IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

CORTEX MCP, INC., Plaintiff, v. VISA, INC. Defendant.	CIVIL ACTION NO. 6:23-CV-00048-FB JURY TRIAL DEMANDED

FIRST AMENDED COMPLAINT FOR
PATENT INFRINGEMENT AND JURY DEMAND

Plaintiff Cortex MCP, Inc. ("Cortex"), by and through its attorneys, files this First Amended Complaint for Patent Infringement against defendant Visa, Inc. ("Visa") and alleges as follows:

1. Cortex was launched in October 2012 as a provider of a next-generation mobile-wallet platform designed for the growing market in mobile commerce. Cortex invented a platform to address the obstacles that had hampered the adoption of existing wallet technologies. The Cortex platform uses the technology of "tokenization" to allow consumers to store their credit cards and identification and conduct transactions on their mobile devices while safeguarding their personal identifying information. Cortex's technology is compatible with any device and can be used without disrupting the merchant's existing point-of-sale infrastructure. On December 21, 2012, Cortex applied for the initial patent for this technology.

2. This complaint arises from Visa's unlawful infringement of the following United States patents owned by Cortex: United States Patent Nos. 9,251,531 ("'531 Patent"); 9,954,854 ("'854 Patent"); 10,749,859 ("'859 Patent"); and 11,329,973 ("'973 Patent") (collectively, the "Asserted Patents").

Parties

3. Plaintiff Cortex MCP, Inc. is a Delaware C-corporation organized and existing under the laws of Delaware, with its principal place of business at 15331 W. Bell Road, Suite #212, Surprise, Arizona 85739.

4. Defendant Visa, Inc. is a corporation organized under the laws of the State of Delaware, with its principal place of business at 900 Metro Center Blvd., Foster City, California 94404. Visa is doing business, either directly or through its agents, on an ongoing basis in this judicial district and elsewhere in the United States, and has a regular and established place of business in this judicial district. Visa may be served with process through its registered agent, Corporation Trust Company, 1209 Orange Street, Corporation Trust Center, Wilmington, Delaware 19801.

Jurisdiction & Venue

5. This Court has subject matter jurisdiction 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.

6. This Court has personal jurisdiction over Visa in this action because Visa has committed acts of infringement of the Asserted Patents within this District giving rise to this action, and has established minimum contacts with this forum such that the exercise of jurisdiction over Visa would not offend traditional notions of fair play and substantial justice. Visa, directly and through subsidiaries or intermediaries, has committed and continues to commit acts of infringement in this District by, among other things, processing credit card transactions with "tokenization methods" that infringe the Asserted Patents. Notably, Visa has admitted or failed to dispute that Texas federal courts have personal jurisdiction over Visa in patent actions. *See, e.g.*, Answer ¶¶ 5-6 (admitting that "it conducts business in the District" and not contesting that "venue

is proper in this District as to Visa"), *SFA Systems, LLC, v. Visa, Inc.*, 6:14-cv-00176 (E.D. Tex. May 19, 2014), ECF No. 13; Answer ¶ 19 ("Visa admits that it is subject to this Court's specific and general personal jurisdiction."), *Actus LLC v. Blaze Mobile. Inc., et al.*, 2:9-cv-00102 (E.D. Tex. Mar. 8, 2010), ECF No. 258.

7. Venue is proper in this District under 28 U.S.C. § 1400(b). Visa is registered to do business in Texas, and upon information and belief, has transacted business in this District and has committed acts of direct and indirect infringement in this District by, among other things, processing credit card transactions with tokenization methods that infringe the Asserted Patents, and engineering the applications and services that support those tokenization methods. Visa has a regular and established place of business in the District, including corporate offices at 12301 Research Blvd., Austin, Texas 78759. Visa has been conducting business in the District since at least 2012, when it opened its first office in Austin[1] and announced plans to open a "global information technology center" at 12301 Research Boulevard.[2] By 2019, Visa had leased space in four buildings near Austin, employing nearly 2,000 people in the area.[3] As of September 23, 2022, Visa was advertising 320 open positions in Austin—including multiple positions in the field of Payment Systems Risk.[4]

---

[1] https://www.bizjournals.com/austin/news/2019/05/14/visa-grows-tech-center-in-north-austin.html.

[2] https://web.archive.org/web/20121215010733/http:/www.statesman.com/news/business/visa-confirms-plans-for-austin-offices/nTSm6/.

[3] https://www.bizjournals.com/austin/news/2019/05/14/visa-grows-tech-center-in-north-austin.html.

[4] https://usa.visa.com/en_us/jobs/?cities=Austin.

The Technology

8. The adoption of mobile wallets and mobile payments lagged behind the rapid growth of smartphones, despite the fact that these "wallet solution" applications were naturally suited to those devices. The primary reason why mobile wallets failed to gain traction with consumers and merchants was that existing payment methods such as credit cards proved ill-suited for storage on mobile devices. For example, early mobile-wallet applications required "secure element chips" to be physically embedded into user devices to ensure the security of the stored data. Most phones, including iPhones, did not include these chips. Because these applications required specialized hardware and/or substantial changes in both user and merchant behavior, they proved less user-friendly than the status quo of credit and debit cards.

9. Cortex's "Officially Verifiable Electronic Representation" or "OVER File" technology addresses these roadblocks to the adoption of mobile-wallet systems. The technology provides a mobile-wallet solution that is both secure and convenient for consumers and merchants alike. The OVER File platform allows consumers to store credit card data and associated personal identifying information on a mobile device without the associated risk if this data is accessed by hackers. Each OVER File is a token that is unique to the user and device. The OVER File is also encrypted, which prevents the use or manipulation of data even if a hacker gains access to the device or to the file. When a customer presents an OVER File identification at a point of sale, the merchant can validate the user's credentials through an authentication application designed to interact with the token. Importantly, the technology is compatible not only with all major smartphones but also with the existing point-of-sale infrastructure used by merchants.

10. In July 2013, representatives from Cortex met with representatives from CyberSource Company, a software company owned by Visa, to discuss a possible business or

commercial relationship between Cortex and Visa. Both parties signed a non-disclosure agreement ahead of that meeting. During that meeting, Cortex gave a presentation of its payment platform, and described Cortex's OVER File technology—as reflected in the '531 patent issued on February 2, 2016. Cortex informed CyberSource that it had filed a patent application for the OVER File technology, and explained why Cortex's OVER File IP would be useful for Visa's mobile commerce business.

11. In or around April of 2016, representatives from Visa requested from Cortex a summary of potential "synergies" between the two companies, again in the context of a possible business relationship. In response to that request, Shaunt Sarkissian, Cortex's Founder and CEO, emailed to Jim McCarthy, then Visa's head of innovation, a three-page overview of Cortex's technologies and their potential application to Visa's Digital Enablement Program. That document noted that Cortex's "Tokenization capabilities can add significant value, IP, and capacities to the Visa Token Service," and expressly stated that Cortex had been issued an OVER File Patent—the '531 patent that had been issued in February 2016. The document also informed Visa that Cortex had new OVER File patent applications that were "Near Issuance," referring to the '854 patent. In that document, Cortex described its OVER File IP as "significant," "covering every aspect of provisioning a representative credential, that can be scanned and verified," and "as an effective leverage tool for Visa across the board." Cortex specifically noted that its OVER File IP was subject to "exi[s]ting infringement from most all Wallet Solution providers." Along with that overview, Mr. Sarkissian sent to Mr. McCarthy a one-page summary of potential synergies between Cortex and Visa, which stated that Cortex's "Enhanced Tokenization Capabilities" could provide a "Critical supporting IP portfolio" for the Visa Token Service. Mr. McCarthy was Visa's head of innovation at the time and, upon information and belief, responsible for the introduction

of the Visa Token Service. In early 2017, Mr. Sarkissian emailed substantially the same information to William Sheedy, Visa's Executive Vice President.

Count 1
(Infringement of the '531 Patent)

12. Cortex repeats and re-alleges the allegations in the preceding paragraphs as if fully set forth herein.

13. On February 2, 2016, the U.S. Patent & Trademark Office duly and legally issued the '531 Patent entitled "File format and platform for storage and verification of credentials." A true and correct copy of the '531 Patent is attached as Exhibit 1 to this Complaint.

14. Cortex is the owner of all rights, title, and interest in and to the '531 Patent, including the right to assert all causes of action arising under the '531 Patent and the right to any remedies for the infringement of the '531 Patent.

15. Claim 1 of the '531 Patent recites:

1. A computer-implemented method comprising:

storing, in a memory of an officially verifiable electronic representation (OVER) generation and verification engine, information associated with a credential of a user for proving the user's identity or qualifications;

receiving, from an OVER file storage client device of the user, an OVER file generation request to provide authentication of the user based on the information associated with the credential;

generating, by a processor of the OVER engine, an OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential, based on the information associated with the credential of the user;

transmitting, to the OVER file storage client device of the user, the OVER file in response to the OVER file generation request;

receiving, from an OVER file third-party client verifying device, a verifying request to verify that the OVER file transmitted to the user authenticates the user based on a scan associated with the OVER file on the OVER file store client device of the user;

> verifying that the scan associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine, in response to the verifying request; and
>
> transmitting, to the OVER file third-party client verifying device, an authentication message comprising an indication of whether the scan associated with the OVER file on the device of the user corresponds to the information associated with the credential of the user that is stored in the OVER engine.

16. Visa has directly infringed and continues to directly infringe, literally and/or under the doctrine of equivalents, one or more claims, including at least claim 1, of the '531 Patent in violation of 35 U.S.C. § 271(a) because Visa makes, uses, offers for sale, and/or sells certain products such as the Visa Token Service (VTS) (the "'531 Accused Products"), including within this Judicial District. VTS implements tokenization processes that are published by EMVCo,[5] a global technology body that is managed by Visa, and in which it has an ownership stake.[6] Upon information and belief, EMV stands for "Europay, Mastercard, and Visa." EMVCo promotes the adoption of tokenization in the payment community and publishes an EMV Payment Tokenization Specification Technical Framework that provides guidelines and instructions for tokenized transactions that are followed by EMVCo members such as Visa.[7]

17. Visa's infringing use of the '531 Accused Products includes its internal use and testing of the '531 Accused Products.

18. The '531 Accused Products satisfy all claim limitations of one or more claims of the '531 Patent, including at least claim 1. To the extent a claim limitation is not met literally, it is

---

[5] Visa Token Service Provisioning and Credential Management, https://developer.visa.com/capabilities/token-service-provisioning ("Tokenization is based on the EMVCo payment tokenization standard and aligns with EMV technology (the global standard for secure payments)").

[6] Overview of EMVCo, https://www.emvco.com/about-us/overview-of-emvco/.

[7] EMV Payment Tokenisation, https://www.emvco.com/cmv-technologies/payment-tokenisation/.

met under the doctrine of equivalents because any differences between the '531 Accused Products and the claims in the '531 Patent are insubstantial.

19. For example, the '531 Accused Products implement a computer-based method for storing, in a memory of an officially verifiable electronic representation (OVER) generation and verification engine, information associated with a credential of a user for proving the user's identity or qualifications. The '531 Accused Products generate a token to act in place as a primary account number (PAN) and then use that token to verify the identity of the cardholder before a transaction is processed by a merchant. The "officially verifiable electronic representation (OVER) generation and verification engine" is the Visa Network that implements Visa Token Service. The PAN (and potentially other cardholder information) is stored in Visa's digital Token Vault—the repository for maintaining tokens.[8] The "credential" is the user's Visa credit card, which proves the user's qualification to make a purchase.

20. The '531 Accused Products also implement a method for receiving, from an OVER file storage client device of the user, an OVER file generation request to provide authentication of the user based on the information associated with the credential. The "OVER file storage client device of the user" is the user's phone. A digital wallet (e.g., Apple Pay, Android Pay, or Samsung Pay) on the user's phone acts as a "Token Requestor" sending an "OVER file generation request" to the Visa Token Service seeking the generation of a payment token.[9] The OVER file generation request sent by the Token Requester includes the PAN (and potentially other cardholder information), which is the "information associated with the credential." The OVER file generated

---

[8] Token Service Provider, https://usa.visa.com/dam/VCOM/regional/na/us/partner-with-us/documents/token-service-provider-product-factsheet.pdf, Pages 1-2.

[9] All you need to know about Tokenization, https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf.

by the Visa Token Service includes the token and potentially other information such as a Token Assurance Level, which is an indication of the confidence level that the token represents the correct PAN and cardholder. This OVER file authenticates the user based on at least the PAN.[10]

21. Additionally, the '531 Accused Products involve generation, by a processor of an OVER engine of an OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential, based on the information associated with the credential of the user. When a consumer initiates a digital payment through a digital wallet, the digital payment service provider requests a payment token (associated with the PAN, i.e., the information associated with the credential of the user) from Visa for the enrolled account. Visa (the "OVER engine") then generates a token and shares it with the credit card issuer (the "issuing agency") for approval. The token is the "virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential." The credit card issuer checks the PAN to determine if it corresponds to the user, and therefore if the associated token corresponds to that user. Once the issuing agency approves or verifies the token request, the token is ready to be sent back to the Token Requester for use.

22. The '531 Accused Products also transmit, to the OVER file storage client device of the user, the OVER file in response to the OVER file generation request. The OVER file, which contains at least the token, is sent back to the digital wallet on the user's phone as the response to the Token Request. The OVER file may also include additional information, such as the Token

[10] Visa Token Service Provisioning and Credential Management, Token Provisioning, https://developer.visa.com/capabilities/token-service-provisioning.

Assurance Level or card art used to provide a representation of the credit card on the user's phone.[11]

23. The '531 Accused Products also involve a method for receiving from an OVER file third-party client verifying device, a verifying request to verify that the OVER file transmitted to the user authenticates the user based on a scan associated with the OVER file on the OVER file store client device of the user. The Visa Token Service enables digital payment services in-store, online, and in-app. When the consumer makes an in-store payment, the consumer places their device near a payment terminal. The "OVER file third-party client verifying device" refers to a point of sale ("POS") terminal at the merchant that processes payment transactions. The "OVER file stor[age] client device of the user" is the user's phone. The merchant, via a POS terminal, initiates token processing by sending a Token Payment Request (i.e., a verifying request), which is received by the Visa Network.[12]

24. The '531 Accused Products also involve a method for verifying that the scan associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine, in response to the verifying request. The Visa Network verifies, in response to a verifying request, that the scan associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine. In response to a proximity-payment request (i.e., scan associated with the OVER file) at the POS

---

[11] All you need to know about Tokenization, https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf; EMV Payment Tokenisation Specification Technical Framework v2.3, https://www.emvco.com/specifications/emv-payment-tokenisation-specification-technical-framework/, Page 90.

[12] EMV Payment Tokenisation A Guide to Use Cases v2.2.1, https://www.emvco.com/specifications/emv-payment-tokenisation-a-guide-to-use-cases-2/, Page 43.

terminal, the Visa Network verifies that the token correlates to the PAN, i.e., the information associated with the credential of the user.

25. The ’531 Accused Products also involve a method for transmitting, to the OVER file third-party client verifying device, an authentication message comprising an indication of whether the scan associated with the OVER file on the device of the user corresponds to the information associated with the credential of the user that is stored in the Visa Network. A payment authorization message (i.e., authentication message) is sent to the POS terminal indicating whether the transaction has been approved. If the transaction is approved, the authorization message indicates that the token originally provided by the user corresponds to the credential stored by Visa Token Service.

26. Upon information and belief, by as early as April, 2016, and at least as of January 27, 2023 when Visa was served with the complaint in this Action, Visa had actual knowledge of the ’531 Patent and the infringing nature of the Accused Products.

27. In addition, Visa has indirectly infringed and continues to indirectly infringe the ’531 Patent in violation of 35 U.S.C. § 271(b). Visa has actively induced issuer banks, merchants, retailers, independent developers, and/or end users of the Accused Products to directly infringe the ’531 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the Accused Products in various websites, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the ’531 Accused Products. For example, Visa, through EMVCo, publishes a 106-page “Payment Tokenisation Specification Technical Framework” that provides detailed instructions on how to implement a tokenization program, with the express purpose of “defin[ing] a basis of Payment Tokenisation by providing a level of commonality across the

payment ecosystem to support adoption."[13] EMVCo's companion payment tokenization use guide (spanning 187 pages) provides guidance on various ways in which payment tokens can be used, and acknowledges that "implementation of this document may violate, infringe, or otherwise exercise the patent … or other intellectual property rights of third parties."[14] Visa also operates a "developer center" website that provides "application program interfaces" (i.e., software) and offers tutorials and webinars on how to implement Visa's technological solutions, including the Visa Token Service.[15] Through its developer center, Visa provides instructions to "Issuer Banks," "Merchants," and "Independent Developers" on how to implement Visa Token Service,[16] and supplies application program interfaces that aid in tokenization processes.[17] Visa's website advertises that its "tokenization technologies can empower banks, merchants and the wider payments ecosystem to boost authorization, drive innovation and create new digital commerce experiences for everyone."[18] Visa-owned CyberSource advertises to retailers "a suite of fast, comprehensive solutions" to "accelerate your business's adoption of emerging network

---

[13] EMV Payment Tokenisation Specification Technical Framework v2.3, https://www.emvco.com/specifications/emv-payment-tokenisation-specification-technical-framework/, Page 1.

[14] EMV Payment Tokenisation A Guide to Use Cases v2.2.1, https://www.emvco.com/specifications/emv-payment-tokenisation-a-guide-to-use-cases-2/, Page i.

[15] About Visa Developer, https://developer.visa.com/developer_program.

[16] Visa Token Service, https://developer.visa.com/capabilities/vts.

[17] Visa Token Service Provisioning and Credential Management, https://developer.visa.com/capabilities/token-service-provisioning.

[18] The Token Transformation, https://usa.visa.com/partner-with-us/payment-technology/visa-tokenization.html.

tokenization technologies."[19] The CyberSource "Guide to Network Tokenization" touts the security and economic benefits of tokenization and offers "modular solutions" to businesses around the globe.[20] Through CyberSource, Visa offers publicly available developer guides that provide detailed instructions to purchasers of CyberSource's "Token Management Service" software on how to implement a tokenization service.[21]

28. Visa does so knowing and intending that its customers and end users will commit these infringing acts. Visa also continues to make, use, offer for sale, sell, and/or import the '531 Accused Products, despite its knowledge of the '531 Patent, thereby specifically intending for and inducing its customers to infringe the '531 Patent through the customers' normal and customary use of the '531 Accused Products.

29. In addition, Visa has indirectly infringed and continues to indirectly infringe the '531 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the '531 Accused Products with knowledge that they are especially designed or adapted to operate in a manner that infringes that patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

30. For example, Visa is aware that the Visa Token Service included in the '531 Accused Products enables such products to operate as described above and that such functionality infringes the '531 Patent, including claim 1. Visa continues to sell and offer to sell such products

---

[19] A Guide to Network Tokenization, https://www.cybersource.com/content/dam/documents/en/network-tokenization-guide-en-us.pdf, Page 7.

[20] *Id.* at 7, 11-12.

[21] *See, e.g.,* Token Management Service, REST API, https://developer.cybersource.com/content/dam/docs/cybs/en-us/tms/developer/ctv/rest/tms.pdf.

in the United States after receiving notice of the ’531 Patent and how the products’ functionality infringes that patent.

31. The infringing aspects of the ’531 Accused Products can be used only in a manner that infringes the ’531 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities have no meaningful use other than in payment tokenization, let alone any meaningful non-infringing use.

32. Cortex has suffered damages as a result of Visa’s direct and indirect infringement of the ’531 Patent in an amount adequate to compensate for Visa’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Visa, together with interest and costs as fixed by the Court.

Count 2
(Infringement of the ’854 Patent)

33. Cortex repeats and re-alleges the allegations in the preceding paragraphs as if fully set forth herein.

34. On April 24, 2018, the U.S. Patent & Trademark Office duly and legally issued the ’854 Patent entitled “File format and platform for storage and verification of credentials.” A true and correct copy of the ’854 Patent is attached as Exhibit 2 to this Complaint.

35. Cortex is the owner of all rights, title, and interest in and to the ’854 Patent, including the right to assert all causes of action arising under the ’854 Patent and the right to any remedies for the infringement of the ’854 Patent.

36. Claim 15 of the ’854 Patent recites:

> 15. A non-transitory computer-readable medium comprising instructions that, when executed by a processor, cause the processor to perform operations comprising:
>
> accessing a first OVER file stored on a first OVER file client device, the first OVER file comprising:

a first virtual representation of an original credential that has been verified by an issuing agency to be a first official representation of the original credential of a user for proving the user's identity or qualifications, based on information associated with the original credential of the user, wherein the first OVER file is itself a first credential of the user;

the first OVER file generated by an OVER engine configured to:

store the information associated with the original credential of the user; and

transmit the first generated OVER file to the first OVER file client device;

transmitting to the OVER engine a first verifying request to verify that the first OVER file accessed from the first OVER file client device authenticates the user;

receiving a first authentication message comprising a first indication of whether a first scan associated with the first OVER file on the first OVER file client device of the user corresponds to the information associated with the original credential of the user that is stored in the OVER engine;

outputting a first status indicator expressing whether the first OVER file authenticates the user;

accessing a second OVER file stored on a second OVER file client device of the user, the second OVER file comprising a second virtual representation of the original credential that has been verified by the issuing agency to be a second official representation of the original credential that is invalid for use in the first OVER file client device for authenticating the user, wherein the second OVER file is itself a second new credential over the first OVER file and the original credential;

transmitting to the OVER engine a second verifying request to verify that the second OVER file scanned at the second client device authenticates the user;

receiving a second authentication message comprising a second indication of whether the second scan associated with the second OVER file on the device of the user corresponds to the information associated with the original credential of the user that is stored in the OVER engine; and

outputting a second status indicator expressing whether the second OVER file authenticates the user.

37. Visa has directly infringed and continues to directly infringe, literally and/or under the doctrine of equivalents, one or more claims, including at least claim 15, of the '854 Patent in violation of 35 U.S.C. § 271(a) because Visa makes, uses, offers for sale, and/or sells certain products ("'854 Accused Products"), including within this Judicial District, such as the VTS. Visa's infringing use of the '854 Accused Products includes its internal use and testing of the '854 Accused Products.

38. The '854 Accused Products satisfy all claim limitations of one or more of the claims of the '854 Patent, including at least claim 15. To the extent a claim limitation is not met literally, it is met under the doctrine of equivalents because any differences between the '854 Accused Products and the claims in the '854 Patent are insubstantial.

39. For example, the '854 Accused Products involve a non-transitory computer-readable medium comprising instructions that, when executed by a processor, cause the processor to access a first OVER file stored on a first OVER file client device. The Visa Token Service is executed through instructions stored on a computer-based medium.[22] The "first OVER file" correlates to a token produced by Visa's Token Vault. A "first OVER file client device" is a user device, typically a phone, that stores the token. Visa Token Service comprises a process whereby the token is used by the client device to process digital transactions.[23]

40. The '854 Accused Products also involve a first OVER file comprising a first virtual representation of an original credential that has been verified by an issuing agency to be a first

[22] *See* EMV Payment Tokenisation Specification Technical Framework v2.3, https://www.emvco.com/specifications/emv-payment-tokenisation-specification-technical-framework/, Page 10.

[23] *See* All you need to know about Tokenization, https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf.

official representation of the original credential of a user for proving the user's identity or qualifications, based on information associated with the original credential of the user, wherein the first OVER file is itself a first credential of the user. The token (i.e., "first OVER file") acts a first virtual representation of the user's credentials, such as the user's PAN.[24] The token functions as the first credential of the user, which establishes their qualifications to perform a digital transaction.

41. The '854 Accused Products also involve a first OVER file generated by an OVER engine, which is configured to store the information associated with the original credential of the user and transmit the first generated OVER file to the first OVER file client device. The Visa Network functions as the "OVER engine." The Visa Network includes the Token Vault, which stores the user's original credentials and generates a token, which is transmitted to the client device.[25]

42. The '854 Accused Products also include instructions that cause a processor to transmit to the OVER engine a first verifying request to verify that the first OVER file accessed from the first OVER file client device authenticates the user. When a client initiates a payment, the user transmits a token to the OVER engine (Visa Network) for verification. Visa sends the

---

[24] Token Service Provider, https://usa.visa.com/dam/VCOM/regional/na/us/partner-with-us/documents/token-service-provider-product-factsheet.pdf; *see also* Primary Account Number (PAN): What It Is, How It Works on Cards, https://www.investopedia.com/terms/p/primary-account-number-pan.asp.

[25] EMV Payment Tokenisation Specification Technical Framework v2.3, https://www.emvco.com/specifications/emv-payment-tokenisation-specification-technical-framework/, Pages 21, 49-50.

token, along with the payment card details, to the card issuer for authorization.[26] The card issuer accepts or declines the transaction and sends its response back to Visa.

43. The '854 Accused Products also include instructions that cause a processor to receive a first authentication message comprising a first indication of whether a first scan associated with the first OVER file on the first OVER file client device of the user corresponds to the information associated with the original credential of the user that is stored in the OVER engine. The user begins a transaction with a merchant via a scan of the first OVER file at the POS terminal. The merchant POS terminal must have the ability to scan the OVER file stored in the digital wallet on the client device, such as through NFC (near-field communication) or a card reader.[27] The merchant processes the requested transaction by sending a verification request to Visa Token Service to verify that the token corresponds to the PAN, which thereby authenticates the user.

44. The '854 Accused Products also include instructions that cause a processor to output a first status indicator expressing whether the first OVER file authenticates the user. When the user initiates payment, the user sends the first OVER file to Visa Network for authentication.

---

[26] EMV Payment Tokenisation A Guide to Use Cases v2.2.1, https://www.emvco.com/wp-content/uploads/documents/EMVCo-Payment-Tokenisation-A-Guide-To-Use-Cases-v2.2.pdf, Page 154.

[27] All you need to know about Tokenization, https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf; *see* EMV Payment Tokenisation Specification Technical Framework v2.3, https://www.emvco.com/specifications/emv-payment-tokenisation-specification-technical-framework/, Page 130.

Once that first OVER file is verified by Visa Network and the card issuer, a first status indicator is sent to Visa Network and to the merchant.[28]

45. The '854 Accused Products also include instructions that cause a processor to access a second OVER file stored on a second OVER file client device of the user, the second OVER file comprising a second virtual representation of the original credential that has been verified by the issuing agency to be a second official representation of the original credential that is invalid for use in the first OVER file client device for authenticating the user, wherein the second OVER file is itself a second new credential over the first OVER file and the original credential. The second OVER file corresponds to a second OVER file client device, i.e., a second mobile phone. The second OVER file, or token, becomes the second virtual representation to the original credentials, i.e., the user's PAN and other information.[29]

46. The '854 Accused Products also include instructions that comprise transmitting to the OVER engine a second verifying request to verify that the second OVER file scanned at the second client device authenticates the user. When the user transmits a second token (i.e., a second OVER file associated with a second OVER file user device), the Visa Network sends the token, along with the payment card details, to the card issuer for authorization. The card issuer accepts or declines the transaction and sends its response back to the Visa Network.

47. The '854 Accused Products also include instructions that cause a processor to receive a second authentication message comprising a second indication of whether the second

---

[28] EMV Payment Tokenisation Specification Technical Framework v2.3, https://www.emvco.com/specifications/emv-payment-tokenisation-specification-technical-framework/, Page 82.

[29] *See* All you need to know about Tokenization, https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf (Steps 2 & 5).

scan associated with the second OVER file on the device of the user corresponds to the information associated with the original credential of the user that is stored in the OVER engine. The merchant processes the requested transaction by sending a second verification request to the Visa Token Service to verify that the second token corresponds to the PAN.[30]

48. The '854 Accused Products also include instructions that cause a processor to output a second status indicator expressing whether the second OVER file authenticates the user. When the user sends a second OVER file to the Visa Network for authentication, that file is verified by the Visa Network and the card issuer, and a second status indicator is sent to the Visa Network and to the merchant. The OVER engine may generate and maintain a status indicator for each stored OVER file credential configured to indicate whether the OVER file credential is currently valid.[31]

49. Visa has received notice and actual knowledge of the '854 Patent and the infringing nature of the accused product since at least January 27, 2023 when Visa was served with the complaint in this Action.

50. Since at least January 27, 2023 when Visa was served with the complaint in this Action, Visa has, thorough its actions, indirectly infringed and continues to indirectly infringe the '854 Patent in violation of 35 U.S.C. § 271(b). Visa has actively induced issuer banks, merchants, retailers, independent developers, and/or end users of the Accused Products to directly infringe the '854 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the Accused Products in various websites, including

---

[30] *Id*.

[31] EMV Payment Tokenisation A Guide to Use Cases v2.2, https://www.emvco.com/specifications/emv-payment-tokenisation-a-guide-to-use-cases-2/, Page 42.

providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the '854 Accused Products. For example, Visa, through EMVCo, publishes a 106-page "Payment Tokenisation Specification Technical Framework" that provides detailed instructions on how to implement a tokenization program, with the express purpose of "defin[ing] a basis of Payment Tokenisation by providing a level of commonality across the payment ecosystem to support adoption."[32] EMVCo's companion payment tokenization use guide (spanning 187 pages) provides guidance on various ways in which payment tokens can be used, and acknowledges that "implementation of this document may violate, infringe, or otherwise exercise the patent … or other intellectual property rights of third parties."[33] Visa also operates a "developer center" website that provides "application program interfaces" (i.e., software) and offers tutorials and webinars on how to implement Visa's technological solutions, including the Visa Token Service.[34] Through its developer center, Visa provides instructions to "Issuer Banks," "Merchants," and "Independent Developers" on how to implement Visa Token Service,[35] and supplies application program interfaces that aid in tokenization processes.[36] Visa's website advertises that its "tokenization technologies can empower banks, merchants and the wider payments ecosystem to boost authorization, drive innovation and create new digital commerce

---

[32] EMV Payment Tokenisation Specification Technical Framework v2.3, https://www.emvco.com/specifications/emv-payment-tokenisation-specification-technical-framework/, Page 1.

[33] EMV Payment Tokenisation A Guide to Use Cases v2.2.1, https://www.emvco.com/specifications/emv-payment-tokenisation-a-guide-to-use-cases-2/, Page i.

[34] About Visa Developer, https://developer.visa.com/developer_program.

[35] Visa Token Service, https://developer.visa.com/capabilities/vts.

[36] Visa Token Service Provisioning and Credential Management, https://developer.visa.com/capabilities/token-service-provisioning.

experiences for everyone."[37] Visa-owned CyberSource advertises to retailers "a suite of fast, comprehensive solutions" to "accelerate your business's adoption of emerging network tokenization technologies."[38] The CyberSource "Guide to Network Tokenization" touts the security and economic benefits of tokenization and offers "modular solutions" to businesses around the globe.[39] Through CyberSource, Visa offers publicly available developer guides that provide detailed instructions to purchasers of CyberSource's "Token Management Service" software on how to implement a tokenization service.[40]

51. Visa does so knowing and intending that its customers and end users will commit these infringing acts. Visa also continues to make, use, offer for sale, and/or sell the '854 Accused Products, despite its knowledge of the '854 Patent, thereby specifically intending for and inducing its customers to infringe the '854 Patent through the customers' normal and customary use of the '854 Accused Products.

52. Since at least January 27, 2023, when Visa was served with the complaint in this Action, Visa has indirectly infringed and continues to indirectly infringe the '854 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the '854 Accused Products with knowledge that they are especially designed or adapted to operate in a manner that infringes that patent and despite the fact that the infringing

---

[37] The Token Transformation, https://usa.visa.com/partner-with-us/payment-technology/visa-tokenization.html.

[38] A Guide to Network Tokenization, https://www.cybersource.com/content/dam/documents/en/network-tokenization-guide-en-us.pdf, Page 7.

[39] *Id.* at 7, 11-12.

[40] *See, e.g.,* Token Management Service, REST API, https://developer.cybersource.com/content/dam/docs/cybs/en-us/tms/developer/ctv/rest/tms.pdf.

technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

53. For example, Visa is aware that the technology described above included in the ’854 Accused Products enables such products to operate as described above and that such functionality infringes the ’854 Patent, including claim 15. Visa continues to sell and offer to sell such products in the United States after receiving notice of the ’854 Patent and how the products’ functionality infringes that patent.

54. The infringing aspects of the ’854 Accused Products can be used only in a manner that infringes the ’854 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities have no meaningful use other than in payment tokenization, let alone any meaningful non-infringing use.

55. Cortex has suffered damages as a result of Visa’s direct and indirect infringement of the ’854 Patent in an amount adequate to compensate for Visa’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Visa, together with interest and costs as fixed by the Court.

Count 3
(Infringement of the ’859 Patent)

56. Cortex repeats and re-alleges the allegations in the preceding paragraphs as if fully set forth herein.

57. On August 18, 2020, the U.S. Patent & Trademark Office duly and legally issued the ’859 Patent entitled “File format and platform for storage and verification of credentials.” A true and correct copy of the ’859 Patent is attached as Exhibit 3 to this Complaint.

58. Cortex is the owner of all rights, title, and interest in and to the ’859 Patent, including the right to assert all causes of action arising under the ’859 Patent and the right to any remedies for the infringement of the ’859 Patent.

59. Claim 1 of the ’859 Patent recites:

> 1. A computer-implemented method comprising:
>
> storing, in a memory of an officially verifiable electronic representation (OVER) generation and verification engine, information associated with a credential of a user for proving the user’s identity or qualifications, wherein said information is used to prove the user’s identity or qualifications;
>
> receiving, from an OVER file storage client device of the user, an OVER file generation request to provide authentication of the user based on the information associated with the credential, wherein the OVER file storage client device of the user is a first Near Field Communication (NFC) enabled device;
>
> generating, by a processor of the OVER engine, an OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential, based on the information associated with the credential of the user;
>
> transmitting, to the OVER file storage client device of the user, the OVER file in response to the OVER file generation request;
>
> receiving, from an OVER file third-party client verifying device that is a second NFC enabled device, a verifying request to verify that the OVER file transmitted to the user authenticates the user, based on a Near Field Communication (NFC) protocol-based communication associated with the OVER file on the OVER file storage client device of the user being transmitted to the OVER file third-party client verifying device via an NFC protocol;
>
> verifying that the NFC protocol-based communication associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine, in response to the verifying request; and
>
> transmitting, to the OVER file third-party client verifying device, an authentication message comprising an indication of whether the NFC protocol-based communication associated with the OVER file on the OVER file storage client device of the user corresponds to the information associated with the credential of the user that is stored in the OVER engine.

60. Visa has directly infringed and continues to directly infringe, literally and/or under the doctrine of equivalents, one or more claims, including at least claim 1, of the ’859 Patent in violation of 35 U.S.C. § 271(a) because Visa makes, uses, offers for sale, and/or sells certain products (“’859 Accused Products”), including within this Judicial District, such as VTS. Visa’s infringing use of the ’859 Accused Products includes its internal use and testing of the ’859 Accused Products.

61. The ’859 Accused Products satisfy all claim limitations of one or more of the claims of the ’859 Patent, including at least claim 1. To the extent a claim limitation is not met literally, it is met under the doctrine of equivalents because any differences between the ‘859 Accused Products and the claims in the ’859 Patent are insubstantial.

62. For example, the ’859 Accused Products implement a computer-based method for storing, in a memory of an officially verifiable electronic representation (OVER) generation and verification engine, information associated with a credential of a user for proving the user’s identity or qualifications, wherein said information is used to prove the user’s identity or qualifications. The ’859 Accused Products generate a token to act in place of a primary account number (“PAN”) and then uses the token to verify the identity of the cardholder before a transaction is processed by a merchant. The “officially verifiable electronic representation (OVER) generation and verification engine” is the Visa Network that implements the Visa Token Service. The PAN (and potentially other cardholder information) is stored in Visa’s digital Token Vault—the repository for maintaining tokens. The “credential” is the user’s Visa credit card, which proves the user’s identity and qualification to make a purchase.

63. The ’859 Accused Products also involve a method for receiving, from an OVER file storage client device of the user, an OVER file generation request to provide authentication of

the user based on the information associated with the credential, wherein the OVER file storage client device of the user is a first Near Field Communication (NFC) enabled device. The "OVER file storage client device of the user" is the user's phone. A digital wallet on the user's phone acts as a "Token Requestor" sending an "OVER file generation request" to the Visa Token Service seeking the generation of a payment token. The OVER file generation request sent by the Token Requester includes the PAN (and potentially other cardholder information), which is the "information associated with the credential."[41] The OVER file generated by the Visa Token Service includes the token (and potentially other information such as a Token Assurance Level) which authenticates the user based on at least the PAN. A user can make an in-store payment by waving the user's device near a payment terminal using Near-Field Communication (NFC). NFC is a short-range wireless connectivity technology that enables communication between devices when they are brought within a few centimeters of each other.[42] The merchant processes the requested NFC transaction by sending a verification request to Visa Token Service seeking to confirm that the token corresponds to the PAN, thereby authenticating the user.

64. Additionally, the method practiced by the '859 Accused Products involves generation, by a processor of an OVER engine of an OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential, based on the information associated with the credential of the user. When a consumer initiates a digital payment through a digital wallet, the digital payment service provider requests a

---

[41] *See* All you need to know about Tokenization, https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf; EMV Payment Tokenisation Specification Technical Framework v2.3, https://www.emvco.com/specifications/emv-payment-tokenisation-specification-technical-framework/, Page 10.

[42] What is near-field communication (NFC)?, https://www.techtarget.com/searchmobilecomputing/definition/Near-Field-Communication.

payment token (associated with the PAN, i.e., the information associated with the credential of the user) from Visa for the enrolled account. The Visa Network then generates a token and shares it with the credit card issuer for approval.[43] The token is the "virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential." The credit card issuer checks the PAN to determine if it correlates to the user, and thereby whether the associated token correlates to that user. Once the issuing agency approves or verifies the token Request, the token is ready to be sent back to the Token Requester for use.

65. The '859 Accused Products also transmit, to the OVER file storage client device of the user, the OVER file in response to the OVER file generation request. The "OVER file storage client device of the user" is the user's phone. The OVER file, which contains at least the token, is sent back to the digital wallet on the user's phone as the response to the Token Request.[44] The OVER file could include additional information, such as the Token Assurance Level or card art used to provide a representation of the credit card on the user's phone.

66. The '859 Accused Products also involve a method for receiving, from an OVER file third-party client verifying device that is a second NFC enabled device, a verifying request to verify that the OVER file transmitted to the user authenticates the user, based on a Near Field Communication (NFC) protocol-based communication associated with the OVER file on the OVER file storage client device of the user being transmitted to the OVER file third-party client verifying device via an NFC protocol. The Visa Token Service enables digital payment services in-store, online, and in-app. When the consumer makes an in-store payment, the consumer waves

---

[43] Token Service Provider, https://usa.visa.com/dam/VCOM/regional/na/us/partner-with-us/documents/token-service-provider-product-factsheet.pdf, Pages 1-2.

[44] *See* EMV Payment Tokenisation A Guide to Use Cases v2.2, https://www.emvco.com/wp-content/uploads/documents/EMVCo-Payment-Tokenisation-A-Guide-To-Use-Cases-v2.2.pdf, Page 154.

their device near the payment terminal, through an NFC protocol.[45] The "OVER file third-party client verifying device" refers to a POS terminal at the merchant that processes payment transactions. The "OVER file stor[age] client device of the user" is the user's phone. The merchant, via a POS terminal, initiates token processing by sending a Token Payment Request (i.e., a verifying request), which is received by the Visa Network.[46]

67. The '859 Accused Products also involve a method for verifying that the NFC protocol-based communication associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine, in response to the verifying request. The Visa Token Service verifies, in response to a verifying request, that the NFC protocol-based communication associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine.[47] In response to an NFC transaction request sent from the POS terminal, the Visa Network verifies that the token correlates to the PAN, i.e., the information associated with the credential of the user.

68. The '859 Accused Products also involve a method for transmitting, to the OVER file third-party client verifying device, an authentication message comprising an indication of whether the NFC protocol-based communication associated with the OVER file on the OVER file storage client device of the user corresponds to the information associated with the credential of the user that is stored in the OVER engine. Visa Network transmits a payment authorization

---

[45] *See, e.g.*, All you need to know about Tokenization, https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf.

[46] EMV Payment Tokenisation A Guide to Use Cases v2.2.1, https://www.emvco.com/specifications/emv-payment-tokenisation-a-guide-to-use-cases-2/, Page 43.

[47] *Id*. at 42.

message (i.e., authentication message) to the merchant POS terminal indicating whether the transaction has been approved.[48] If the transaction is approved, the authorization message indicates that the token originally provided by the user via NFC (i.e., "the NFC protocol-based communication associated with the OVER file") corresponds to the credential stored by Visa Token Service.

69. Visa has received notice and actual knowledge of the '859 Patent and the infringing nature of the accused product since at least January 27, 2023 when Visa was served with the complaint in this Action.

70. Since at least January 27, 2023 when Visa was served with the complaint in this Action, Visa has, thorough its actions, indirectly infringed and continues to indirectly infringe the '859 Patent in violation of 35 U.S.C. § 271(b). Visa has actively induced issuer banks, merchants, retailers, independent developers, and/or end users of the Accused Products to directly infringe the '859 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the Accused Products in various websites, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the '859 Accused Products. For example, Visa, through EMVCo, publishes a 106-page "Payment Tokenisation Specification Technical Framework" that provides detailed instructions on how to implement a tokenization program, with the express purpose of "defin[ing] a basis of Payment Tokenisation by providing a level of commonality across the

[48] *See* All you need to know about Tokenization, https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf.

payment ecosystem to support adoption."[49] EMVCo's companion payment tokenization use guide (spanning 187 pages) provides guidance on various ways in which payment tokens can be used, and acknowledges that "implementation of this document may violate, infringe, or otherwise exercise the patent … or other intellectual property rights of third parties."[50] Visa also operates a "developer center" website that provides "application program interfaces" (i.e., software) and offers tutorials and webinars on how to implement Visa's technological solutions, including the Visa Token Service.[51] Through its developer center, Visa provides instructions to "Issuer Banks," "Merchants," and "Independent Developers" on how to implement Visa Token Service,[52] and supplies application program interfaces that aid in tokenization processes.[53] Visa's website advertises that its "tokenization technologies can empower banks, merchants and the wider payments ecosystem to boost authorization, drive innovation and create new digital commerce experiences for everyone."[54] Visa-owned CyberSource advertises to retailers "a suite of fast, comprehensive solutions" to "accelerate your business's adoption of emerging network

---

[49] EMV Payment Tokenisation Specification Technical Framework v2.3, https://www.emvco.com/specifications/emv-payment-tokenisation-specification-technical-framework/, Page 1.

[50] EMV Payment Tokenisation A Guide to Use Cases v2.2.1, https://www.emvco.com/specifications/emv-payment-tokenisation-a-guide-to-use-cases-2/, Page i.

[51] About Visa Developer, https://developer.visa.com/developer_program.

[52] Visa Token Service, https://developer.visa.com/capabilities/vts.

[53] Visa Token Service Provisioning and Credential Management, https://developer.visa.com/capabilities/token-service-provisioning.

[54] The Token Transformation, https://usa.visa.com/partner-with-us/payment-technology/visa-tokenization.html.

tokenization technologies."[55] The CyberSource "Guide to Network Tokenization" touts the security and economic benefits of tokenization and offers "modular solutions" to businesses around the globe.[56] Through CyberSource, Visa offers publicly available developer guides that provide detailed instructions to purchasers of CyberSource's "Token Management Service" software on how to implement a tokenization service.[57]

71. Visa does so knowing and intending that its customers and end users will commit these infringing acts. Visa also continues to make, use, offer for sale, and/or sell the '859 Accused Products, despite its knowledge of the '859 Patent, thereby specifically intending for and inducing its customers to infringe the '859 Patent through the customers' normal and customary use of the '859 Accused Products.

72. Since at least January 27, 2023 when Visa was served with the complaint in this Action, Visa has indirectly infringed and continues to indirectly infringe the '859 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the '859 Accused Products with knowledge that they are especially designed or adapted to operate in a manner that infringes that patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

73. For example, Visa is aware that the technology described above included in the '859 Accused Products enables such products to operate as described above and that such

---

[55] A Guide to Network Tokenization, https://www.cybersource.com/content/dam/documents/en/network-tokenization-guide-en-us.pdf, Page 7.

[56] *Id.* at 7, 11-12.

[57] *See, e.g.,* Token Management Service, REST API, https://developer.cybersource.com/content/dam/docs/cybs/en-us/tms/developer/ctv/rest/tms.pdf.

functionality infringes the ’859 Patent, including claim 1. Visa continues to sell and offer to sell such products in the United States after receiving notice of the ’859 Patent and how the products’ functionality infringes that patent.

74. The infringing aspects of the ’859 Accused Products can be used only in a manner that infringes the ’859 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities have no meaningful use other than in payment tokenization, let alone any meaningful non-infringing use.

75. Cortex has suffered damages as a result of Visa’s direct and indirect infringement of the ’859 Patent in an amount adequate to compensate for Visa’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Visa, together with interest and costs as fixed by the Court.

Count 4
(Infringement of the ’973 Patent)

76. Cortex repeats and re-alleges the allegations in the preceding paragraphs as if fully set forth herein.

77. On May 10, 2022, the U.S. Patent & Trademark Office duly and legally issued the ’973 Patent entitled “File format and platform for storage and verification of credentials.” A true and correct copy of the ’973 Patent is attached as Exhibit 4 to this Complaint.

78. Cortex is the owner of all rights, title, and interest in and to the ’973 Patent, including the right to assert all causes of action arising under the ’973 Patent and the right to any remedies for the infringement of the ’973 Patent.

79. Claim 1 of the ’973 Patent recites:

1. A computer-implemented method comprising:

storing, in a memory of an officially verifiable electronic representation (OVER) generation and verification engine, information associated with a credential of a user for proving the user's identity or qualifications;

receiving, from an OVER file storage client device of the user, an OVER file generation request to provide authentication of the user based on the information associated with the credential;

generating, by a processor of an OVER engine, an OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential, based on the information associated with the credential of the user;

transmitting, to the OVER file storage client device of the user, the OVER file in response to the OVER file generation request;

receiving, from an OVER file third-party client verifying device, a verifying request to verify that the OVER file transmitted to the user authenticates the user based on a Near Field Communication (NFC) protocol-based communication associated with the OVER file on the OVER file storage client device of the user;

verifying that the NFC protocol-based communication associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine, in response to the verifying request;

transmitting, to the OVER file third-party client verifying device, an authentication message comprising an indication of whether the NFC protocol-based communication associated with the OVER file on the OVER file storage client device of the user corresponds to the information associated with the credential of the user that is stored in the OVER engine;

requesting, by the processor of the OVER engine to the issuing agency, an agency authentication to validate the credential, wherein the issuing agency issued the credential of the user;

receiving, by the OVER engine, a status indicator and credential information associated with the credential;

and storing, by the OVER engine, the status indicator.

80. Visa has directly infringed and continues to directly infringe, literally and/or under the doctrine of equivalents, one or more claims, including at least claim 1, of the '973 Patent in violation of 35 U.S.C. § 271(a) because Visa makes, uses, offers for sale, and/or sells certain products ("'973 Accused Products"), including within this Judicial District, such as VTS. Visa's

infringing use of the ’973 Accused Products includes its internal use and testing of the ’973 Accused Products.

81. The ’973 Accused Products satisfy all claim limitations of one or more of the claims of the ’973 Patent, including at least claim 1. To the extent a claim limitation is not met literally, it is met under the doctrine of equivalents because any differences between the ‘973 Accused Products and the claims in the ‘973 Patent are insubstantial.

82. For example, the ’973 Accused Products implement a computer-based method for storing, in a memory of an officially verifiable electronic representation (OVER) generation and verification engine, information associated with a credential of a user for proving the user’s identity or qualifications. The ’973 Accused Products use a tokenization process that generates a token to act in place as a PAN and then uses the token to verify the identity of the cardholder before a transaction is processed by a merchant. The “officially verifiable electronic representation (OVER) generation and verification engine” is the Visa Network that implements Visa Token Service. The PAN is stored in Visa’s digital Token Vault.[58] The tokens could also include additional cardholder information such as a user’s address, account passwords or biometric data.

83. The ’973 Accused Products also involve a method for receiving, from an OVER file storage client device of the user, an OVER file generation request to provide authentication of the user based on the information associated with the credential. The “OVER file storage client device of the user” is the user’s phone. A digital payment service provider, i.e., a digital wallet on the user’s phone, acts as a “Token Requestor” sending an “OVER file generation request” to Visa

[58] *See* All you need to know about Tokenization, https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf; EMV Payment Tokenisation Specification Technical Framework v2.3, https://www.emvco.com/specifications/emv-payment-tokenisation-specification-technical-framework/, Page 10.

Token Service, which seeks the generation of a token[59]. The OVER file generation request sent by the Token Requester includes the PAN and potentially other cardholder information, which is the "information associated with the credential." The OVER file generated by Visa Token Service includes the token, which authenticates the user based on at least the PAN.[60]

84. Additionally, the method practiced by the '973 Accused Products involves generation of an OVER file comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential, based on the information associated with the credential of the user. The token is the "virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential." The token is generated by the Visa Token Service and mapped to a specific PAN.[61] The Visa Token Service sends the Token Request to the issuing agency (i.e., the credit card issuer) to get verification or approval. The information sent to the issuing agency includes at least the PAN (i.e., information associated with the credential of the user). The credit card issuer checks the PAN to determine if it correlates to the user, and thereby whether the associated token correlates to that user.[62] Once the issuing agency approves or verifies the Token Request, the token is ready to be sent back to the Token Requester for use.

---

[59] Token Service Provider, https://usa.visa.com/dam/VCOM/regional/na/us/partner-with-us/documents/token-service-provider-product-factsheet.pdf, Pages 1-2.

[60] EMV Payment Tokenisation Specification Technical Framework v2.3, https://www.emvco.com/specifications/emv-payment-tokenisation-specification-technical-framework/, Page 21.

[61] *See* Visa Token Service Provisioning and Credential Management, https://developer.visa.com/capabilities/token-service-provisioning, Page 4.

[62] EMV Payment Tokenisation Specification Technical Framework v2.3, https://www.emvco.com/specifications/emv-payment-tokenisation-specification-technical-framework/, Page 31.

85. The ’973 Accused Products also transmit, to the OVER file storage client device of the user, the OVER file in response to the OVER file generation request. The “OVER file storage client device of the user” is the user’s phone. The OVER file, which contains at least the token, is sent back to the digital wallet on the user’s phone as the response to the Token Request. The OVER file could include additional information, such as card art used to provide a representation of the credit card on the user’s phone.

86. The ’973 Accused Products also involve a method for receiving from an OVER file third-party client verifying device, a verifying request to verify that the OVER file transmitted to the user authenticates the user based on a Near Field Communication (NFC) protocol-based communication associated with the OVER file on the OVER file storage client device of the user. The “OVER file third-party client verifying device” is a point of sale (“POS”) terminal at the merchant that processes payment transactions. The “OVER file stor[age] client device of the user” is the user’s phone. The merchant POS terminal must have the ability to scan the OVER file stored in the digital wallet on the user’s phone, such as through an NFC or a card reader. The OVER file is a file that includes at least the token and may include additional information, such as a Token Assurance Level.

87. The ’973 Accused Products also involve a method for verifying that the NFC protocol-based communication associated with the OVER file corresponds with the information associated with the credential of the user that is stored in the OVER engine, in response to the verifying request. The POS terminal provides the token and related data for the merchant from an NFC protocol. The merchant then initiates a token payment request. In response, the Visa Network

verifies that the request (i.e., the NFC protocol-based communication) corresponds with the token (i.e., the information associated with the credential of the user) stored in the OVER engine.[63]

88. The '973 Accused Products also involve a method for transmitting, to the OVER file third-party client verifying device, an authentication message comprising an indication of whether the NFC protocol-based communication associated with the OVER file on the OVER file storage client device of the user corresponds to the information associated with the credential of the user that is stored in the OVER engine. Visa Network transmits a payment authorization message to the merchant POS terminal, the OVER file third-party client verifying device, indicating whether the transaction has been approved. If the transaction is approved, the authorization message indicates that the token originally provided from the user device via NFC (i.e., the NFC protocol-based communication associated with the OVER file) corresponds to the user's credential, which is stored by the Visa Token Service.[64]

89. The '973 Accused Products also involve a method for requesting, by the processor of the OVER engine to the issuing agency, an agency authentication to validate the credential, wherein the issuing agency issued the credential of the user. The Visa Network requests validation from the card issuer (i.e., the issuing agency) that the token corresponds to the user's PAN.[65]

90. The '973 Accused Products also involve a method for receiving, by the OVER engine, a status indicator and credential information associated with the credential. The Visa

---

[63] EMV Payment Tokenisation A Guide to Use Cases v2.2.1, https://www.emvco.com/wp-content/uploads/documents/EMVCo-Payment-Tokenisation-A-Guide-To-Use-Cases-v2.2.pdf, Page 154.

[64] *Id*.

[65] *See* All you need to know about Tokenization, https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf.

Network, the OVER engine, shares the token request with the card issuer, which authenticates the user by verifying that user's password or identity information. Once verified, the issuer sends an Authentication Successful status (i.e., a status indicator and credential information associated with the credential) to the Visa Network which in turn conveys it to the merchant.

91. The '973 Accused Products also involve a method for storing, by the OVER engine, the status indicator. Visa Network utilizes an Authentication History Server to store data about authentication transactions on the Visa Network.

92. Visa has received notice and actual knowledge of the '973 Patent and the infringing nature of the accused product since at least January 27, 2023 when Visa was served with the complaint in this Action.

93. Since at least January 27, 2023 when Visa was served with the complaint in this Action, Visa has, thorough its actions, indirectly infringed and continues to indirectly infringe the '973 Patent in violation of 35 U.S.C. § 271(b). Visa has actively induced issuer banks, merchants, retailers, independent developers, and/or end users of the Accused Products to directly infringe the '973 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the Accused Products in various websites, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the '973 Accused Products. For example, Visa, through EMVCo, publishes a 106-page "Payment Tokenisation Specification Technical Framework" that provides detailed instructions on how to implement a tokenization program, with the express purpose of "defin[ing] a basis of Payment Tokenisation by providing a level of commonality across the

payment ecosystem to support adoption."[66] EMVCo's companion payment tokenization use guide (spanning 187 pages) provides guidance on various ways in which payment tokens can be used, and acknowledges that "implementation of this document may violate, infringe, or otherwise exercise the patent … or other intellectual property rights of third parties."[67] Visa also operates a "developer center" website that provides "application program interfaces" (i.e., software) and offers tutorials and webinars on how to implement Visa's technological solutions, including the Visa Token Service.[68] Through its developer center, Visa provides instructions to "Issuer Banks," "Merchants," and "Independent Developers" on how to implement Visa Token Service,[69] and supplies application program interfaces that aid in tokenization processes.[70] Visa's website advertises that its "tokenization technologies can empower banks, merchants and the wider payments ecosystem to boost authorization, drive innovation and create new digital commerce experiences for everyone."[71] Visa-owned CyberSource advertises to retailers "a suite of fast, comprehensive solutions" to "accelerate your business's adoption of emerging network

---

[66] EMV Payment Tokenisation Specification Technical Framework v2.3, https://www.emvco.com/specifications/emv-payment-tokenisation-specification-technical-framework/, Page 1.

[67] EMV Payment Tokenisation A Guide to Use Cases v2.2.1, https://www.emvco.com/specifications/emv-payment-tokenisation-a-guide-to-use-cases-2/, Page i.

[68] About Visa Developer, https://developer.visa.com/developer_program.

[69] Visa Token Service, https://developer.visa.com/capabilities/vts.

[70] Visa Token Service Provisioning and Credential Management, https://developer.visa.com/capabilities/token-service-provisioning.

[71] The Token Transformation, https://usa.visa.com/partner-with-us/payment-technology/visa-tokenization.html.

tokenization technologies."[72] The CyberSource "Guide to Network Tokenization" touts the security and economic benefits of tokenization and offers "modular solutions" to businesses around the globe.[73] Through CyberSource, Visa offers publicly available developer guides that provide detailed instructions to purchasers of CyberSource's "Token Management Service" software on how to implement a tokenization service.[74]

94. Visa does so knowing and intending that its customers and end users will commit these infringing acts. Visa also continues to make, use, offer for sale, and/or sell the '973 Accused Products, despite its knowledge of the '973 Patent, thereby specifically intending for and inducing its customers to infringe the '973 Patent through the customers' normal and customary use of the '973 Accused Products.

95. Since at least January 27, 2023 when Visa was served with the complaint in this Action, Visa has indirectly infringed and continues to indirectly infringe the '973 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the '973 Accused Products with knowledge that they are especially designed or adapted to operate in a manner that infringes that patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

96. For example, Visa is aware that the technology described above included in the '973 Accused Products enables such products to operate as described above and that such

---

[72] A Guide to Network Tokenization, https://www.cybersource.com/content/dam/documents/en/network-tokenization-guide-en-us.pdf, Page 7.

[73] *Id.* at 7, 11-12.

[74] *See, e.g.,* Token Management Service, REST API, https://developer.cybersource.com/content/dam/docs/cybs/en-us/tms/developer/ctv/rest/tms.pdf.

functionality infringes the ’973 Patent, including claim 1. Visa continues to sell and offer to sell such products in the United States after receiving notice of the ’973 Patent and how the products’ functionality infringes that patent.

97. The infringing aspects of the ’973 Accused Products can be used only in a manner that infringes the ’973 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities have no meaningful use other than in payment tokenization, let alone any meaningful non-infringing use.

98. Cortex has suffered damages as a result of Visa’s direct and indirect infringement of the ’973 Patent in an amount adequate to compensate for Visa’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Visa, together with interest and costs as fixed by the Court.

Willful Infringement of the ’531 Patent

99. Cortex repeats and re-alleges the allegations in the preceding paragraphs as if fully set forth herein.

100. Visa’s infringement of the ’531 Patent is willful and deliberate, entitling Cortex to increased damages under 35 U.S.C. § 284 and to attorneys’ fees and costs incurred in prosecuting this action pursuant to 35 U.S.C. § 285.

101. After speaking with representatives from Cortex about the ’531 Patent who informed Visa that the patent was infringed by nearly all wallet-solution providers on the market, Visa nonetheless continued to sell and offer for sale infringing products, including the Visa Token Service.

102. Visa has infringed and continues to infringe the ’531 Patent despite the fact that it knew that its conduct amounted to infringement of the ’531 Patent.

Demand for Jury Trial

103. Cortex hereby demands a jury trial for all issues so triable.

Prayer for Relief

WHEREFORE, Cortex requests the that the Court:

(a) enter judgment that Visa infringes one or more claims of the Asserted Patents literally and/or under the doctrine of equivalents;

(b) enter judgment that Visa has induced and/or contributed to infringement literally and/or under the doctrine of equivalents and continues to induce and/or contribute to infringement of one or more claims of the Asserted Patents;

(C) award Cortex damages, to be paid by Visa in an amount adequate to compensate Cortex for such damages, including enhanced damages, together with pre-judgment and post-judgment interest for the infringement by Visa of the Asserted Patents through the date such judgment is entered in accordance with 35 U.S.C. § 284;

(e) declare this case exceptional pursuant to 35 U.S.C. § 285; and

(f) award Cortex its costs, disbursements, attorneys' fees, and such further and additional relief as is deemed appropriate by this Court, and all other relief to which the Court finds Cortex is entitled.

Dated: April 10, 2023

Respectfully submitted,

By: /s/ Max L. Tribble, Jr.

Max L. Tribble, Jr.
Bar No. 20213950
Bryce T. Barcelo
Bar No. 24092081
SUSMAN GODFREY L.L.P.
1000 Louisiana Street, Suite 5100
Houston, Texas 77002-5096
Telephone: (713) 651-9366
Fax: (713) 654-6666
mtribble@susmangodfrey.com
bbarcelo@susmangodfrey.com

Kalpana Srinivasan
Bar No. 237460
Davida Brook (admitted *pro hac vice*)
Bar No. 275370
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, 14th Floor
Los Angeles, California 90067-6029
Telephone: (310) 789-3100
Fax: (310) 789-3150
ksrinivasan@susmangodfrey.com
dbrook@susmangodfrey.com

Tyler Finn (admitted *pro hac vice*)
Bar No. 5772215
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas, 32nd Floor
New York, New York 10019
Telephone: (212) 336-8330
Fax: (212) 336-8340
tfinn@susmangodfrey.com

Mark D. Siegmund
Bar No. 24117055
CHERRY JOHNSON SIEGMUND JAMES
400 Austin Avenue, Suite 903
Waco, Texas 76701
Telephone: (254) 732-2242
msiegmund@cjsjlaw.com

Ricardo G. Cedillo
Bar No. 04043600
Joseph Korbel
Bar No. 24127174
DAVIS CEDILLO & MENDOZA INC.
755 E. Mulberry Avenue, Suite 250
San Antonio, Texas 78212
Telephone: (210) 822-6666
Fax: (210) 660-3795
rcedillo@lawdcm.com
jkorbel@lawdcm.com

COUNSEL FOR PLAINTIFF CORTEX MCP, INC.

CERTIFICATE OF SERVICE

A true and correct copy of the foregoing instrument was served or delivered electronically via U.S. District Court [LIVE] – Document Filing System, to all counsel of record, on this the 10th day of April 2023.

/s/ Tyler Finn
TYLER FINN