

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

PROXENSE, LLC,

Plaintiff,

v.

MASTERCARD INTERNATIONAL
INCORPORATED, and MASTERCARD
INCORPORATED.

Defendants.

Civil Action No. 26-cv-9333

**COMPLAINT FOR PATENT
INFRINGEMENT**

JURY TRIAL DEMANDED

Plaintiff Proxense, LLC (“Proxense”), by and through its undersigned counsel, for its Complaint against Defendants Mastercard Incorporated and Mastercard International Incorporated (together, “Mastercard” or “Defendants”), alleges as follows:

NATURE OF THE ACTION

1. This is an action for patent infringement arising under the Patent Laws of the United States, 35 U.S.C. § 1 *et seq.*, based on Mastercard’s infringement of U.S. Patent No. 8,352,730 (the “730 Patent”), as amended by Ex Parte Reexamination Certificate No. US 8,352,730 C1, and U.S. Patent No. 8,886,954 (the “954 Patent”) (together, the “Patents-in-Suit”).

2. The Patents-in-Suit claim priority to December 2004 and describe and claim methods of authenticating a biometrically verified user. In the claimed methods, codes including a device ID code uniquely identifying an integrated device are received from the user’s device; authentication of those codes is requested from a trusted authority operated by a third party that possesses a list of codes identifying legitimate devices; and, upon receipt of an access message from the trusted authority, the biometrically verified user is allowed to access an application and complete a transaction.

3. Mastercard practices the claimed methods through the Mastercard Digital Enablement Service (“MDES”), the tokenization platform at the center of Mastercard’s digital payments business. When a cardholder taps an iPhone, or other mobile device enrolled in Apple Pay (or another smartphone, watch, or tablet using a competing digital wallet app) at a contactless point-of-sale terminal that accepts Mastercard, the terminal receives a device-specific Mastercard Token and a transaction-unique cryptogram that the phone generates after the cardholder authenticates on the device, including with Face ID, Touch ID, a fingerprint, or an iris scan. The token and cryptogram are routed through the acquirer to Mastercard, which validates them against the Mastercard Token Vault that Mastercard owns and operates, maps the token to the cardholder’s underlying account number, and forwards the authorization request containing that account number to the issuing bank’s authorization system, which then processes and approves the transaction.

4. Mastercard performs, and directs and controls the performance of, each step of the claimed methods. Mastercard promulgates and enforces the Mastercard Rules and the MDES specifications, conditions participation in its payment network and in MDES on compliance with them, and thereby establishes the manner and timing of every step performed by issuers, acquirers, merchants, and the wallet operators Mastercard calls “Pass-through Digital Wallet Operators.” Mastercard has done so since at least 2014, when it launched MDES, and MDES today “helps secure billions of transactions each year.”

5. Proxense seeks damages adequate to compensate it for Mastercard’s infringement, together with the other relief set forth below.

THE PARTIES

6. Plaintiff Proxense, LLC is a limited liability company organized and existing under the laws of the State of Delaware, with its principal place of business at 689 NW Stonepine Drive, Bend, Oregon 97703.

7. Defendant Mastercard Incorporated is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business and global headquarters at 2000 Purchase Street, Purchase, New York 10577, in Westchester County, within this District.

8. Defendant Mastercard International Incorporated is a non-stock corporation organized and existing under the laws of the State of Delaware, with its principal place of business at 2000 Purchase Street, Purchase, New York 10577, within this District. Mastercard International Incorporated is the principal operating subsidiary of Mastercard Incorporated, through which Mastercard Incorporated conducts its business.

9. Mastercard International Incorporated promulgates the Mastercard Rules, which govern every participant in Mastercard's payment network. The Mastercard Rules define the "Corporation" that issues and enforces them as "Mastercard International Incorporated, Maestro International Inc., and their subsidiaries and affiliates," and define MDES as "the services offered by the Corporation exclusively to Customers for the digital enablement of Account ... data, including but not limited to ID&V Service, Tokenization Service, Digitization Service, Token Mapping Service, Mastercard Cloud-Based Payments, Digital Card Image Database, CVC 3 pre-validation and other on-behalf cryptographic validation services, and Service Requests."

10. Upon information and belief, Mastercard Incorporated and Mastercard International Incorporated act in concert, and as a single integrated enterprise, in designing,

operating, marketing, and controlling MDES, the Mastercard Token Vault, the Mastercard network, and the Mastercard Rules, and each is liable for the acts of infringement alleged herein.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because this action arises under the Patent Laws of the United States, 35 U.S.C. § 1 *et seq.*

12. This Court has personal jurisdiction over each Defendant. Each Defendant maintains its principal place of business and global headquarters in Purchase, New York, within this District, and is therefore at home in, and subject to general personal jurisdiction in, the State of New York. See N.Y. C.P.L.R. § 301. Each Defendant also transacts business in New York and has committed, and continues to commit, acts of patent infringement in New York and in this District, including by operating, directing, and controlling MDES and the Mastercard network from its Purchase, New York headquarters and by causing tokenized Mastercard transactions to be initiated, authenticated, and authorized in this District. See N.Y. C.P.L.R. § 302(a).

13. Venue is proper in this District under 28 U.S.C. § 1400(b). Each Defendant has committed acts of infringement in this District and has a regular and established place of business in this District: its global headquarters at 2000 Purchase Street, Purchase, New York 10577, a physical place that Defendants own or lease, from which Defendants conduct their business, and which Defendants hold out as their headquarters. Upon information and belief, MDES, the Mastercard Rules, and the Mastercard Token program are directed, managed, and controlled by Mastercard personnel located at that headquarters. In addition, tokenized Mastercard transactions using Apple Pay, and other such services, are initiated at contactless terminals, and authorized by issuing banks, throughout this District every day, including in Manhattan and Westchester County.

THE PATENTS-IN-SUIT

A. The '730 Patent

14. On January 8, 2013, the United States Patent and Trademark Office (“USPTO”) duly and lawfully issued the '730 Patent, titled “Biometric Personal Data Key (PDK) Authentication,” to inventor John J. Giobbi. The '730 Patent issued from U.S. Patent Application No. 11/314,199, filed December 20, 2005, and claims priority to U.S. Provisional Application No. 60/637,538, filed December 20, 2004, and U.S. Provisional Application No. 60/652,765, filed February 14, 2005.

15. On January 29, 2026, following an *ex parte* reexamination of the '730 Patent (Reexamination Control No. 90/015,052, requested June 8, 2022), the USPTO issued Ex Parte Reexamination Certificate No. US 8,352,730 C1. The Reexamination Certificate cancelled original claims 1–17 and added new claims 18–34, which the USPTO determined to be patentable. Claims 18–34 of the '730 Patent, as set forth in the Reexamination Certificate, are the claims of the '730 Patent in effect today. A true and correct copy of the '730 Patent is attached as **Exhibit 1**, and a true and correct copy of the Reexamination Certificate is attached as **Exhibit 2**.

16. Claim 29 of the '730 Patent recites:

A method for authenticating a verified user using a computer processor configured to execute method steps, comprising: receiving one or more codes from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and the other data values comprise the device ID code uniquely identifying an integrated device and a secret decryption value associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices; requesting authentication of the one or more codes and the other data values by the agent, wherein the authentication determines whether the one or more codes and the other data values are legitimate; receiving an access message by an application from the agent; and in response to a positive access

message, allowing the biometrically verified user access to the application and complete a transaction of the user accessing the application, wherein principal parties to the transaction are the user and the application, and wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

17. Claim 31 of the '730 Patent depends from claim 29 and further recites “establishing a secure communications channel with a biometric key, wherein the one or more codes and the other data values associated with the biometrically verified user is received from the biometric key.”

B. The '954 Patent

18. On November 11, 2014, the USPTO duly and lawfully issued the '954 Patent, titled “Biometric Personal Data Key (PDK) Authentication,” to inventor John J. Giobbi. The '954 Patent issued from U.S. Patent Application No. 13/710,109, filed December 10, 2012, which is a continuation of the application that issued as the '730 Patent, and claims priority to the same December 20, 2004 and February 14, 2005 provisional applications. A true and correct copy of the '954 Patent is attached as **Exhibit 3**.

19. Claim 16 of the '954 Patent recites:

A method for authenticating a verified user using a computer processor configured to execute method steps, comprising: wirelessly receiving one or more codes and other data values from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and other data values comprises the device ID code uniquely identifying an integrated device associated with a biometrically verified user, the device ID code being registered with a trusted authority for authentication, the trusted authority operated by a third party; requesting authentication of the integrated device using the one or more codes and other data values by the trusted authority; receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party; and in response to receiving the access

message, allowing the biometrically verified user access to the application.

20. Claim 18 of the '954 Patent depends from claim 16 and further recites “establishing a secure communications channel with the integrated device, wherein the one or more codes and other data values associated with the biometrically verified user is received from the integrated device.” Claim 19 of the '954 Patent depends from claim 16 and further recites that “the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.”

C. Ownership

21. Proxense is the sole and exclusive owner of all right, title, and interest to and in each of the Patents-in-Suit, and holds the exclusive right to take all actions necessary to enforce its rights in the Patents-in-Suit, including the filing of this lawsuit. Proxense also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law. Each of the Patents-in-Suit is valid and enforceable.

22. The asserted claims of the Patents-in-Suit are method claims, to which the marking provisions of 35 U.S.C. § 287 do not apply. In any event, Proxense has at all times complied with the marking provisions of 35 U.S.C. § 287 with respect to the Patents-in-Suit, and, on information and belief, any prior assignees and licensees have also either complied with the marking provisions of 35 U.S.C. § 287 or were excused from the obligation to mark.

FACTUAL ALLEGATIONS

A. The Patented Inventions

23. The Patents-in-Suit share a common specification that describes the problem the inventor set out to solve. “Conventional user authentication techniques are designed to prevent

access by unauthorized users. One technique is to require a user being authenticated to provide secret credentials, such as a password, before allowing access.” ’954 Patent at 1:26–29. Another technique “is to provide the user with an access object such as a key (e.g., an electronic key) that the user can present to obtain access,” but “authentication merely proves that the access object itself is valid; it does not verify that the legitimate user is using the access object. That is, [an] illegitimate user can use a stolen access object to enter a secured location because the user’s identity is never checked.” *Id.* at 1:36–46.

24. The inventor, John Giobbi, solved this problem with an “integrated device” (also called a “biometric key”) that stores a user’s biometric data and a device ID code in a tamper-proof format, verifies the user’s identity on the device itself by comparing a biometric scan to the stored biometric data, and, only after successful verification, wirelessly transmits one or more codes, including the device ID code, to an authentication module. *Id.* at 2:59–3:2. The specification explains that the biometric key may be “integrated into a mobile phone (e.g. a cellular phone or smartphone), tablet, laptop, mp3 player, mobile gaming device, watch, key fob or other mobile device, thereby making the biometric key 100 unobtrusive to carry.” *Id.* at 3:9–13.

25. The patented methods add a further layer of security in the form of a “trusted key authority,” which “is a third-party authority that is present in some embodiments in order to provide enhanced security. In one embodiment, trusted key authority 320 verifies that a code from a biometric key is legitimate. To do so, the trusted key authority 320 stores a list of codes for legitimate biometric keys.” *Id.* at 6:35–40. The trusted authority is especially valuable “[i]n an open system, where unknown users can attempt authentication (e.g., in a public grocery store),” because it “provides verification that a key presenting a certain code is legitimate.” *Id.* at 6:48–51. Upon successful authentication, “the trusted key authority sends an access message to the

application to allow user access,” *id.* at 8:12–14, and the user is allowed to access an application such as “computer software” or “a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.),” *id.* at 6:19–26. The specification further discloses that the key and the authentication module may “establish a secure communications channel,” *id.* at 7:15–17, and that the key may “provide a secret decryption value that can be used to communicate with the biometric key,” *id.* at 8:21–23.

26. The claimed methods thus allow a user to be authenticated for a transaction with “an application that is open to the public (i.e., in an open loop system),” *id.* at 3:7–9, without the application ever receiving the user’s biometric data or underlying credentials, and without the user having to memorize or key in credentials. “Advantageously, user authentication is bolstered with highly reliable biometric verification of the user in an integrated device.” *Id.* at 3:3–5. That is precisely the architecture that Mastercard adopted a decade later when it launched MDES.

27. The tokenized payment architecture that Mastercard implements in MDES uses a token issued by a third party and stored on the user’s phone. The token is a surrogate for the primary account number and can be used anywhere the underlying account is accepted as payment. The token is locked in the device and can be released only after the device has verified the user, so the release and presentation of the token is indicative both of the user’s authentication and of the user’s consent to the accompanying charge to the user’s account. The third party that issued the token, here Mastercard, then validates the token and the accompanying cryptogram before the issuing bank is asked to authorize the transaction. Each of those elements is described and claimed in the Patents-in-Suit.

B. Proxense and Its Innovative Technologies

28. Proxense was founded in 2001 and is based in Bend, Oregon. The company was formally organized as a limited liability company in 2001 under the name Margent Development LLC and was renamed Proxense LLC in 2005. From approximately 2004 through 2012, Proxense developed, among other things, mobile payment technologies and commercial products, employing more than thirty engineers and investing many millions of dollars in product development and other research and development efforts. The foundational capabilities of Proxense's technology included a secure element, biometrics captured and stored on that element, retrieval of the biometric and the passing of a token to a trusted third party, and the completion of a mobile payment transaction.

29. Proxense also developed sophisticated, proprietary, proximity-based detection, authentication, and automation technology, built on the concept of wirelessly detecting, authenticating, and communicating with personal digital keys ("PDKs"). Proxense's technology enabled PDKs to run for as long as two years on tiny batteries. Proxense's "ProxPay" technology included biometrically based user and device authentication options, the ability to conduct biometrically verified transactions without sending or exposing the underlying biometric data or storing it anywhere except on the PDK, and a registration for maintaining and verifying the PDK. Significant financial and engineering resources were deployed to make this possible, and the resulting developments became primary differentiators of Proxense's product line and significant elements on which its business was built.

30. John Giobbi is the founder and chief executive officer of Proxense. He is an experienced product designer and prolific inventor, a named inventor on approximately 200 patents, including the Patents-in-Suit, with over 35 years of experience as an entrepreneur and

product development executive. Mr. Giobbi was a Senior Vice President at WMS Gaming, where he managed over 200 staff and during whose six-year tenure the company's market capitalization grew from approximately \$80 million to approximately \$1 billion. Mr. Giobbi was also the founder and President of Prelude Technology Corp. and InPen.

31. The innovative, visionary nature of Proxense's technology was recognized in the media beginning in mid-2008, when *The Bulletin* featured a story on Proxense's mobile payment technology titled "A pint-sized virtual wallet." Andrew Moore, *The Bulletin* (May 7, 2008). The story describes a future that greatly resembles the present day, including a "wireless wallet" with "fingerprint" verification used to pay for goods wirelessly. In 2009, *Trend Hunter* ran a similar story titled "Virtual Biometric Wallets," featuring Proxense and Mr. Giobbi. Michael Plishka, *Trend Hunter* (Jan. 4, 2009). Another 2009 article, in *DARKReading*, a publication in InformationWeek's IT Network, featured the company and Mr. Giobbi in an article titled "Startup May Just Digitize Your Wallet." George V. Hulme, *DARKReading* (Feb. 8, 2009). The *DARKReading* article described that Proxense was "in the process of bringing to market a proximity-based communications device that aims to provide a way to securely share information and conduct payments," and described Proxense's PDKs as "carried by users, perhaps even within a cell phone," and able to hold data securely and manage authentication. As Mr. Giobbi explained, "the data within the PDK also can be protected by additional layers of authentication, such as biometric."

32. Proxense's technology was years ahead of the industry. Google Wallet did not launch until 2011, Apple Pay until 2014, and Samsung Pay until 2015; Apple's Touch ID fingerprint sensor was introduced in 2013; and Mastercard did not launch MDES, the tokenization service through which each of those wallets pays with Mastercard accounts, until 2014. After those

services launched and became inextricably linked to the most popular smartphones in the United States and the world, Proxense found itself unable to compete, even though Proxense invented the technology those solutions use.

33. Today, Proxense holds approximately 80 patents on related technology, including digital content distribution, digital rights management, personal authentication, biometric data management, and mobile payments, and continues to prosecute new patents on its proprietary technology.

C. Mastercard and the Mastercard Digital Enablement Service

34. Mastercard operates one of the world's largest payment networks. Through that network, Mastercard "switches," that is, authorizes, clears, and settles, payment transactions between the banks that issue Mastercard-branded cards and accounts ("Issuers") and the banks that acquire transactions from merchants ("Acquirers"). The computer hardware and software that Mastercard operates to route and process those transactions is referred to in the Mastercard Rules as the "Interchange System."

35. In 2014, Mastercard launched MDES. Mastercard describes MDES as "a single integrated platform for Issuers, Wallet Providers, Merchants, and other Token Requestors to enable the digitization of supported Mastercard card types for many digital payment methods," and states that "[t]he MDES end-to-end services are supported by the reliability and global reach of the Mastercard network." According to Mastercard, MDES works in four steps: "Tokenization replaces PAN"; the "Token is specific to the platform, wallet application, device"; "Digitization provisions the token to the target platform or device"; and the "Token is used for transactions instead of PAN."

36. The Mastercard Rules define “Tokenization” as “[t]he process by which a Mastercard Token replaces an Account PAN,” and a “Mastercard Token” as “[a] Token allocated from a Mastercard Token Account Range that the Corporation has designated to an Issuer ... and that corresponds to an Account PAN.” Mastercard requires that “[a]n Account PAN must be Tokenized whenever a Mobile Payment Device, Access Device, or other non-Card method is used, in addition to a Card, to provide access to an Account.” Mastercard retains “the sole right to designate a Mastercard Token Account Range to an Issuer,” requires that “[e]ach Mastercard Token must be allocated by the Corporation,” and declares that “[t]he Corporation exclusively owns all right, title, and interest in any Mastercard Token.”

37. Mastercard stores the mapping between each Mastercard Token and the underlying account number in the Mastercard Token Vault, which the Mastercard Rules define as “[t]he Token Vault owned and operated by Mastercard and enabled by means of the Mastercard Digital Enablement Service.” A “Token Vault” is “[a] repository of tokens that are implemented by a tokenization system, which may also perform primary account number (PAN) mapping and cryptography validation.” Mastercard requires that it “be provided the mapping between the PAN assigned to a Card, and each Mastercard Token associated with the Account,” and provides that, for wallet tokens, “the Mastercard Token Vault will perform primary account number (PAN) mapping and cryptography validation of the Mastercard Tokens.”

38. Each tokenized transaction is accompanied by a transaction-unique cryptogram generated by the cardholder’s device. As Mastercard explains, “the card stored inside your device ... generates a one-time code, or cryptogram, for every transaction. This makes sure every transaction is really coming from your device.” The Mastercard Rules mandate that “[t]he

Mastercard Token cryptogram, when present, must be validated during the authorization of all Transactions involving Tokenized Accounts.”

39. Mastercard Tokens are provisioned to consumers’ mobile devices through digital wallets such as Apple Pay. The Mastercard Rules refer to such wallets as “Device Wallets,” defined as “Pass-through Digital Wallet[s] that provide[] access to a Mastercard or Maestro Account provisioned as a Mastercard Token onto a Mobile Payment Device or other Access Device,” and refer to their operators as “Pass-through Digital Wallet Operators” or “Pass-through DWOs.” A pass-through wallet stores only the Mastercard Token, not the underlying account, and “upon the performance of a Transaction, transfers the Account data to the Merchant.” Mastercard confirms that each Mastercard Token “is specific to the platform, wallet application, device.” Apple, for its part, explains that when a card is added to Apple Pay, “a unique Device Account Number is created, encrypted, and then stored in the Secure Element” of the iPhone; Google explains that Google Pay “stores a uniquely generated token on the device.”

40. Mastercard requires that every such transaction begin with verification of the user on the device. The Mastercard Rules require each Pass-through DWO to “ensure that each Mobile Payment Device or Access Device used in connection with the Pass-through Digital Wallet can perform ... [a]ny form of Consumer Device Cardholder Verification Method (CDCVM),” and provide that a Pass-through DWO “must only use a CDCVM qualified by the Corporation for use with a Mastercard Account credential.” A CDCVM is “[a] CVM that occurs when personal credentials established by the Cardholder to access an Account by means of a particular Access Device are entered on the Access Device and verified, either within the Access Device or by the Issuer during online authorization.” As Mastercard explains, “on-device authentication confirms your identity directly with your device, typically by tapping in a code or using your fingerprint or

face scan.” Apple Pay for example requires that “the user must authenticate using Touch ID, Face ID or their passcode” before any payment information is transmitted.

41. At the point of sale, the contactless terminal communicates with the cardholder’s device using the EMV contactless kernel that EMVCo, of which Mastercard is a member and owner, specifies for Mastercard-branded cards and devices: EMV Contactless Specifications for Payment Systems, Book C-2, Kernel 2 Specification (“Kernel 2”). Kernel 2 “defines the behaviour of the Kernel used in combination with cards supporting a Mastercard brand,” and treats the cardholder’s phone as the “Card,” defined as “a consumer device supporting contactless transactions.” In every Kernel 2 transaction, “the Kernel reads data record(s) from the Card (through one or more READ RECORD commands),” thereby receiving the Mastercard Token in place of the account number, and “[t]hen the Kernel requests the Card to generate a cryptogram, which is then included in the Data Record” that the terminal assembles “for authorization and clearing.” Kernel 2 recognizes that “the phone can be used to authenticate the cardholder,” provides that, when the device performs cardholder verification, “the Kernel delegates the CVM processing to the phone,” and requires that in such transactions Combined Data Authentication (“CDA”) “is to be used in the GENERATE AC command to avoid fraud,” under which the phone returns a “[d]igital signature on critical application parameters” that the terminal verifies using the phone’s public key certificate.

42. The Mastercard Token and cryptogram received by the terminal are transmitted through the Acquirer to Mastercard. Mastercard requires each Pass-through DWO to “ensure its capability to transmit all required Mastercard Token authorization request message data.” Mastercard, through MDES and the Mastercard Token Vault, validates the cryptogram and maps the Mastercard Token to the underlying account number, and then forwards an authorization

request containing the account number to the Issuer's authorization system, which approves or declines the transaction. The Issuer's authorization system is computer software, and it provides access to the cardholder's financial account.

43. Mastercard dictates each of the foregoing steps and conditions participation in its network and in MDES on their performance. The Mastercard Rules "are Standards and Mastercard has the sole right to interpret and enforce the Rules and other Standards." Issuers must "[c]omply with all technical specifications and other Standards applicable to Tokenization and Digitization" and must "[c]omplete all testing and certifications as may be required by the Corporation." Acquirers are "responsible for ensuring that each of [their] Merchants and Sponsored Merchants complies with the Standards," and failure to comply "may result in chargebacks, an assessment to the Acquirer, and/or other disciplinary action." Each Pass-through DWO "must operate a Pass-through Digital Wallet in accordance with the Standards," must "[s]upport a Mastercard Token," must "[p]resent a Mastercard Token if the Issuer, at the time of provisioning, Tokenized the Account," must "[u]se a Mastercard Token solely for the purpose for which the Token was generated," and, "[b]efore MDES participation begins and on an ongoing basis thereafter, ... must perform testing and obtain any necessary certifications of its equipment, procedures, and systems as the Corporation may require." Mastercard "reserves the right to approve, refuse to approve, require the modification of, or withdraw the approval of a Token Implementation Plan, and to suspend, either temporarily or permanently, a Wallet Token Requestor's MDES participation, in its sole discretion."

44. MDES tokenized transactions using Apple Pay, for example, are performed in the United States, including in this District, billions of times per year.

D. The Accused Instrumentalities

45. The accused instrumentalities include MDES and the Mastercard tokenized contactless payment system, including without limitation: Mastercard Tokens provisioned to Device Wallets (including Apple Pay) on mobile devices; the Mastercard Token Vault and Mastercard's token mapping, de-tokenization, and cryptogram validation services; the Interchange System and Mastercard's routing of token authorization requests and PAN authorization requests; the Mastercard Rules, MDES specifications, Token Implementation Plans, and certification and testing programs by which Mastercard governs Issuers, Acquirers, Merchants, and Pass-through DWOs; and contactless point-of-sale terminals implementing Kernel 2 that are certified to accept Mastercard contactless transactions (collectively, the "Accused Instrumentalities").

46. A claim chart demonstrating how the Accused Instrumentalities practice claims 29 and 31 of the '730 Patent is attached as **Exhibit 4**. A claim chart demonstrating how the Accused Instrumentalities practice claims 16, 18, and 19 of the '954 Patent is attached as **Exhibit 5**. Exhibits 4 and 5 are incorporated by reference in their entirety.

E. Mastercard's Knowledge of the Patents-in-Suit

47. Mastercard has had knowledge of the Patents-in-Suit and of its infringement at least as of the filing and service of this Complaint.

48. Mastercard is a member of EMVCo, LLC, and the EMV specifications that Mastercard co-authors and relies upon expressly warn that the specifications "may provide for the use of public key encryption and other technology, which may be the subject matter of patents in several countries," that "[a]ny party seeking to implement these Specifications is solely responsible for determining whether its activities require a license to any such technology," and that "any person who implements any part of the EMV® Specifications should consult an intellectual

property attorney before any such implementation.” Mastercard nonetheless has continued to operate, promote, and expand MDES without a license from Proxense.

COUNT I

(Infringement of U.S. Patent No. 8,352,730)

49. Proxense incorporates by reference the allegations of the preceding paragraphs as if fully set forth herein.

50. Mastercard has directly infringed, and continues to directly infringe, at least claims 29 and 31 of the ’730 Patent under 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by performing, in the United States, each step of the claimed methods through the Accused Instrumentalities, as set forth in **Exhibit 4**.

51. To the extent any step of the claimed methods is performed by an entity other than Mastercard, including an Issuer, an Acquirer, a Merchant, a Pass-through DWO, or a contactless terminal operating under the Mastercard Rules and the EMV specifications, Mastercard directs and controls the performance of that step such that it is attributable to Mastercard. Mastercard conditions participation in the Mastercard network and in MDES, and the receipt of the benefits of that participation, including the right to issue, provision, present, accept, and be paid for Mastercard Tokens, upon performance of the claimed steps, and Mastercard establishes the manner and timing of that performance through the Mastercard Rules, the MDES specifications, Token Implementation Plans, certification and testing requirements, and the EMV specifications that Mastercard co-authors and mandates. See *Akamai Techs., Inc. v. Limelight Networks, Inc.*, 797 F.3d 1020, 1022–23 (Fed. Cir. 2015) (en banc). Mastercard is therefore liable for direct infringement of the ’730 Patent as a single actor.

52. By way of example, with respect to claim 29, in a Mastercard tokenized contactless transaction: (a) a contactless terminal, operating under Mastercard’s direction and control, receives

from the cardholder's mobile device one or more codes and other data values including a Mastercard Token that uniquely identifies the device and a transaction-unique cryptogram, both associated with a user who has been biometrically verified on the device, the Mastercard Token having been registered with Mastercard, a third-party trusted authority that possesses, in the Mastercard Token Vault, a list of the Mastercard Tokens it has issued to legitimate devices; (b) the terminal and Acquirer, operating under Mastercard's direction and control, request authentication of the Mastercard Token and cryptogram by routing them to Mastercard, which validates the cryptogram and maps the Mastercard Token to the underlying account number, thereby determining that they are legitimate; (c) the Issuer's authorization system, an application comprising computer software, receives from Mastercard an access message in the form of a PAN authorization request containing the account number; and (d) in response to that message, the Issuer's authorization system allows the biometrically verified user access to the application and completes the transaction, the principal parties to which are the user and the Issuer's authorization system.

53. With respect to claim 31, the contactless terminal, operating under Mastercard's direction and control pursuant to Kernel 2, establishes a secure communications channel with the cardholder's mobile device, which operates as a biometric key, including through Combined Data Authentication, the Relay Resistance Protocol, and the exchange of transaction-unique cryptograms generated with keys that Mastercard provisioned to the device, and the Mastercard Token and cryptogram associated with the biometrically verified user are received from that device over that channel.

54. Mastercard has also actively induced, and continues to actively induce, infringement of at least claims 29 and 31 of the '730 Patent under 35 U.S.C. § 271(b). With

knowledge of the '730 Patent at least as of the filing and service of this Complaint, Mastercard has knowingly and intentionally induced Issuers, Acquirers, Merchants, Pass-through DWOs, terminal vendors, and cardholders to perform the claimed methods by, among other things, promulgating and enforcing the Mastercard Rules and MDES specifications; requiring that accounts be tokenized whenever a mobile device is used to access them; requiring Pass-through DWOs to support, present, and transmit Mastercard Tokens and to use Mastercard-qualified CDCVMs; certifying wallets, devices, and terminals for MDES and Mastercard contactless acceptance; operating the Mastercard Token Vault and the Interchange System to authenticate and route tokenized transactions; and marketing and promoting MDES, Mastercard Tokens, and contactless payments with Apple Pay, and similar apps, with the specific intent that those parties perform the claimed methods and with knowledge that their performance constitutes infringement.

55. Mastercard has also contributorily infringed, and continues to contributorily infringe, at least claims 29 and 31 of the '730 Patent under 35 U.S.C. § 271(c), by providing in the United States MDES, Mastercard Tokens, the Mastercard Token Vault, and Mastercard's token mapping and cryptogram validation services, which constitute a material part of the claimed inventions, are especially made or especially adapted for use in practicing the claimed methods, and are not staple articles or commodities of commerce suitable for substantial non-infringing use, with knowledge of the '730 Patent and of the infringing use.

56. Mastercard's infringement has damaged, and continues to damage, Proxense. Proxense is entitled to recover damages adequate to compensate it for Mastercard's infringement, which in no event can be less than a reasonable royalty, together with interest and costs, pursuant to 35 U.S.C. § 284.

57. Mastercard's continued infringement after receiving notice of the '730 Patent is willful, deliberate, and in reckless disregard of Proxense's patent rights, entitling Proxense to enhanced damages under 35 U.S.C. § 284 and rendering this an exceptional case under 35 U.S.C. § 285.

COUNT II

(Infringement of U.S. Patent No. 8,886,954)

58. Proxense incorporates by reference the allegations of the preceding paragraphs as if fully set forth herein.

59. Mastercard has directly infringed, and continues to directly infringe, at least claims 16, 18, and 19 of the '954 Patent under 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by performing, in the United States, each step of the claimed methods through the Accused Instrumentalities, as set forth in **Exhibit 5**.

60. To the extent any step of the claimed methods is performed by an entity other than Mastercard, Mastercard directs and controls the performance of that step, such that it is attributable to Mastercard, for the reasons set forth above and in Exhibit 5. Mastercard conditions participation in the Mastercard network and in MDES, and the receipt of the benefits of that participation, upon performance of the claimed steps, and establishes the manner and timing of that performance through the Mastercard Rules, the MDES specifications, Token Implementation Plans, certification and testing requirements, and the EMV specifications. Mastercard is therefore liable for direct infringement of the '954 Patent as a single actor.

61. By way of example, with respect to claim 16, in a Mastercard tokenized contactless transaction: (a) a contactless terminal, operating under Mastercard's direction and control, wirelessly receives from the cardholder's mobile device, over the contactless radio-frequency interface specified by Kernel 2, one or more codes and other data values including a Mastercard

Token that uniquely identifies the device, which is associated with a user who has been biometrically verified on the device, the Mastercard Token having been registered for authentication with the Mastercard Token Vault, a trusted authority operated by Mastercard, a third party to the user and the Issuer; (b) the terminal and Acquirer, operating under Mastercard's direction and control, request authentication of the device by routing the Mastercard Token and cryptogram to Mastercard, which validates the cryptogram and maps the Mastercard Token to the underlying account number; (c) the Issuer's authorization system, an application, receives from Mastercard an access message in the form of a PAN authorization request containing the account number and the Mastercard Token, which indicates that Mastercard successfully authenticated the Mastercard Token and cryptogram; and (d) in response, the Issuer's authorization system allows the biometrically verified user access to the application.

62. With respect to claim 18, the contactless terminal, operating under Mastercard's direction and control pursuant to Kernel 2, establishes a secure communications channel with the cardholder's mobile device, including through Combined Data Authentication, the Relay Resistance Protocol, and the exchange of transaction-unique cryptograms generated with keys that Mastercard provisioned to the device, and the Mastercard Token and cryptogram associated with the biometrically verified user are received from that device over that channel. With respect to claim 19, the Issuer's authorization system is computer software and provides access to a financial account.

63. Mastercard has also actively induced, and continues to actively induce, infringement of at least claims 16, 18, and 19 of the '954 Patent under 35 U.S.C. § 271(b). With knowledge of the '954 Patent at least as of the filing and service of this Complaint, Mastercard has knowingly and intentionally induced Issuers, Acquirers, Merchants, Pass-through DWOs, terminal

vendors, and cardholders to perform the claimed methods by, among other things, promulgating and enforcing the Mastercard Rules and MDES specifications; requiring that accounts be tokenized whenever a mobile device is used to access them; requiring Pass-through DWOs to support, present, and transmit Mastercard Tokens and to use Mastercard-qualified CDCVMs; certifying wallets, devices, and terminals for MDES and Mastercard contactless acceptance; operating the Mastercard Token Vault and the Interchange System to authenticate and route tokenized transactions; and marketing and promoting MDES, Mastercard Tokens, and contactless payments with Apple Pay, and similar payment apps, with the specific intent that those parties perform the claimed methods and with knowledge that their performance constitutes infringement.

64. Mastercard has also contributorily infringed, and continues to contributorily infringe, at least claims 16, 18, and 19 of the '954 Patent under 35 U.S.C. § 271(c), by providing in the United States MDES, Mastercard Tokens, the Mastercard Token Vault, and Mastercard's token mapping and cryptogram validation services, which constitute a material part of the claimed inventions, are especially made or especially adapted for use in practicing the claimed methods, and are not staple articles or commodities of commerce suitable for substantial non-infringing use, with knowledge of the '954 Patent and of the infringing use.

65. Mastercard's infringement has damaged, and continues to damage, Proxense. Proxense is entitled to recover damages adequate to compensate it for Mastercard's infringement, which in no event can be less than a reasonable royalty, together with interest and costs, pursuant to 35 U.S.C. § 284.

66. Mastercard's continued infringement after receiving notice of the '954 Patent is willful, deliberate, and in reckless disregard of Proxense's patent rights, entitling Proxense to

enhanced damages under 35 U.S.C. § 284 and rendering this an exceptional case under 35 U.S.C. § 285.

PRAYER FOR RELIEF

WHEREFORE, Proxense respectfully requests that the Court enter judgment in its favor and against Mastercard as follows:

- A. A judgment that Mastercard has infringed, directly and indirectly, one or more claims of each of the Patents-in-Suit;
- B. An award of damages adequate to compensate Proxense for Mastercard's infringement, in an amount to be determined at trial, but in no event less than a reasonable royalty, pursuant to 35 U.S.C. § 284;
- C. An award of enhanced damages, up to three times the amount of damages found or assessed, pursuant to 35 U.S.C. § 284;
- D. An accounting and award of supplemental damages for any infringement occurring after the period for which discovery is taken through entry of final judgment;
- E. An award of ongoing royalties, or, in the alternative, a permanent injunction, for any post-judgment infringement;
- F. A declaration that this case is exceptional and an award to Proxense of its reasonable attorneys' fees pursuant to 35 U.S.C. § 285;
- G. An award of pre-judgment and post-judgment interest and costs; and
- H. Such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Proxense demands a trial by jury on all issues so triable.

Dated: New York, New York
October 26, 2026

Respectfully submitted,

HECHT PARTNERS LLP

By: /s/ David L. Hecht

David L. Hecht

Maxim Price

Michael S. DeVincenzo

Andrea Pacelli, PhD

Charles Wizenfeld

Delphine W. Knight Brown

125 Park Avenue, 25th Floor

New York, New York 10017

Tel.: (212) 851-6821

dhecht@hechtpartners.com

mprice@hechtpartners.com

mdevincenzo@hechtpartners.com

apacelli@hechtpartners.com

cwizenfeld@hechtpartners.com

dkbrown@hechtpartners.com

Attorneys for Plaintiff Proxense, LLC