidelines).

3.4 Render PAN unreadable anywhere it is stored – including on portable digital media, backup media, in logs, and data received from or stored by wireless networks. Technology solutions for this requirement may include strong one-way hash functions of the entire PAN, truncation, index tokens with securely stored pads, or strong cryptography. (See PCI DSS Glossary for definition of strong cryptography.)

PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard, PCI, available at https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf, version 3.2.1 (July 2018) (last visited Oct. 18, 2023).

134. The merchant receives an authorization response and the token.

135. While the initial transaction will use a payment card's real account number, subsequent transactions, such as recurring invoices or future purchases (i.e., settlement requests), will use the token instead of the account number.

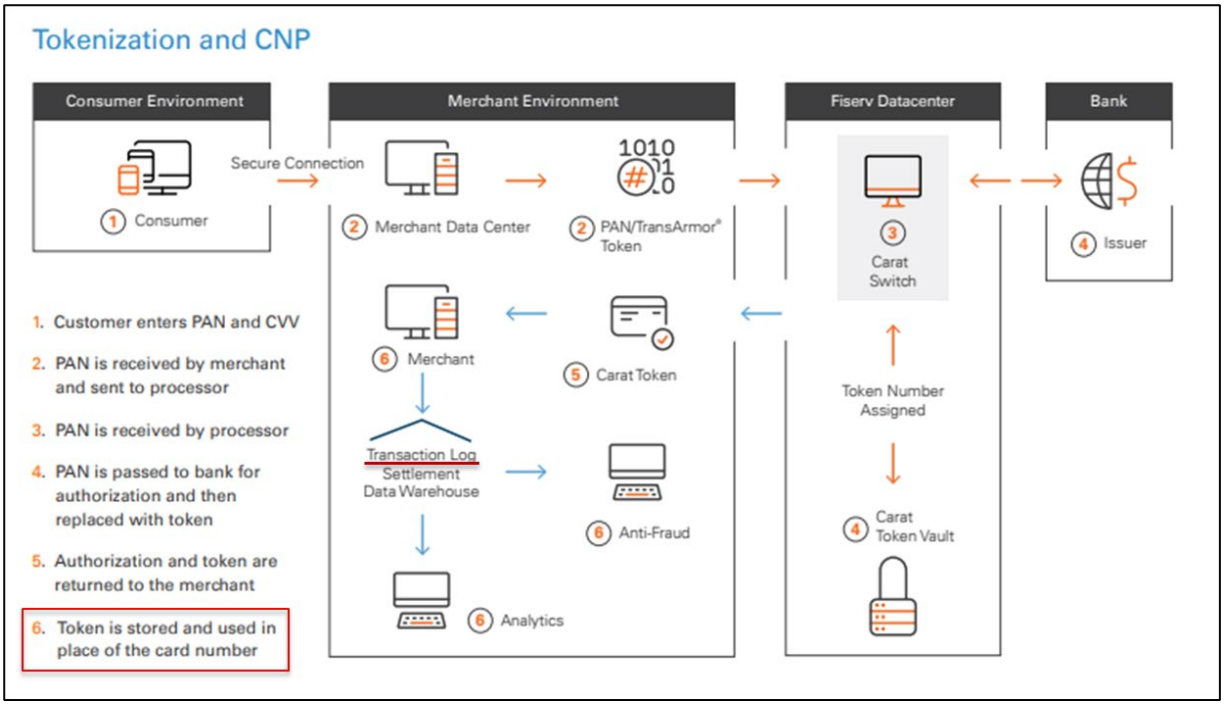
> An important feature of multi-pay tokens is that they are unique not only to the particular PAN but also to that merchant; only the merchant can use the token to process subsequent transactions, making it highly resistant to theft. While the merchant's initial transaction with the consumer's payment card uses the real account data, all subsequent transactions (for example: to process refunds, credits and future purchases) with the same payment card use the token instead.

> To more easily protect that data, "multi-pay" tokens give merchants the ability to utilize the token for subsequent card-on-file transactions. This makes multi-pay tokens an ideal solution for eCommerce merchants and service providers submitting recurring invoices.

Reducing PCI Scope With Omnichannel Tokens, CARAT, https://www.carat.fiserv.com/content/dam/carat/us/en/pdf/multi-pay-token-whitepaper.pdf (2021) (last visited Oct. 18, 2023).

136. When using Fiserv's tokenization services, the merchant does not maintain a record of the account number. Thus, the settlement request sent by the merchant uses the token in lieu of the account number in clearing and settlement messages.

137. Merchants maintain a transaction log and other records of the transaction, wherein the token is used in lieu of the account number.



Reducing PCI Scope With Omnichannel Tokens, CARAT, https://www.carat.fiserv.com/content/dam/carat/us/en/pdf/multi-pay-token-whitepaper.pdf (2021) (last visited Oct. 18, 2023).

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

139. By utilizing EMV standards and performing the patented methods for transaction processing, the Accused Instrumentalities include Defendants' products, methods, and/or services for offering, issuing, providing, registering, facilitating, maintaining, authenticating, validating, processing, directing, controlling and/or deriving substantial revenue from commercial transactions via Fiserv Transaction Instruments (e.g., Mastercard Cards) and other associated accounts that are

covered by the Asserted Patents. Furthermore, the Accused Instrumentalities include products, methods, and/or services for initiating secure communications between users of Defendants' websites and Defendants' web servers and for providing self-auditing features of users' privacy data that are also covered by the Asserted Patents. Along with the above technology discussion, each respective Count below describes how the Accused Instrumentalities infringe on specific claims of the Asserted Patents.

COUNT I

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

140. Plaintiff incorporates paragraphs 1 through 139 herein by reference.

141. 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.

142. 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.

143. 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.

144. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '369 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those

associated with payment transaction instruments (e.g., EMV contactless cards made by Fiserv and sold to financial institutions, Fiserv Transaction Devices, Fiserv Cards, Mastercard Transaction Instruments, and/or Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

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

146. Defendant FSI directly infringes the '369 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant FSS, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '369 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused

Instrumentalities. For example, on information and belief, FSS, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

147. 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/or consumers to perform one or more steps of the claimed methods of the '369 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) ("[A]n actor is liable for infringement under § 271(a) if it acts through an agent … or contracts with another to perform one or more steps of a claimed method."). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants' agreements with such third parties to provide access to Defendants' products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants' products, systems, methods, and/or services, for example, Fiserv Cards and/or

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

148. In addition to the liability arising from the Defendants' relationship with third parties, Defendants also directly infringe, individually and/or jointly, the '369 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards). On information and belief, Defendants design and develop payment applications for accounts used in connection with Fiserv Transaction Instruments and/or Fiserv Cards, which are used with physical Fiserv Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Secure Payment Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-

solutions/products-and-services/secure-payment-cards.html (last visited Oct. 20, 2023) ("Fiserv offers high-quality, cost-effective manufacturing, personalization and delivery services for a wide variety of cards including debit, credit, ATM, prepaid and gift cards; EMV® and contactless cards; photo cards; membership; and healthcare ID cards. Fulfillment options include central and in-branch issuance to meet immediate needs."); *EMV and Contactless EMV Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards/central-issuance/emv-chip-cards.html (last visited Oct. 20, 2023) (noting "Fiserv offers the industry's most complete, comprehensive and integrated EMV solution" including "processing EMV transactions on the Visa®, Mastercard® and Accel® debit networks" and "[c]ontactless EMV cards").

149. For example, Defendants infringe claim 1 of the '369 patent via their Accused Instrumentalities that implement EMV standards to provide processing, authorization, clearing, and/or settlement services to Defendants' card issuer customers; and/or for mobile and/or contactless payments, including Fiserv's contactless chip devices and technology provided to consumers via licenses with at least issuers, acquirers, chip vendors, and/or merchants. These services and devices and the technology utilized within them implement and perform methods pursuant to at least EMV standards, including without limitation standards incorporated into rules established by Fiserv and/or Mastercard. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Fiserv Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and/or use Fiserv's products, systems, devices and/or methods for the authorization and settlement of payment transactions. Defendants' mobile payments can be facilitated by Fiserv provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for

financial accounts associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards). Or such contactless payments can be facilitated by using contactless chips embedded on physical Fiserv Cards, for example, those provided, provisioned and/or issued by Fiserv. Defendants perform and/or direct and control infringement of the infringing products, systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, merchants, customers, consumers, and/or clients, for the authorization of and settlement of these mobile or contactless payments conducted using Fiserv Cards.

150. The Accused Instrumentalities implement the method of claim 1 of the '369 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff's allegations that each of those limitations is met. For example, the Accused Instrumentalities include a method implementing the steps: receiving, at a smartcard, a payment request for a transaction; determining, by the smartcard, a first payment system for processing at least a portion of the transaction, wherein said determining includes the smartcard querying payment directory information stored on the smartcard; and transmitting, by the smartcard, an identification of the first payment system to a point of service (POS) device, wherein the identification is usable by the POS device to transmit a first authorization request related to at least a portion of the transaction to the first payment system.

151. At a minimum, Defendants have known of the '369 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '369 patent. Defendants have known about the patent portfolio including the '369 patent, since at least on or around September 15, 2023, when, via email, a representative of 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, requested a phone call to discuss the licensing opportunity, and indicated Defendants would be provided with access to a data room containing information related to the American Express patent portfolio. On October 3, 2023, via email, DHG again requested a call to discuss the licensing opportunity on behalf of Plaintiff. On October 25, 2023, DHG again emailed Defendants on behalf of Plaintiff, requested a call to discuss the licensing opportunity, and provided Defendants with access to a data room with detailed portfolio information specific to Defendants. The data room included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '369 patent.

152. On information and belief, since at least each of the above-mentioned dates when Defendants were on notice of their infringement, Defendants have actively induced, under U.S.C. § 271(b), intermediaries, distributors, suppliers, partners, issuers, acquirers, merchants, customers, clients, consumers, and/or payment platforms (e.g., Samsung and Google mobile wallets) that distribute, make, purchase, offer to sell, sale, use, and/or service the Accused Instrumentalities to directly infringe one or more claims of the '369 patent by distributing, making, using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date and/or dates, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '369 patent.

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

use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards), providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction 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 without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., Fiserv.com; carat.Fiserv.com; developer.Fiserv.com; clover.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, in the United States. *See, e.g.*, *Moving*, FISERV, https://www.Fiserv.com/ (last visited Oct. 31, 2023) ("Every minute of the day, people, businesses and financial institutions are connecting with one another through payments and financial services technology from Fiserv.");

Run your business smarter, faster, easier, CLOVER, https://get.clover.com/clover-pos-systems (last visited Oct. 31, 2023) ("Want to learn more? Ready to get started? Contact the Clover sales team today."); *Welcome to Fiserv Merchant Services*, FISERV, https://merchants.Fiserv.com/en-ca/client-support/getting-started/ (last visited Oct. 31, 2023) ("1. Visit and enroll in businesstrack.com to view transaction and funding data as well as monthly statements. You can also use the tool to respond to cardholder disputes. 2. Read Your Payment Acceptance Guide for the latest information about accepting cards. 3. Read your Merchant Terms and Conditions for an outline of responsibilities, transactions, equipment, fees, charges, rules and regulations and much more."); *AuthHub*, FISERV, https://www.youtube.com/watch?v=I5vYNpUFOyo (last visited Oct. 31, 2023) ("Welcome to a smarter future with AuthHub from Fiserv.").

154. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients to directly infringe via Fiserv's Developer Studio, which is "a developer portal built by Fiserv to bring their financial technology products onto one platform." Developer Studio enables developers to access APIs and build and test Fiserv product integrations. *See Developer Studio*, FISERV, https://developer.Fiserv.com/support/docs/?path=docs/about-developer-studio.md&branch=main (last visited Oct. 20, 2023).

155. 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.

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

COUNT II

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

157. Plaintiff incorporates paragraphs 1 through 156 herein by reference.

158. 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.

159. 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.

160. 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.

161. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '039 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling,

and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., EMV contactless cards made by Fiserv and sold to financial institutions, Fiserv Transaction Devices, Fiserv Cards, Mastercard Transaction Instruments, and/or Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

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

163. Defendant FSI directly infringes the '039 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant FSS, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '039 patent under 35 U.S.C. § 271(a) by importing,

distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, FSS, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

164. 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/or consumers to perform one or more steps of the claimed methods of the '039 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) ("[A]n actor is liable for infringement under § 271(a) if it acts through an agent … or contracts with another to perform one or more steps of a claimed method."). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants' agreements with such third parties to provide access to Defendants' products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions

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

165. In addition to the liability arising from the Defendants' relationship with third parties, Defendants also directly infringe, individually and/or jointly, the '039 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards). On information and belief, Defendants design and develop payment applications for accounts used in connection with Fiserv Transaction Instruments and/or Fiserv Cards, which are used with physical Fiserv Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Secure Payment Cards*, FISERV,

https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards.html (last visited Oct. 20, 2023) ("Fiserv offers high-quality, cost-effective manufacturing, personalization and delivery services for a wide variety of cards including debit, credit, ATM, prepaid and gift cards; EMV® and contactless cards; photo cards; membership; and healthcare ID cards. Fulfillment options include central and in-branch issuance to meet immediate needs."); *EMV and Contactless EMV Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards/central-issuance/emv-chip-cards.html (last visited Oct. 20, 2023) (noting "Fiserv offers the industry's most complete, comprehensive and integrated EMV solution" including "processing EMV transactions on the Visa®, Mastercard® and Accel® debit networks" and "[c]ontactless EMV cards").

166. For example, Defendants infringe claim 1 of the '039 patent via their Accused Instrumentalities that implement EMV standards to provide tokenization, processing, authorization, clearing, and/or settlement services to Defendants' card issuer customers; and/or for mobile and/or contactless payments, including Fiserv's contactless chip devices and technology provided to consumers via licenses with at least issuers, acquirers, chip vendors, and/or merchants. These services and devices and the technology utilized within them implement and perform methods pursuant to at least EMV standards, including without limitation standards incorporated into rules established by Fiserv and/or Mastercard. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Fiserv Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and/or use Fiserv's products, systems, devices and/or methods for the authorization and settlement of payment transactions. Defendants' mobile payments can be facilitated by Fiserv provisioning

mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards). Or such contactless payments can be facilitated by using contactless chips embedded on physical Fiserv Cards, for example, those provided, provisioned and/or issued by Fiserv. Defendants perform and/or direct and control infringement of the infringing products, systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, merchants, customers, consumers, and/or clients, for the authorization of and settlement of these mobile or contactless payments conducted using Fiserv Cards.

167. The Accused Instrumentalities implement the method of claim 1 of the '039 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff's allegations that each of those limitations is met. For example, the Accused Instrumentalities include a method for facilitating a transaction at a first point of sale (POS) device, said method implementing the steps: sending a query from a computer based system to a payment system directory, wherein the query includes a request to locate a candidate payment system that is configured to process at least a portion of said transaction, wherein said candidate payment system is configured to receive payment information related to said transaction at said first POS device; causing, by said computer based system, a payment authorization request related to said transaction to be transmitted from said first POS device to said candidate payment system; receiving, by said computer based system, payment authorization from said candidate payment system; and sending, by said computer based system, said payment authorization to said first POS device.

168. At a minimum, Defendants have known of the '039 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants

with notice of Plaintiff's American Express patent portfolio and the '039 patent. Defendants have known about the patent portfolio including the '039 patent, since at least on or around September 15, 2023, when, via email, a representative of 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, requested a phone call to discuss the licensing opportunity, and indicated Defendants would be provided with access to a data room containing information related to the American Express patent portfolio. On October 3, 2023, via email, DHG again requested a call to discuss the licensing opportunity on behalf of Plaintiff. On October 25, 2023, DHG again emailed Defendants on behalf of Plaintiff, requested a call to discuss the licensing opportunity, and provided Defendants with access to a data room with detailed portfolio information specific to Defendants. The data room included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '039 patent.

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

170. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards), providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction 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 without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., Fiserv.com; carat.Fiserv.com; developer.Fiserv.com; clover.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems,

methods, and services to licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, in the United States. *See, e.g.*, *Moving*, FISERV, https://www.Fiserv.com/ (last visited Oct. 31, 2023) ("Every minute of the day, people, businesses and financial institutions are connecting with one another through payments and financial services technology from Fiserv."); *Run your business smarter, faster, easier*, CLOVER, https://get.clover.com/clover-pos-systems (last visited Oct. 31, 2023) ("Want to learn more? Ready to get started? Contact the Clover sales team today."); *Welcome to Fiserv Merchant Services*, FISERV, https://merchants.Fiserv.com/en-ca/client-support/getting-started/ (last visited Oct. 31, 2023) ("1. Visit and enroll in businesstrack.com to view transaction and funding data as well as monthly statements. You can also use the tool to respond to cardholder disputes. 2. Read Your Payment Acceptance Guide for the latest information about accepting cards. 3. Read your Merchant Terms and Conditions for an outline of responsibilities, transactions, equipment, fees, charges, rules and regulations and much more."); *AuthHub*, FISERV, https://www.youtube.com/watch?v=I5vYNpUFOyo (last visited Oct. 31, 2023) ("Welcome to a smarter future with AuthHub from Fiserv.").

171. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients to directly infringe via Fiserv's Developer Studio, which is "a developer portal built by Fiserv to bring their financial technology products onto one platform." Developer Studio enables developers to access APIs and build and test Fiserv product integrations. *See Developer Studio*, FISERV, https://developer.Fiserv.com/support/docs/?path=docs/about-developer-studio.md&branch=main (last visited Oct. 20, 2023).

172. 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.

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

COUNT III

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

174. Plaintiff incorporates paragraphs 1 through 173 herein by reference.

175. 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.

176. 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.

177. 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.

178. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '509 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., EMV contactless cards made by Fiserv and sold to financial institutions, Fiserv Transaction Devices, Fiserv Cards, Mastercard Transaction Instruments, and/or Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

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

180. Defendant FSI directly infringes the '509 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant FSS, for example, by

importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '509 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, FSS, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

181. 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/or consumers to perform one or more steps of the claimed methods of the '509 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) ("[A]n actor is liable for infringement under § 271(a) if it acts through an agent … or contracts with another to perform one or more steps of a claimed method."). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation,

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

182. In addition to the liability arising from the Defendants' relationship with third parties, Defendants also directly infringe, individually and/or jointly, the '509 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards). On information and belief, Defendants design and develop payment applications for accounts used in connection with Fiserv

Transaction Instruments and/or Fiserv Cards, which are used with physical Fiserv Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Secure Payment Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards.html (last visited Oct. 20, 2023) ("Fiserv offers high-quality, cost-effective manufacturing, personalization and delivery services for a wide variety of cards including debit, credit, ATM, prepaid and gift cards; EMV® and contactless cards; photo cards; membership; and healthcare ID cards. Fulfillment options include central and in-branch issuance to meet immediate needs."); *EMV and Contactless EMV Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards/central-issuance/emv-chip-cards.html (last visited Oct. 20, 2023) (noting "Fiserv offers the industry's most complete, comprehensive and integrated EMV solution" including "processing EMV transactions on the Visa®, Mastercard® and Accel® debit networks" and "[c]ontactless EMV cards").

183. For example, Defendants infringe claim 1 of the '509 patent via their Accused Instrumentalities that implement EMV standards to provide tokenization, processing, authorization, clearing, and/or settlement services to Defendants' card issuer customers; and/or for mobile and/or contactless payments, including Fiserv's contactless chip devices and technology provided to consumers via licenses with at least issuers, acquirers, chip vendors, and/or merchants. These services and devices and the technology utilized within them implement and perform methods pursuant to at least EMV standards, including without limitation standards incorporated into rules established by Fiserv and/or Mastercard. Defendants, for example, by their own actions and/or

direction and control of third parties, provide to consumers Fiserv Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and/or use Fiserv's products, systems, devices and/or methods for the authorization and settlement of payment transactions. Defendants' mobile payments can be facilitated by Fiserv provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards). Defendants perform and/or direct and control infringement of the infringing products, systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, merchants, customers, consumers, and/or clients, for the authorization of and settlement of these mobile or contactless payments conducted using Fiserv Cards.

184. 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.

185. At a minimum, Defendants have known of the '509 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '509 patent. Defendants have known about the patent portfolio including the '509 patent, since at least on or around September 15, 2023, when, via email, a representative of 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, requested a phone call to discuss the licensing opportunity, and indicated Defendants would be provided with access to a data room containing information related to the American Express patent portfolio. On October 3, 2023, via email, DHG again requested a call to discuss the licensing opportunity on behalf of Plaintiff. On October 25, 2023, DHG again emailed Defendants on behalf of Plaintiff, requested a call to discuss the licensing opportunity, and provided Defendants with access to a data room with detailed portfolio information specific to Defendants. The data room included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including, by no later October 31, 2023, at least one claim of the '509 patent.

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

directly infringe one or more claims of the '509 patent by distributing, making, using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date and/or dates, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '509 patent.

187. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards), providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction 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 without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing Defendants' mobile and contactless payment features in the

Accused Instrumentalities; providing websites (e.g., Fiserv.com; carat.Fiserv.com; developer.Fiserv.com; clover.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, in the United States. *See, e.g.*, *Moving*, FISERV, https://www.Fiserv.com/ (last visited Oct. 31, 2023) ("Every minute of the day, people, businesses and financial institutions are connecting with one another through payments and financial services technology from Fiserv."); *Run your business smarter, faster, easier*, CLOVER, https://get.clover.com/clover-pos-systems (last visited Oct. 31, 2023) ("Want to learn more? Ready to get started? Contact the Clover sales team today."); *Welcome to Fiserv Merchant Services*, FISERV, https://merchants.Fiserv.com/en-ca/client-support/getting-started/ (last visited Oct. 31, 2023) ("1. Visit and enroll in businesstrack.com to view transaction and funding data as well as monthly statements. You can also use the tool to respond to cardholder disputes. 2. Read Your Payment Acceptance Guide for the latest information about accepting cards. 3. Read your Merchant Terms and Conditions for an outline of responsibilities, transactions, equipment, fees, charges, rules and regulations and much more."); *AuthHub*, FISERV, https://www.youtube.com/watch?v=I5vYNpUFOyo (last visited Oct. 31, 2023) ("Welcome to a smarter future with AuthHub from Fiserv.").

188. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients to directly infringe via Fiserv's Developer Studio, which is "a developer portal built by Fiserv to bring their financial technology products onto one platform." Developer Studio enables developers to access APIs and build and test Fiserv product integrations.

See Developer Studio, FISERV, https://developer.Fiserv.com/support/docs/?path=docs/about-developer-studio.md&branch=main (last visited Oct. 20, 2023).

189. 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.

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

COUNT IV

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

191. Plaintiff incorporates paragraphs 1 through 190 herein by reference.

192. 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.

193. 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.

194. 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.

195. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '671 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., EMV contactless cards made by Fiserv and sold to financial institutions, Fiserv Transaction Devices, Fiserv Cards, Mastercard Transaction Instruments, and/or Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

196. Defendants directly infringe, individually and/or jointly with at least one other entity, the '671 patent via 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities, their components, and/or products

and processes containing the same that incorporate the fundamental technologies covered by the '671 patent for and/or to, for example, its alter egos, agents, intermediaries, licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients. Defendants' infringement involves Defendants' own action and/or direction and control of third parties' actions.

197. Defendant FSI directly infringes the '671 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant FSS, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '671 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, FSS provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

198. 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/or consumers to perform one or more steps of the claimed methods of the '671 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) ("[A]n actor is liable for

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

199. In addition to the liability arising from the Defendants' relationship with third parties, Defendants also directly infringe, individually and/or jointly, the '671 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards). On information and belief, Defendants design and develop payment applications for accounts used in connection with Fiserv Transaction Instruments and/or Fiserv Cards, which are used with physical Fiserv Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Secure Payment Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards.html (last visited Oct. 20, 2023) ("Fiserv offers high-quality, cost-effective manufacturing, personalization and delivery services for a wide variety of cards including debit, credit, ATM, prepaid and gift cards; EMV® and contactless cards; photo cards; membership; and healthcare ID cards. Fulfillment options include central and in-branch issuance to meet immediate needs."); *EMV and Contactless EMV Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards/central-issuance/emv-chip-cards.html (last visited Oct. 20, 2023) (noting "Fiserv offers the industry's most complete, comprehensive and integrated EMV solution" including "processing EMV transactions on the Visa®, Mastercard® and Accel® debit networks" and "[c]ontactless EMV cards").

200. For example, Defendants infringe claim 1 of the '671 patent via their Accused Instrumentalities that implement EMV standards to provide tokenization, processing, authorization,

clearing, and/or settlement services to Defendants' card issuer customers; and/or for mobile and/or contactless payments, including Fiserv's contactless chip devices and technology provided to consumers via licenses with at least issuers, acquirers, chip vendors, and/or merchants. These services and devices and the technology utilized within them implement and perform methods pursuant to at least EMV standards, including without limitation standards incorporated into rules established by Fiserv and/or Mastercard. Defendants, for example, by their own actions and/or direction and control of third parties, provide to consumers Fiserv Cards that support, via contactless chip devices and technology, mobile or contactless payments that conform to the EMV standards and/or use Fiserv's products, systems, devices and/or methods for the authorization and settlement of payment transactions. Defendants' mobile payments can be facilitated by Fiserv provisioning mobile wallets such as Google Pay and Samsung Pay with contactless payment functions for financial accounts associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards). Defendants perform and/or direct and control infringement of the infringing products, systems and methods, including via their alter egos, agents, intermediaries, licensees, issuers, acquirers, partners, merchants, customers, consumers, and/or clients, for the authorization of and settlement of these mobile or contactless payments conducted using Fiserv Cards.

201. 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.

202. At a minimum, Defendants have known of the '671 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '671 patent. Defendants have known about the patent portfolio including the '671 patent, since at least on or around September 15, 2023, when, via email, a representative of 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, requested a phone call to discuss the licensing opportunity, and indicated Defendants would be provided with access to a data room containing information related to the American Express patent portfolio. On October 3, 2023, via email, DHG again requested a call to discuss the licensing opportunity on behalf of Plaintiff. On October 25, 2023, DHG again emailed Defendants on behalf of Plaintiff, requested a call to discuss the licensing opportunity, and provided Defendants with access to a data room with detailed portfolio information specific to Defendants. The data room included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '671 patent.

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

204. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards), providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction 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 without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., Fiserv.com; carat.Fiserv.com; developer.Fiserv.com; clover.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, in the United States. *See, e.g.*, *Moving*, FISERV, https://www.Fiserv.com/ (last visited Oct. 31, 2023) ("Every minute of the day, people, businesses and financial institutions are connecting with one another through payments and financial services technology from Fiserv."); *Run your business smarter, faster, easier*, CLOVER, https://get.clover.com/clover-pos-systems (last visited Oct. 31, 2023) ("Want to learn more? Ready to get started? Contact the Clover sales team today."); *Welcome to Fiserv Merchant Services*, FISERV, https://merchants.Fiserv.com/en-ca/client-support/getting-started/ (last visited Oct. 31, 2023) ("1. Visit and enroll in businesstrack.com to view transaction and funding data as well as monthly statements. You can also use the tool to respond to cardholder disputes. 2. Read Your Payment Acceptance Guide for the latest information about accepting cards. 3. Read your Merchant Terms and Conditions for an outline of responsibilities, transactions, equipment, fees, charges, rules and regulations and much more."); *AuthHub*, FISERV, https://www.youtube.com/watch?v=I5vYNpUFOyo (last visited Oct. 31, 2023) ("Welcome to a smarter future with AuthHub from Fiserv.").

205. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients to directly infringe via Fiserv's Developer Studio, which is "a developer portal built by Fiserv to bring their financial technology products onto one platform." Developer Studio enables developers to access APIs and build and test Fiserv product integrations. *See Developer Studio*, FISERV, https://developer.Fiserv.com/support/docs/?path=docs/about-developer-studio.md&branch=main (last visited Oct. 20, 2023).

206. 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.

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

COUNT V

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

208. Plaintiff incorporates paragraphs 1 through 207 herein by reference.

209. 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.

210. 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.

211. 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.

212. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '985 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., EMV contactless cards made by Fiserv and sold to financial institutions, Fiserv Transaction Devices, Fiserv Cards, Mastercard Transaction Instruments, and/or Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

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

214. Defendant FSI directly infringes the '985 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant FSS, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '985 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, FSS, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

215. 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/or consumers to perform one or more steps of the claimed methods of the '985 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) ("[A]n actor is liable for infringement under § 271(a) if it acts through an agent … or contracts with another to perform one or more steps of a claimed method."). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants' agreements with such third parties to provide access to Defendants' products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants' products, systems, methods, and/or services, for example, Fiserv Cards and/or Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for contactless and mobile payments, as a condition of each third party's access to, use of, and/or participation in such products, systems, methods, and/or services. *See id*. ("[L]iability under § 271(a) can also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance."). The activities of each third party (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) in providing services to holders of Defendants' Fiserv Transaction Instruments, cardholders of Defendants'

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

216. In addition to the liability arising from the Defendants' relationship with third parties, Defendants also directly infringe, individually and/or jointly, the '985 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards). On information and belief, Defendants design and develop payment applications for accounts used in connection with Fiserv Transaction Instruments and/or Fiserv Cards used with digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Secure Payment Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards.html (last visited Oct. 20, 2023) ("Fiserv offers high-quality, cost-effective manufacturing, personalization and delivery services for a wide variety of cards including debit, credit, ATM, prepaid and gift cards; EMV® and contactless cards; photo cards; membership; and healthcare ID cards. Fulfillment options include central and in-branch issuance to meet immediate needs."); *EMV and Contactless EMV Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards/central-issuance/emv-chip-cards.html (last visited Oct. 20, 2023) (noting "Fiserv offers the industry's most complete, comprehensive and integrated EMV solution" including "processing EMV transactions on the Visa®, Mastercard® and Accel® debit networks" and "[c]ontactless EMV cards").

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

218. The Accused Instrumentalities implement the method of claim 1 of the '985 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Instrumentalities include a method implementing the steps: receiving, by a computer system, an authorization request from a merchant for a transaction, wherein the authorization request indicates

that the transaction has been initiated using a first transaction instrument corresponding to a user; based on the authorization request, the computer system determining a second transaction instrument corresponding to the user; the computer system analyzing transaction data for the transaction, wherein the analyzing includes determining whether the transaction data at least partially corresponds to particular transaction data associated with the second transaction instrument; and based on said analyzing, the computer system transmitting a response to the authorization request to the merchant, wherein the response indicates whether the transaction is authorized.

219. At a minimum, Defendants have known of the '985 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '985 patent. Defendants have known about the patent portfolio including the '985 patent, since at least on or around September 15, 2023, when, via email, a representative of 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, requested a phone call to discuss the licensing opportunity, and indicated Defendants would be provided with access to a data room containing information related to the American Express patent portfolio. On October 3, 2023, via email, DHG again requested a call to discuss the licensing opportunity on behalf of Plaintiff. On October 25, 2023, DHG again emailed Defendants on behalf of Plaintiff, requested a call to discuss the licensing opportunity, and provided Defendants with access to a data room with detailed portfolio information specific to Defendants. The data room included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '985 patent.

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

221. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards), providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction 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 without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., Fiserv.com; carat.Fiserv.com; developer.Fiserv.com; clover.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, in the United States. *See, e.g.*, *Moving*, FISERV, https://www.Fiserv.com/ (last visited Oct. 31, 2023) ("Every minute of the day, people, businesses and financial institutions are connecting with one another through payments and financial services technology from Fiserv."); *Run your business smarter, faster, easier*, CLOVER, https://get.clover.com/clover-pos-systems (last visited Oct. 31, 2023) ("Want to learn more? Ready to get started? Contact the Clover sales team today."); *Welcome to Fiserv Merchant Services*, FISERV, https://merchants.Fiserv.com/en-ca/client-support/getting-started/ (last visited Oct. 31, 2023) ("1. Visit and enroll in businesstrack.com to view transaction and funding data as well as monthly statements. You can also use the tool to respond to cardholder disputes. 2. Read Your Payment Acceptance Guide for the latest information about accepting cards. 3. Read your Merchant Terms and Conditions for an outline of responsibilities, transactions, equipment, fees, charges, rules and regulations and much more."); *AuthHub*, FISERV, https://www.youtube.com/watch?v=I5vYNpUFOyo (last visited Oct. 31, 2023) ("Welcome to a smarter future with AuthHub from Fiserv.").

222. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients to directly infringe via Fiserv's Developer Studio, which is "a developer portal built by Fiserv to bring their financial technology products onto one platform." Developer Studio enables developers to access APIs and build and test Fiserv product integrations. *See Developer Studio*, FISERV, https://developer.Fiserv.com/support/docs/?path=docs/about-developer-studio.md&branch=main (last visited Oct. 20, 2023).

223. 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.

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

COUNT VI

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

225. Plaintiff incorporates paragraphs 1 through 224 herein by reference.

226. 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.

227. 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.

228. 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.

229. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '756 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., EMV contactless cards made by Fiserv and sold to financial institutions, Fiserv Transaction Devices, Fiserv Cards, Mastercard Transaction Instruments, and/or Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, point of sale, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

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

231. Defendant FSI directly infringes the '756 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant FSS, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '756 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, FSS, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants' point of sale products (e.g., Clover POS terminals), as used with contactless chips, mobile payments, and digital wallets.

232. 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/or consumers to perform one or more steps of the claimed methods of the '756 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) ("[A]n actor is liable for infringement under § 271(a) if it acts through an agent … or contracts with another to perform one or more steps of a claimed method."). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, payment acceptance, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants' agreements with such third parties to provide access to Defendants' products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants' products, systems, methods, and/or services, for example, Fiserv Cards and/or Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for contactless and mobile payments, as a condition of each third party's access to, use of, and/or participation in such products, systems, methods, and/or services. *See id*. ("[L]iability under § 271(a) can also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance."). The activities of each third party (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) in providing services to holders of Defendants' Fiserv Transaction Instruments, cardholders of

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

233. In addition to the liability arising from the Defendants' relationship with third parties, Defendants also directly infringe, individually and/or jointly, the '756 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments), point-of-sale terminals, and/or Fiserv Cards (e.g., Mastercard Cards). On information and belief, Defendants design and develop payment applications for accounts used in connection with Fiserv Transaction Instruments and/or Fiserv Cards, which are used with physical Fiserv Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Secure Payment Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards.html (last visited Oct. 20, 2023) ("Fiserv offers high-quality, cost-effective manufacturing, personalization and delivery services for a wide variety of cards including debit, credit, ATM, prepaid and gift cards; EMV® and contactless cards; photo cards; membership; and healthcare ID cards. Fulfillment options include central and in-branch issuance to meet immediate needs."); *EMV and Contactless EMV Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards/central-issuance/emv-chip-cards.html (last visited Oct. 20, 2023) (noting "Fiserv offers the industry's most complete, comprehensive and

integrated EMV solution" including "processing EMV transactions on the Visa®, Mastercard® and Accel® debit networks" and "[c]ontactless EMV cards").

234. For example, Defendants infringe claim 1 of the '756 patent via their Accused Instrumentalities that implement EMV standards to provide EMV complaint point of sale systems and devices (e.g., Clover systems) that perform a method of securing a transaction utilizing a proximity integrated circuit transaction device.

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

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

236. At a minimum, Defendants have known of the '756 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '756 patent. Defendants have known about the patent portfolio including the '756 patent, since at least on or around September 15, 2023, when, via email, a representative of 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, requested a phone call to discuss the licensing opportunity, and indicated Defendants would be provided with access to a data room containing information related to the American Express patent portfolio. On October 3, 2023, via email, DHG again requested a call to discuss the licensing opportunity on behalf of Plaintiff. On October 25, 2023, DHG again emailed Defendants on behalf of Plaintiff, requested a call to discuss the licensing opportunity, and provided Defendants with access to a data room with detailed portfolio information specific to Defendants. The data room included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '756 patent.

237. On information and belief, since at least each of the above-mentioned dates when Defendants were on notice of their infringement, Defendants have actively induced, under U.S.C.

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

238. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards), providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction 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 without limitation via

vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., Fiserv.com; carat.Fiserv.com; developer.Fiserv.com; clover.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, in the United States. *See, e.g.*, *Moving*, FISERV, https://www.Fiserv.com/ (last visited Oct. 31, 2023) ("Every minute of the day, people, businesses and financial institutions are connecting with one another through payments and financial services technology from Fiserv."); *Run your business smarter, faster, easier*, CLOVER, https://get.clover.com/clover-pos-systems (last visited Oct. 31, 2023) ("Want to learn more? Ready to get started? Contact the Clover sales team today."); *Welcome to Fiserv Merchant Services*, FISERV, https://merchants.Fiserv.com/en-ca/client-support/getting-started/ (last visited Oct. 31, 2023) ("1. Visit and enroll in businesstrack.com to view transaction and funding data as well as monthly statements. You can also use the tool to respond to cardholder disputes. 2. Read Your Payment Acceptance Guide for the latest information about accepting cards. 3. Read your Merchant Terms and Conditions for an outline of responsibilities, transactions, equipment, fees, charges, rules and regulations and much more."); *AuthHub*, FISERV, https://www.youtube.com/watch?v=I5vYNpUFOyo (last visited Oct. 31, 2023) ("Welcome to a smarter future with AuthHub from Fiserv.").

239. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients to directly infringe via Fiserv's Developer Studio, which is "a

developer portal built by Fiserv to bring their financial technology products onto one platform." Developer Studio enables developers to access APIs and build and test Fiserv product integrations. *See Developer Studio*, FISERV, https://developer.Fiserv.com/support/docs/?path=docs/about-developer-studio.md&branch=main (last visited Oct. 20, 2023).

240. 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.

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

COUNT VII

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

242. Plaintiff incorporates paragraphs 1 through 241 herein by reference.

243. 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.

244. 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.

245. 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.

246. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the ‘750 patent, which includes Defendants’ offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., EMV contactless cards made by Fiserv and sold to financial institutions, Fiserv Transaction Devices, Fiserv Cards, Mastercard Transaction Instruments, and/or Mastercard Cards) and related products, methods, and/or services for Defendants’ licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, including Defendants’ issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants’ payment processing, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants’ card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

247. Defendants directly infringe, individually and/or jointly with at least one other entity, the ‘750 patent via 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities, their components, and/or products

and processes containing the same that incorporate the fundamental technologies covered by the '750 patent for and/or to, for example, its alter egos, agents, intermediaries, licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients. Defendants' infringement involves Defendants' own action and/or direction and control of third parties' actions.

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

249. 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/or consumers to perform one or more steps of the claimed methods of the '750 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) ("[A]n actor is liable for

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

250. In addition to the liability arising from the Defendants' relationship with third parties, Defendants also directly infringe, individually and/or jointly, the '750 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards). On information and belief, Defendants design and develop payment applications for accounts used in connection with Fiserv Transaction Instruments and/or Fiserv Cards, which are used with physical Fiserv Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Secure Payment Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards.html (last visited Oct. 20, 2023) ("Fiserv offers high-quality, cost-effective manufacturing, personalization and delivery services for a wide variety of cards including debit, credit, ATM, prepaid and gift cards; EMV® and contactless cards; photo cards; membership; and healthcare ID cards. Fulfillment options include central and in-branch issuance to meet immediate needs."); *EMV and Contactless EMV Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards/central-issuance/emv-chip-cards.html (last visited Oct. 20, 2023) (noting "Fiserv offers the industry's most complete, comprehensive and integrated EMV solution" including "processing EMV transactions on the Visa®, Mastercard® and Accel® debit networks" and "[c]ontactless EMV cards").

251. For example, Defendants infringe at least claim 1 of the '750 patent via their Accused Instrumentalities that implement EMV standards to provide EMV complaint point of sale

systems and devices (e.g., Clover systems) that perform a method of securing a RFID transactions with mobile wallets (e.g., Google Pay and/or Samsung Pay) using host card emulation.

252. 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.

253. At a minimum, Defendants have known of the '750 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '750 patent. Defendants have known about the patent portfolio including the '750 patent, since at least on or around September 15, 2023, when, via email, a representative of 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, requested a phone call to discuss the licensing opportunity, and indicated Defendants would be provided with access to a data room containing information related to the American Express patent portfolio. On October 3, 2023, via email, DHG again requested a call to discuss the licensing

opportunity on behalf of Plaintiff. On October 25, 2023, DHG again emailed Defendants on behalf of Plaintiff, requested a call to discuss the licensing opportunity, and provided Defendants with access to a data room with detailed portfolio information specific to Defendants. The data room included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '750 patent.

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

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

Cards), providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction 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 without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., Fiserv.com; carat.Fiserv.com; developer.Fiserv.com; clover.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, in the United States. *See, e.g.*, *Moving*, FISERV, https://www.Fiserv.com/ (last visited Oct. 31, 2023) ("Every minute of the day, people, businesses and financial institutions are connecting with one another through payments and financial services technology from Fiserv."); *Run your business smarter, faster, easier*, CLOVER, https://get.clover.com/clover-pos-systems (last visited Oct. 31, 2023) ("Want to learn more? Ready to get started? Contact the Clover sales team today."); *Welcome to Fiserv Merchant Services*, FISERV, https://merchants.Fiserv.com/en-ca/client-support/getting-started/ (last visited Oct. 31, 2023) ("1. Visit and enroll in businesstrack.com to view transaction and funding data as well as monthly statements. You can also use the tool to

respond to cardholder disputes. 2. Read Your Payment Acceptance Guide for the latest information about accepting cards. 3. Read your Merchant Terms and Conditions for an outline of responsibilities, transactions, equipment, fees, charges, rules and regulations and much more."); *AuthHub*, FISERV, https://www.youtube.com/watch?v=I5vYNpUFOyo (last visited Oct. 31, 2023) ("Welcome to a smarter future with AuthHub from Fiserv.").

256. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients to directly infringe via Fiserv's Developer Studio, which is "a developer portal built by Fiserv to bring their financial technology products onto one platform." Developer Studio enables developers to access APIs and build and test Fiserv product integrations. *See Developer Studio*, FISERV, https://developer.Fiserv.com/support/docs/?path=docs/about-developer-studio.md&branch=main (last visited Oct. 20, 2023).

257. 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.

258. 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. 7,312,707)

259. Plaintiff incorporates paragraphs 1 through 258 herein by reference.

260. Plaintiff is the assignee of the '707 patent, entitled "System and Method for Authenticating a RF Transaction Using a Transaction Account Routing Number," with ownership of all substantial rights in the '707 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

261. The '707 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '707 patent issued from U.S. Patent Application No. 10/905,006.

262. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '707 patent in this District and elsewhere in Texas and the United States.

263. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '707 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., EMV contactless cards made by Fiserv and sold to financial institutions, Fiserv Transaction Devices, Fiserv Cards, Mastercard Transaction Instruments, and/or Mastercard Cards) and related products, methods, and/or services for

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

264. Defendants directly infringe, individually and/or jointly with at least one other entity, the '707 patent via 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '707 patent for and/or to, for example, its alter egos, agents, intermediaries, licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients. Defendants' infringement involves Defendants' own action and/or direction and control of third parties' actions.

265. Defendant FSI directly infringes the '707 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant FSS, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '707 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, FSS, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients including without limitation

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

266. 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/or consumers to perform one or more steps of the claimed methods of the '707 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) ("[A]n actor is liable for infringement under § 271(a) if it acts through an agent … or contracts with another to perform one or more steps of a claimed method."). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants' agreements with such third parties to provide access to Defendants' products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants' products, systems, methods, and/or services, for example, Fiserv Cards and/or Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for contactless and mobile payments, as a condition of each third party's access to, use of, and/or participation in such products, systems, methods, and/or services. *See id*.

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

267. In addition to the liability arising from the Defendants' relationship with third parties, Defendants also directly infringe, individually and/or jointly, the '707 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards). On information and belief, Defendants design and develop payment applications for accounts used in connection with Fiserv Transaction Instruments and/or Fiserv Cards, which are used with physical Fiserv Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks) to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Secure Payment Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards.html (last visited Oct. 20, 2023) ("Fiserv offers high-quality, cost-effective manufacturing, personalization and delivery services for a wide variety of cards including debit, credit, ATM, prepaid and gift cards; EMV® and contactless cards;

photo cards; membership; and healthcare ID cards. Fulfillment options include central and in-branch issuance to meet immediate needs."); *EMV and Contactless EMV Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards/central-issuance/emv-chip-cards.html (last visited Oct. 20, 2023) (noting "Fiserv offers the industry's most complete, comprehensive and integrated EMV solution" including "processing EMV transactions on the Visa®, Mastercard® and Accel® debit networks" and "[c]ontactless EMV cards").

268. For example, Defendants infringe claim 1 of the '707 patent via their Accused Instrumentalities that implement EMV standards to provide EMV complaint point of sale systems and devices (e.g., Clover systems) that perform a method of securing a RFID transactions with mobile wallets (e.g., Google Pay and/or Samsung Pay) using host card emulation.

269. The Accused Instrumentalities implement the method of claim 1 of the '707 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 securing a radio frequency identification (RFID) transaction. The method implements the steps: transmitting a random number from an RFID reader to an RFID transaction device; creating, in the RFID transaction device, an RFID transaction device authentication tag using at least (a) the random number, (b) a routing number associated with a transaction account, and (c) a stored counter value; transmitting the RFID transaction device authentication tag to the RFID reader; incrementing the stored counter value in the RFID transaction device; transmitting a transaction request for verification, the transaction request being formed from at least the RFID transaction device authentication tag and the stored counter value; and processing

the transaction request, wherein at least one of the RFID transaction device authentication tag and the stored counter value is verified.

270. At a minimum, Defendants have known of the '707 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '707 patent. Defendants have known about the patent portfolio including the '707 patent, since at least on or around September 15, 2023, when, via email, a representative of 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, requested a phone call to discuss the licensing opportunity, and indicated Defendants would be provided with access to a data room containing information related to the American Express patent portfolio. On October 3, 2023, via email, DHG again requested a call to discuss the licensing opportunity on behalf of Plaintiff. On October 25, 2023, DHG again emailed Defendants on behalf of Plaintiff, requested a call to discuss the licensing opportunity, and provided Defendants with access to a data room with detailed portfolio information specific to Defendants. The data room included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '707 patent.

271. On information and belief, since at least each of the above-mentioned dates when Defendants were on notice of their infringement, Defendants have actively induced, under U.S.C. § 271(b), intermediaries, distributors, suppliers, partners, issuers, acquirers, merchants, customers, clients, consumers, and/or payment platforms (e.g., Samsung and Google mobile wallets) that distribute, make, purchase, offer to sell, sale, use, and/or service the Accused Instrumentalities to directly infringe one or more claims of the '707 patent by distributing, making, using, offering for

sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date and/or dates, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '707 patent.

272. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards), providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction 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 without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., Fiserv.com; carat.Fiserv.com;

developer.Fiserv.com; clover.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, in the United States. *See, e.g.*, *Moving*, FISERV, https://www.Fiserv.com/ (last visited Oct. 31, 2023) ("Every minute of the day, people, businesses and financial institutions are connecting with one another through payments and financial services technology from Fiserv."); *Run your business smarter, faster, easier*, CLOVER, https://get.clover.com/clover-pos-systems (last visited Oct. 31, 2023) ("Want to learn more? Ready to get started? Contact the Clover sales team today."); *Welcome to Fiserv Merchant Services*, FISERV, https://merchants.Fiserv.com/en-ca/client-support/getting-started/ (last visited Oct. 31, 2023) ("1. Visit and enroll in businesstrack.com to view transaction and funding data as well as monthly statements. You can also use the tool to respond to cardholder disputes. 2. Read Your Payment Acceptance Guide for the latest information about accepting cards. 3. Read your Merchant Terms and Conditions for an outline of responsibilities, transactions, equipment, fees, charges, rules and regulations and much more."); *AuthHub*, FISERV, https://www.youtube.com/watch?v=I5vYNpUFOyo (last visited Oct. 31, 2023) ("Welcome to a smarter future with AuthHub from Fiserv.").

273. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients to directly infringe via Fiserv's Developer Studio, which is "a developer portal built by Fiserv to bring their financial technology products onto one platform." Developer Studio enables developers to access APIs and build and test Fiserv product integrations. *See Developer Studio*, FISERV, https://developer.Fiserv.com/support/docs/?path=docs/about-developer-studio.md&branch=main (last visited Oct. 20, 2023).

274. On information and belief, despite having knowledge of the '707 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '707 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Defendants' infringing activities relative to the '707 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.

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

COUNT IX

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

276. Plaintiff incorporates paragraphs 1 through 275 herein by reference.

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

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

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

280. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '207 patent, which includes Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with card-not-present transactions (e.g., transactions implementing EMV 3D Secure) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in card-not-present transactions.

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

282. Defendant FSI directly infringes the '207 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant FSS, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants' divisions, subsidiaries, partners, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '207 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, FSS, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in card-not-present transactions.

283. 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/or consumers to perform one or more steps of the claimed methods of the '207 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) ("[A]n actor is liable for infringement under § 271(a) if it acts through an agent … or contracts with another to perform one or more steps of a claimed method."). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless

chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants' agreements with such third parties to provide access to Defendants' products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants' products, systems, methods, and/or services, for example, Fiserv Cards and/or Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for securing card-not-present transactions, as a condition of each third party's access to, use of, and/or participation in such products, systems, methods, and/or services. *See id*. ("[L]iability under § 271(a) can also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance."). The activities of each third party (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) in providing services to holders of Defendants' Fiserv Transaction Instruments, cardholders of Defendants' Fiserv Cards, and users of other products, systems, methods, and/or services are thus attributed to the Defendants such that Defendants become the "single actor" chargeable with the direct infringement.

284. In addition to the liability arising from the Defendants' relationship with third parties, Defendants also directly infringe, individually and/or jointly, the '207 patent via their own provision of products, systems, methods, and services that implement the EMV 3D Secure standards for securing card-not-present transactions. On information and belief, Defendants design

and develop software and services used in connection with Fiserv 3D Secure product offerings. These products are offered to merchants that accept payments through online portals.

285. For example, Defendants infringe claim 1 of the '207 patent via their Accused Instrumentalities that implement EMV standards for processing services in connection with commercial transactions that implement the EMV 3-D Secure specification; payment processing for merchant customers; and/or gateway services for merchant customers.

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

287. At a minimum, Defendants have known of the '207 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants

with notice of Plaintiff's American Express patent portfolio and the '207 patent. Defendants have known about the patent portfolio including the '207 patent, since at least on or around September 15, 2023, when, via email, a representative of 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, requested a phone call to discuss the licensing opportunity, and indicated Defendants would be provided with access to a data room containing information related to the American Express patent portfolio. On October 3, 2023, via email, DHG again requested a call to discuss the licensing opportunity on behalf of Plaintiff. On October 25, 2023, DHG again emailed Defendants on behalf of Plaintiff, requested a call to discuss the licensing opportunity, and provided Defendants with access to a data room with detailed portfolio information specific to Defendants. The data room included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '207 patent.

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

289. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards), providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction 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 without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., Fiserv.com; carat.Fiserv.com; developer.Fiserv.com; clover.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems,

methods, and services to licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, in the United States. *See, e.g.*, *Moving*, FISERV, https://www.Fiserv.com/ (last visited Oct. 31, 2023) ("Every minute of the day, people, businesses and financial institutions are connecting with one another through payments and financial services technology from Fiserv."); *Run your business smarter, faster, easier*, CLOVER, https://get.clover.com/clover-pos-systems (last visited Oct. 31, 2023) ("Want to learn more? Ready to get started? Contact the Clover sales team today."); *Welcome to Fiserv Merchant Services*, FISERV, https://merchants.Fiserv.com/en-ca/client-support/getting-started/ (last visited Oct. 31, 2023) ("1. Visit and enroll in businesstrack.com to view transaction and funding data as well as monthly statements. You can also use the tool to respond to cardholder disputes. 2. Read Your Payment Acceptance Guide for the latest information about accepting cards. 3. Read your Merchant Terms and Conditions for an outline of responsibilities, transactions, equipment, fees, charges, rules and regulations and much more."); *AuthHub*, FISERV, https://www.youtube.com/watch?v=I5vYNpUFOyo (last visited Oct. 31, 2023) ("Welcome to a smarter future with AuthHub from Fiserv.").

290. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients to directly infringe via Fiserv's Developer Studio, which is "a developer portal built by Fiserv to bring their financial technology products onto one platform." Developer Studio enables developers to access APIs and build and test Fiserv product integrations. *See Developer Studio*, FISERV, https://developer.Fiserv.com/support/docs/?path=docs/about-developer-studio.md&branch=main (last visited Oct. 20, 2023).

291. On information and belief, despite having knowledge of the '207 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '207 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively

high likelihood of infringement. Defendants' infringing activities relative to the '207 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

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

COUNT X

(INFRINGEMENT OF U.S. PATENT NO. 7,835,960)

293. Plaintiff incorporates paragraphs 1 through 292 herein by reference.

294. Plaintiff is the assignee of the '960 patent, entitled "System for Facilitating a Transaction," with ownership of all substantial rights in the '960 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

295. The '960 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '960 patent issued from U.S. Patent Application No. 10/709,978.

296. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '960 patent in this District and elsewhere in Texas and the United States.

297. On information and belief, Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '960 patent, which includes

Defendants' offering, providing, issuing, provisioning, registering, facilitating, maintaining, authenticating, validating, authorizing, clearing, settling, processing, directing and controlling, and/or deriving substantial revenue from financial transactions, including without limitation those associated with payment transaction instruments (e.g., EMV contactless cards made by Fiserv and sold to financial institutions, Fiserv Transaction Devices, Fiserv Cards, Mastercard Transaction Instruments, and/or Mastercard Cards) and related products, methods, and/or services for Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, including Defendants' issuing and provisioning products, systems, methods, and/or services, for example, for cards and/or tokens; and/or Defendants' payment processing, authentication, authorization, validation, and fraud detection products, systems, methods, and/or services, including at least those related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

298. Defendants directly infringe, individually and/or jointly with at least one other entity, the '960 patent via 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '960 patent for and/or to, for example, its alter egos, agents, intermediaries, licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients. Defendants' infringement involves Defendants' own action and/or direction and control of third parties' actions.

299. Defendant FSI directly infringes the '960 patent through its direct involvement in the activities of its subsidiaries, including without limitation Defendant FSS, for example, by importing, distributing, making, offering for sale, selling, using and/or servicing the Accused Instrumentalities in the U.S. directly for Defendants. On information and belief, Defendants'

divisions, subsidiaries, partners, and/or affiliates conduct activities that constitute direct infringement, individually and/or jointly, of the '960 patent under 35 U.S.C. § 271(a) by importing, distributing, making, offering for sale, selling, using and/or servicing those Accused Instrumentalities. For example, on information and belief, FSS, provides at least products, systems, methods, services (e.g., software services) and/or solutions to Defendants' licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients including without limitation products, systems, methods, and/or services in connection with providing, issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection related to Defendants' card products (e.g., Fiserv Cards and/or Mastercard Cards), as used in contactless chips, mobile payments, and digital wallets.

300. 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/or consumers to perform one or more steps of the claimed methods of the '960 patent. *Akamai Techs. v. Limelight Networks*, 797 F.3d 1020, 1023-24 (Fed. Cir. 2015) ("[A]n actor is liable for infringement under § 271(a) if it acts through an agent … or contracts with another to perform one or more steps of a claimed method."). For example, on information and belief, Defendants direct and control the activities of such third parties in complying with the EMV standards for contactless and mobile payments so that Defendants' cards (including, for example, as used in contactless chips, mobile payments and digital wallets); tokens; and/or products, systems, methods, and/or services for issuing, provisioning, payment processing, authentication, authorization, validation, and/or fraud detection may utilize such features in a transaction (e.g., point-of-sale transaction). As part of the Defendants' agreements with such third parties to provide access to Defendants'

products, systems, methods, and/or services, Defendants establish the manner of the performance of such products, systems, devices, networks, services and/or methods, e.g., so that transactions using Defendants' products, systems, methods, and/or services, for example, Fiserv Cards and/or Mastercard Cards, tokens, payment solutions, point-of-sale terminals, and other products, must support EMV standards for contactless and mobile payments, as a condition of each third party's access to, use of, and/or participation in such products, systems, methods, and/or services. *See id*. ("[L]iability under § 271(a) can also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance."). The activities of each third party (including as alter egos, intermediaries, agents, subsidiaries, affiliates, partners, licensees, clients, issuers, acquirers, merchants, customers, businesses, financial institutions, and consumers) in providing services to holders of Defendants' Fiserv Transaction Instruments, cardholders of Defendants' Fiserv Cards, and users of other products, systems, methods, and/or services are thus attributed to the Defendants such that Defendants become the "single actor" chargeable with the direct infringement.

301. In addition to the liability arising from the Defendants' relationship with third parties, Defendants also directly infringe, individually and/or jointly, the '960 patent via their own provision of products, tokens, systems, methods, and services that implement EMV standards in mobile or contactless transactions associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards). On information and belief, Defendants design and develop payment applications for accounts used in connection with Fiserv Transaction Instruments and/or Fiserv Cards, which are used with physical Fiserv Cards and digital wallets. These products are issued by Defendants and/or partners of Defendants (e.g., issuing banks)

to individual and commercial consumers as part of a financial account (e.g., credit, debit, and/or prepaid account). *See, e.g., Secure Payment Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards.html (last visited Oct. 20, 2023) ("Fiserv offers high-quality, cost-effective manufacturing, personalization and delivery services for a wide variety of cards including debit, credit, ATM, prepaid and gift cards; EMV® and contactless cards; photo cards; membership; and healthcare ID cards. Fulfillment options include central and in-branch issuance to meet immediate needs."); *EMV and Contactless EMV Cards*, FISERV, https://www.Fiserv.com/en/solutions/customer-and-channel-management/output-solutions/products-and-services/secure-payment-cards/central-issuance/emv-chip-cards.html (last visited Oct. 20, 2023) (noting "Fiserv offers the industry's most complete, comprehensive and integrated EMV solution" including "processing EMV transactions on the Visa®, Mastercard® and Accel® debit networks" and "[c]ontactless EMV cards").

302. For example, Defendants infringe claim 1 of the '960 patent via their Accused Instrumentalities that implement Fiserv's tokenization services (e.g., Multi-pay Token service), for example, in connection with Fiserv Transaction Instruments.

303. The Accused Instrumentalities implement the method of claim 1 of the '960 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff's allegations that each of those limitations is met. For example, the Accused Instrumentalities include a method for processing a transaction, the method implementing the steps: receiving, by a merchant and via a processor, an account number of a user; submitting, by the merchant and via the processor, the account number to a provider of the account number and requesting authorization of the transaction; requesting, by the merchant and via the processor, that

the provider return a secondary transaction number (STN) in lieu of returning the account number; receiving, from the provider and via the processor, an authorization record referencing the STN; issuing, via the processor, a settlement request associated with the transaction, wherein the settlement request includes the STN and does not include the account number; maintaining, by the merchant and via the processor, a record of the transaction; and replacing the account number with the STN, wherein the record of the transaction includes the STN and the record of the transaction does not include the account number.

304. At a minimum, Defendants have known of the '960 patent at least as early as the filing date of this complaint. In addition, Defendants have been contacted to provide Defendants with notice of Plaintiff's American Express patent portfolio and the '960 patent. Defendants have known about the patent portfolio including the '960 patent, since at least on or around September 15, 2023, when, via email, a representative of 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, requested a phone call to discuss the licensing opportunity, and indicated Defendants would be provided with access to a data room containing information related to the American Express patent portfolio. On October 3, 2023, via email, DHG again requested a call to discuss the licensing opportunity on behalf of Plaintiff. On October 25, 2023, DHG again emailed Defendants on behalf of Plaintiff, requested a call to discuss the licensing opportunity, and provided Defendants with access to a data room with detailed portfolio information specific to Defendants. The data room included examples of how Defendants infringed the claims of numerous patents in the American Express patent portfolio, including at least one claim of the '960 patent.

305. On information and belief, since at least each of the above-mentioned dates when Defendants were on notice of their infringement, Defendants have actively induced, under U.S.C. § 271(b), intermediaries, distributors, suppliers, partners, issuers, acquirers, merchants, customers, clients, consumers, and/or payment platforms (e.g., Samsung and Google mobile wallets) that distribute, make, purchase, offer to sell, sale, use, and/or service the Accused Instrumentalities to directly infringe one or more claims of the '960 patent by distributing, making, using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date and/or dates, Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute an infringement of the '960 patent.

306. On information and belief, Defendants intend to cause, and have taken affirmative steps to induce, infringement by intermediaries, distributors, suppliers, licensees, issuers, acquirers, merchants, partners, customers, clients, consumers, and/or payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Defendants' Accused Instrumentalities with mobile payment systems, including with mobile wallet applications; as provider of products, systems, methods, and services associated with Fiserv Transaction Instruments (e.g., Mastercard Transaction Instruments) and/or Fiserv Cards (e.g., Mastercard Cards), providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet users and/or providers, point of sale terminal users and/or providers, merchants (including online and mail order), and/or users of Defendants' Accused Instrumentalities; maintaining such EMV payment applications by personalizing transaction 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 without limitation via vendors, the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing Defendants' mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., Fiserv.com; carat.Fiserv.com; developer.Fiserv.com; clover.com) and mobile applications for clients, customers, and consumers for accessing, obtaining, purchasing, registering, activating, maintaining, and/or using the Accused Instrumentalities; and/or providing technical support and services for these products, systems, methods, and services to licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients, in the United States. *See, e.g.*, *Moving*, FISERV, https://www.Fiserv.com/ (last visited Oct. 31, 2023) ("Every minute of the day, people, businesses and financial institutions are connecting with one another through payments and financial services technology from Fiserv."); *Run your business smarter, faster, easier*, CLOVER, https://get.clover.com/clover-pos-systems (last visited Oct. 31, 2023) ("Want to learn more? Ready to get started? Contact the Clover sales team today."); *Welcome to Fiserv Merchant Services*, FISERV, https://merchants.Fiserv.com/en-ca/client-support/getting-started/ (last visited Oct. 31, 2023) ("1. Visit and enroll in businesstrack.com to view transaction and funding data as well as monthly statements. You can also use the tool to respond to cardholder disputes. 2. Read Your Payment Acceptance Guide for the latest information about accepting cards. 3. Read your Merchant Terms and Conditions for an outline of responsibilities, transactions, equipment, fees, charges, rules and regulations and much more."); *AuthHub*, FISERV, https://www.youtube.com/watch?v=I5vYNpUFOyo (last visited Oct. 31, 2023) ("Welcome to a smarter future with AuthHub from Fiserv.").

307. Moreover, Defendants induce licensees, issuers, acquirers, merchants, partners, customers, consumers, and/or clients to directly infringe via Fiserv's Developer Studio, which is "a developer portal built by Fiserv to bring their financial technology products onto one platform." Developer Studio enables developers to access APIs and build and test Fiserv product integrations. *See Developer Studio*, FISERV, https://developer.Fiserv.com/support/docs/?path=docs/about-developer-studio.md&branch=main (last visited Oct. 20, 2023).

308. On information and belief, despite having knowledge of the '960 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '960 patent, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Defendants' infringing activities relative to the '960 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.

309. 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

310. 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.

311. 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

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

PRAYER FOR RELIEF

313. 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: November 9, 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