

Filed on behalf of Cortex MCP, Inc.

By: Michelle E. Armond

Douglas R. Wilson

Patrick Maloney

Yue Han

ARMOND WILSON LLP

4685 MacArthur Court, Suite 390

Newport Beach, CA 92660

Telephone: (949) 932-0778

Email: ipr@armondwilson.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA INC.,
Petitioner,

v.

CORTEX MCP, INC.,
Patent Owner.

Case No. IPR2024-00486
U.S. Patent No. 9,251,531

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	BACKGROUND.....	4
	A. Security And Other Challenges In Mobile Payment Systems	4
	B. '531 Patent File History	7
III.	LEVEL OF ORDINARY SKILL IN THE ART.....	8
IV.	CLAIM CONSTRUCTION	8
	A. “OVER file”	9
	B. “scan”/“scanned”	9
	C. “verified by an issuing agency”	10
V.	VISA NEVER MET ITS BURDEN TO SHOW OBVIOUSNESS BASED ON OBOURNE (GROUNDS 1-4)	10
	A. All Claims: Osborne Did Not Teach Or Suggest An Issuing Agency Verification Of An “OVER file”	10
	1. Osborne Did Not Disclose Issuing Agency Verification	12
	2. The Petition Did Not Prove That Issuing Agency Verification Was Obvious Over Osborne	16
	a. Visa Has Not Met Its Burden To Show That Common Sense Substitutes For This Key Claim Limitation	17
	b. Digital Payment Systems Are Not Straightforward Technology	19
	c. The Petition Provides No Reasoned Analysis Or Evidence Showing Osborne’s Missing Feature Was Obvious	21

d.	Dr. Shamos’ Conclusory And Contradictory Testimony Provides No Evidence Of Obviousness	22
e.	The Petition Provides No Motivation To Modify Osborne To Address A Problem Osborne Already Solved.....	24
f.	Requiring Cortex To Disprove Any Motivation To Modify Osborne Invites Legal Error.....	27
g.	Visa Has Not Sustained Its Burden On Its Alternate Argument	29
B.	All Claims: The Petitions Never Establish <i>Prima Facie</i> Obviousness By Failing To Identify Osborne’s Alleged “OVER engine”	30
C.	The Petition Fails To Show Obviousness Of The Dependent Claims	34
1.	Claim 2	34
a.	Visa Does Not Show That Osborne Suggests “generating... a second OVER file”	36
b.	Visa Does Not Prove That Osborne Suggests “a second OVER file” That Is “invalid for use” In The First Device	38
2.	Claims 7 and 20	42
3.	Claims 8 and 29	44
4.	Claims 12-13.....	46
5.	Claim 19	47
6.	Claims 23-26 and 28-33	48

VI.	VISA NEVER MET ITS BURDEN TO SHOW OBVIOUSNESS BASED ON STAFFORD (GROUNDS 5-6)	51
A.	Visa Has Not Met Its Burden To Show That Stafford Teaches Or Suggests The Claimed “OVER File”	51
1.	Stafford’s Key Signatures Are Not “based on the information associated with the credential of the user”	52
2.	Stafford’s Key Signatures Are Not “verified by an issuing agency”	54
3.	Purves Also Did Not Teach Or Suggest The Claimed “virtual representation of the credential”	55
a.	Dr. Shamos’ Admission That Purves Never Stores The Card Images Shows They Do Not Satisfy the Claimed Requirements Of The “virtual representation” In The Claimed “OVER file”	55
b.	Purves Does Not Teach Using Card Images For Verification	57
4.	Visa’s Petition Does Not Establish A Motivation To Modify Stafford With Card Images or QR Codes From Purves	60
a.	There Is No Reason To Use Purves’ Card Images To Identify Stafford’s Single-Use Keys	60
b.	Using Purves’ Card Images or QR Codes Would Introduce Security Risks in Stafford’s Secure System	62
VII.	CONCLUSION	67

All emphasis is added in quoted material unless otherwise indicated.

TABLE OF AUTHORITIES

	Page No(s).
<i>Absolute Dental Servs. v. Watson Guide IP</i> , IPR2023-00177, 2023 WL 5047049 (P.T.A.B. May 4, 2023).....	60
<i>ActiveVideo Networks v. Verizon Commc’ns</i> , 694 F.3d 1312 (Fed. Cir. 2012)	50
<i>Alcon v. AMO Dev.</i> , IPR2021-00858, 2022 WL 17585777 (P.T.A.B. Dec. 12, 2022).....	45
<i>Apple v. Contentguard Holdings</i> , IPR2015-00453, 2015 WL 4467403 (P.T.A.B. July 13, 2015) ...	11, 17, 21, 23
<i>Arendi S.A.R.L. v. Apple</i> , 832 F.3d 1355 (Fed. Cir. 2016)	<i>passim</i>
<i>Becton, Dickinson v. Tyco Healthcare</i> , 616 F.3d 1249 (Fed. Cir. 2010)	33
<i>Belden v. Berk-Tek</i> , 805 F.3d 1064 (Fed. Cir. 2015)	36
<i>Cisco Sys. v. Centripetal Networks</i> , IPR2018-01655, 2019 WL 2004230 (P.T.A.B. May 6, 2019).....	61
<i>Dexcom v. WaveForm Techs.</i> , IPR2016-01680, 2018 WL 1137089 (P.T.A.B. Feb. 28, 2018)	27, 34
<i>DSS Tech. v. Apple Inc.</i> , 885 F.3d 1367 (Fed. Cir. 2018)	<i>passim</i>
<i>Engel Indus. v. Lockformer</i> , 96 F.3d 1398 (Fed. Cir. 1996)	33
<i>In re Gordon</i> , 733 F.2d 900 (Fed. Cir. 1984)	62

<i>Icon Health v. Strava</i> , 849 F.3d 1034 (Fed. Cir. 2017)	15
<i>Intelligent Bio-Sys. v. Illumina Cambridge</i> , 821 F.3d 1359 (Fed. Cir. 2016)	27, 31, 34
<i>K/S Himpp v. Hear-Wear Techs.</i> , 751 F.3d 1362 (Fed. Cir. 2014)	20
<i>Kyocera Senco v. Int’l Trade Comm’n</i> , 22 F.4th 1369 (Fed. Cir. 2022)	33
<i>In re Lee</i> , 277 F.3d 1338 (Fed. Cir. 2002)	28
<i>Litton Indus. v. Solid State Sys.</i> , 755 F.2d 158 (Fed. Cir. 1985)	60
<i>In re Magnum Oil Tools</i> , 829 F.3d 1364 (Fed. Cir. 2016)	23, 27
<i>Metalcraft of Mayville v. Toro Co.</i> , 848 F.3d 1358 (Fed. Cir. 2017)	38, 41, 49
<i>Mintz v. Dietz & Watson</i> , 679 F.3d 1372 (Fed. Cir. 2012)	18
<i>In re Nuvasive</i> , 842 F.3d 1376 (Fed. Cir. 2016)	16, 17
<i>One World Techs. v. Chevron</i> , PGR2020-00059, 2020 WL 7222691 (P.T.A.B. Dec. 7, 2020)	16
<i>Palo Alto Networks v. BT Ams.</i> , IPR2023-00888, Paper 12 (P.T.A.B. Apr. 1, 2024)	38, 41, 49
<i>Perfect Web Technologies v. InfoUSA</i> , 587 F.3d 1324 (Fed. Cir. 2009)	19
<i>Realtime Data v. Iancu</i> , 912 F.3d 1368 (Fed. Cir. 2019)	9

Visa v. Cortex MCP Patent No. 9,251,531 – IPR2024-00486	
<i>Redline Detection v. Star Envirotech</i> , 811 F.3d 435 (Fed. Cir. 2015)	62
<i>Securus Techs. v. Glob. Tel*Link</i> , 701 F. App’x 971 (Fed. Cir. 2017)	49
<i>Sisvel Int’l v. Sierra Wireless</i> , 82 F.4th 1355 (Fed. Cir. 2023)	49
<i>Streck v. Ravgen</i> , IPR2021-01577, Paper 62 (P.T.A.B. Apr. 18, 2023)	62
<i>Univ. of Strathclyde v. Clear-Vu Lighting</i> , 17 F.4th 155 (Fed. Cir. 2021)	64
<i>Vermeer Mfg. v. Toro Co.</i> , PGR2020-00081, 2021 WL 972419 (P.T.A.B. Mar. 15, 2021)	17, 22
<i>W.R. Grace v. Cochise Tech.</i> , IPR2023-01063, 2023 WL 8590764 (P.T.A.B. Dec. 11, 2023)	38
<i>Wi-LAN v. Apple</i> , 811 F.3d 455 (Fed. Cir. 2016)	34, 46
<i>Xerox Corp. v. Bytemark</i> , IPR2022-00624, 2022 WL 3648989 (P.T.A.B. Aug. 24, 2022)	<i>passim</i>
<i>Zero Gravity v. Footbalance Sys.</i> , IPR2015-01769, 2017 WL 505951 (P.T.A.B. Feb. 3, 2017)	15
<i>In re Zurko</i> , 258 F.3d 1379 (Fed. Cir. 2001)	22, 28
<i>Zurn Indus. v. Sioux Chief Mfg.</i> , IPR2018-00973, 2018 WL 5880931 (P.T.A.B. Nov. 8, 2018)	20, 21

OTHER AUTHORITIES

37 C.F.R. § 42.6.....	45
37 C.F.R. § 42.65.....	16
37 C.F.R. § 42.100.....	8
37 C.F.R. § 42.104.....	31
35 U.S.C. § 103	60
35 U.S.C. § 312	31
35 U.S.C. § 316	27

TABLE OF EXHIBITS

Exhibit No.	Description
2001	U.S. Patent No. 9,996,835 to Visa
2002	U.S. Patent Publication No. 2007/0208665 to Ohara (“Ohara”)
2003	U.S. Patent No. 8,540,149 to Chu (“Chu”)
2004	Defendant Visa Inc.’s Invalidity Contentions, <i>Cortex MCP, Inc. v. Visa Inc.</i> , Case No. 5:23-CV-05720 (N.D. Cal. Mar. 15, 2024)
2005	U.S. Patent Publication No. 2009/0307756 to Kang (“Kang”)
2006	U.S. Patent Publication No. 2012/0240204 to Bhatnagar et al., (“Bhatnagar”)
2007	Cortex’s Preliminary Claim Constructions and Extrinsic Evidence (Patent L.R. 4-2), <i>Cortex MCP, Inc. v. Visa Inc.</i> , Case No. 5:23-CV-05720 (N.D. Cal. Apr. 19, 2024)
2008	Visa Inc.’s Preliminary Claim Constructions and Evidence Pursuant to Patent L.R. 4-2, <i>Cortex MCP, Inc. v. Visa Inc.</i> , Case No. 5:23-CV-05720 (N.D. Cal. Apr. 19, 2024)
2009	Declaration of Dr. Sam Malek
2010	CV of Dr. Sam Malek
2011	Cortex’s Opening Claim Construction Brief, <i>Cortex MCP, Inc. v. Visa Inc.</i> , Case No. 5:23-CV-05720, Dkt. No. 99 (N.D. Cal. June 21, 2024)
2012	Visa’s Responsive Claim Construction Brief, <i>Cortex MCP, Inc. v. Visa Inc.</i> , Case No. 5:23-CV-05720, Dkt. No. 104 (N.D. Cal. July 12, 2024) (redacted in district court)
2013	Cortex’s Reply Claim Construction Brief, <i>Cortex MCP, Inc. v. Visa Inc.</i> , Case No. 5:23-CV-05720, Dkt. No. 105 (N.D. Cal. July 19, 2024)
2014	Parties Joint Claim Construction And Prehearing Statement, <i>Cortex MCP, Inc. v. Visa Inc.</i> , Case No. 5:23-CV-05720, Dkt. No. 89 (N.D. Cal. May 7, 2024) (excerpted)
2015	Docket for <i>Cortex MCP, Inc. v. Visa Inc.</i> , Case No. 5:23-CV-05720 (N.D. Cal.)

Exhibit No.	Description
2016	Transcript of September 25, 2024 Deposition of Dr. Michael Shamos
2017	Martin E. Hellman, <i>An Overview of Public Key Cryptography</i> , IEEE Communications Society Magazine (Nov. 1978)
2018	Christian Boyce, <i>iOS 8 Tip #8: Make and Answer Phone Calls From Your iPad</i> (Apr. 13, 2020), https://christianboyce.com/ios-8-tip-8-make-and-answer-phone-calls-from-your-ipad/#google_vignette
2019	Eric Dash, <i>Visa Seeks New Ways to Keep Data Secret</i> , N.Y. Times (Aug. 25, 2005), https://www.nytimes.com/2005/08/25/business/visa-seeks-new-waysto-keep-data-secret.html
2020	Eric Dash & Brad Stone, <i>Credit Card Processor Says Some Data Was Stolen</i> , N.Y. Times (Jan. 21, 2009), https://www.nytimes.com/2009/01/21/technology/21breach.html
2021	U.S. Dept. of Justice Press Release, <i>Justice Department Sues to Block Visa's Proposed Acquisition of Plaid</i> (Nov. 5, 2020), https://www.justice.gov/opa/pr/justice-department-sues-block-visas-proposed-acquisition-plaid
2022	Jennifer Surane & Leah Nylen, <i>Visa Faces DOJ Scrutiny for How It Prices 'Token' Technology</i> , Bloomberg (Aug. 16, 2023)
2023	U.S. Dept. of Justice Press Release, <i>Justice Department Sues Visa for Monopolizing Debit Markets</i> (Sept. 24, 2024), https://www.justice.gov/opa/pr/justice-department-sues-visa-monopolizing-debit-markets
2024	Lauren Hirsch & Danielle Kaye, <i>U.S. Accuses Visa of Monopoly in Debit Cards</i> , N.Y. Times (Sept. 24, 2024), https://www.nytimes.com/2024/09/24/business/dealbook/visa-antitrustlawsuit-debit-cards.html

I. INTRODUCTION

This saga began more than a decade ago, when Cortex invented a new concept to simplify and secure electronic payments using a verified tokenization technology called an “OVER file.” Visa and its subsidiaries initially expressed interest in the invention, gleaming the details under NDA over multiple meetings with Cortex in 2013 and 2016. EX1018 ¶¶10-11. But Visa soon dropped the pretense by deciding not to partner with Cortex, filing its own patents on a very similar technology and launching the Visa Token Service. 486-POPR at 10-11.

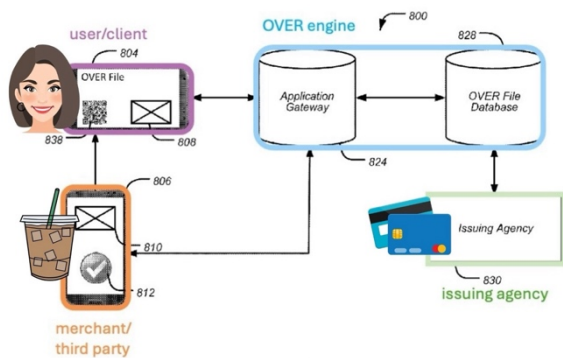


Fig. 11

**Cortex's Patent
'531 Patent, Fig. 11 (annotated)**

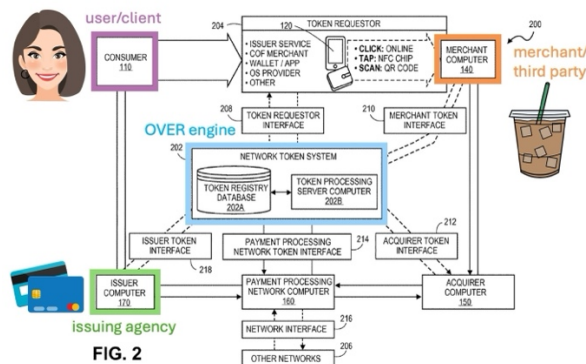


FIG. 2

**Visa's Later Patent
EX2001, Fig. 2 (annotated)**

Visa plainly benefitted from the increased security and innovative design conferred by Cortex's patented OVER file system. It then sought to take over the tokenization space and attracted the attention of government regulators when Visa reportedly came under investigation by the U.S. Department of Justice over

allegations it was “charging retailers more if they don’t use Visa’s proprietary ‘tokenization’ technology.” EX2022 at 1.

This was not the first time that Visa threw its market power around to benefit itself and stifle innovation. In 2020, the Justice Department successfully blocked a deal where “Visa intended to stamp out a nascent rival.” EX2024 at 2. In targeting that deal, the DOJ announced that: “Visa has dominated online debit for years and has protected its monopoly with exclusionary tactics that have prevented rivals” from entering. EX2021 at 2. Just last month, in September 2024, the Department filed yet another antitrust suit because Visa

illegally maintains a monopoly over debit network markets by using its dominance to thwart the growth of its existing competitors and ***prevent others from developing new and innovative alternatives.***

EX2023 at 1; *see also* EX2024 at 1.

After Cortex stood up to Visa, suing for patent infringement, Visa asked the Board to cancel Cortex’s patents covering the same technology in which Visa initially feigned interest. Visa overlooks that canceling patents for obviousness requires establishing a *prima facie* case. The Board found at institution that the Stafford grounds are insufficient. The Petition’s remaining Osborne grounds fare no better under further consideration.

Visa points out that during examination of the '531 application, the Examiner found that “[t]he closest prior art of record” did not teach the issuing agency verification of “an OVER file” required by every claim. 486-Pet. at 5 (quoting EX1007 at 20). Nonetheless, Visa’s Petition musters not a single prior art reference (including Osborne) teaching that key limitation.

Instead, Visa essentially argues that waving a magic wand with an incantation of common sense meets its burden here. Supplying a limitation entirely absent from Osborne requires more. Visa made no effort to meet the threshold requirements of invoking common sense, and ratifying its approach would only run afoul of the Federal Circuit’s decision in *Arendi* and its progeny. Certainly, placing the burden instead on Cortex to disprove obviousness is legally a non-starter. Dr. Shamos’ parroting of the Petition does not provide the evidence Visa needs: his testimony that adding verification would solve the problem of forged credentials in Osborne cannot be credited when his declaration also explained this problem was solved decades earlier “in 1967,” EX1005 ¶120, especially when Osborne discloses use of that very solution (user authentication). Nor does Visa or Dr. Shamos explain why one of skill would have replaced Osborne’s teachings of authentication with verification by an issuing agency.

Visa had to do better. Cortex respectfully requests that the Board confirm patentability of the claims over all grounds.¹

II. BACKGROUND

A. Security And Other Challenges In Mobile Payment Systems

Why do you rob banks? “Because that’s where the money is.” –Willie Sutton

Electronic payment systems face the most aggressive and widespread attacks in the world. Visa’s exhibits chronicle the ordeals. Protecting cardholder data in electronic payments is a “[d]aunting [c]hallenge.” EX1027 at 4-5. With financial fraud so lucrative, “cybercriminals are devising ever more sophisticated methods to access the data they desire.” EX1027 at 5. Two decades ago, the *New York Times* called Visa’s specific challenge “a herculean task, because virtually every step is outsourced from the time a card is swiped to the time the monthly statement arrives.” EX2019 at 1. Put mildly, combating the many flavors of financial fraud all at once is a complex challenge. EX2009 ¶¶63-82. A 2011 transaction processing patent Visa submitted here recognized “a long-felt but unresolved need exists for a system

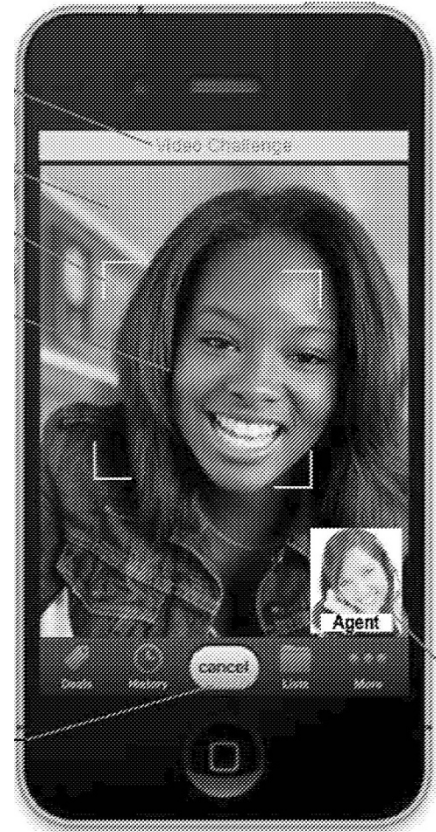
¹ After instituting review of IPR2024-00486 and -00487, both challenging the ’531 Patent, the Board consolidated them. Paper 10 at 2-3. Unless otherwise indicated, all exhibits cited herein are from the -00486 IPR.

or method that provides secure access to sensitive data, while maintaining the data format for easy utilization by existing systems.” EX1034 at 1:20, 1:47-50.

The decade leading up to the December 2012 filing of Cortex’s ’531 Patent witnessed an explosion of “data breaches exposing millions of customer records.” EX1020 at 2; *see also* EX1031 at 4-9 (summarizing data breaches). Visa and other credit card networks were hard hit. In 2005, a breach at payment processor CardSystems Solutions “exposed the personal information of more than 40 million cardholders.” EX2019 at 1; *see also* EX2020 at 1. Three years later, the infamous Heartland Payments Systems attack compromised 160 million accounts, EX1020 at 2, “in spite of the adoption of more stringent standards” and industry investment of “over \$2 billion” for improved security standards, EX2020 at 2.

Visa’s former CEO called the intrusions “akin to terrorist attacks; we must take very aggressive steps” because “[i]f trust is eroded, the very foundation of the system will be eroded.” EX2019 at 1. Visa submitted a 2010 paper observing that “such criminal efforts are increasing in organization and scale.” EX1031 at 1. Yet when presented with Cortex’s innovative solution to increase electronic payment security, Visa turned away and decided to go its own way. EX1018 ¶¶10-11; 486-POPR/487-POPR at 10-11.

One conventional form of electronic payment security was user authentication. Dr. Shamos testified that a challenge in digital payments was that “a digital credential can easily be copied, forged, or altered.” EX1005 ¶118. The solution “starting in 1967” was “to require the presenter of the credential to furnish additional information” to prove their identity. EX1005 ¶120. Dr. Shamos gave the example of “requiring the user to enter a PIN.” *Id.* Osborne also describes authenticating users for “preventing fraud” using “VerifyChat” to confirm identities via “a video chat” (shown at right) or “text challenge.” EX1011 ¶¶30-31, Fig. 3A (excerpted).



Other obstacles further hampered the adoption of existing electronic payment technologies. Despite the rapid growth of smartphones, mobile payments and mobile wallet systems lagged behind because existing payment methods, such as credit cards, proved ill-suited for storage on mobile devices. Some early mobile wallet applications physically embedded “secure element chips” into user devices, EX1018 ¶8, an option proposed by Osborne, EX1011 ¶26 (describing a “custom hardware authentication chip... embedded into the client”). Yet most phones did not

include these chips, and manufacturers were reluctant to redesign their phones to include them. EX1018 ¶8; *see also* 486-POPR/487-POPR at 7-8.

B. '531 Patent File History

After Cortex filed the '531 Patent application, the Examiner issued an office action rejecting all pending claims as obvious. EX1007 at 127-51; *see* 486-Pet./487-Pet. at 4. During an interview after Cortex amended the claims, the Examiner “communicated that additional searching would be performed.” EX1007 at 114. After another rejection, EX1007 at 60-91, in a second interview the Examiner suggested adding a limitation specifying the “difference between issuing agency and third party verifying device[] in claim 1 to get rid of any ambiguity.” EX1007 at 53. Cortex amended the claims to specify that the “OVER file” comprises “a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential.” EX1007 at 30; *see also* 486-POPR/487-POPR at 13-14.

The Examiner then allowed the claims, finding this limitation distinguished from “[t]he closest prior art of record”:

Allowable Subject Matter

1. The following is an examiner's statement of reasons for allowance:

The closest prior art of record, Ohara and Chu does not teach “generating 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”.

Similar reasoning is applied to independent claims 17 & 26.

EX1007 at 20; *see also* 486-Pet./487-Pet. at 4-5; 486-POPR/487-POPR at 14.

III. LEVEL OF ORDINARY SKILL IN THE ART

At institution, the Board found

that a person of ordinary skill in the art at the time of the alleged invention would typically have a bachelor's degree in computer science, computer engineering, or a related field, with at least two years of work involving electronic payment systems, network authentication systems, or related areas... [and] could have less education but significant professional experience in one or more of these fields.

486-DI at 6-7; 487-DI at 6 (internal quotation marks and citation omitted). Cortex agrees with this definition of the level of ordinary skill in the art. EX2009 ¶¶37-41.

IV. CLAIM CONSTRUCTION

Claims in an IPR are “construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” 37 C.F.R. §42.100(b).

The parties briefed claim construction to the district court. EX2011-EX2014; *see also* EX2015. Cortex maintains that claim construction is unnecessary to confirm patentability of the claims here. 486-POPR/487-POPR at 20-21; *Realtime Data v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe only those terms that are in controversy, and only to the extent necessary to resolve the controversy.” (cleaned up)); EX2009 ¶¶42-45.

A. “OVER file”

The Board held “that the term ‘OVER file’ encompasses a virtual representation of one or more credentials, to be used for verification of those credentials.” 486-DI at 9-10; 487-DI at 9. Although no construction of this term is required, EX2011 at 14, the claims may be confirmed under the Board’s construction, EX2009 ¶¶43, 46-48.

B. “scan”/“scanned”

The institution decision construed “scan” to “encompass[] an optical scan as well as an NFC interaction.” 486-DI at 12-13; 487-DI at 11-12 (citing EX1001 at 5:7-25, 11:64-12:29). Cortex maintains that no construction is necessary to confirm patentability. EX2009 ¶44. This term should be given its plain and ordinary meaning where the claimed “scan” encompasses optical scans, NFC, and Bluetooth. *E.g.*, EX1001 at 5:7-25, 11:64-12:29; *see also* EX2011 at 7-10; EX2013 at 7-10.

C. “verified by an issuing agency”

The Board applied Visa’s construction “that an issuing agency have verified a *virtual representation* in an OVER file as being an official representation of a credential.” 486-DI at 13 (emphasis in original); 487-DI at 12-13 (same). Cortex maintains that no construction is necessary to confirm the claims. Cortex agrees in substance with the Board’s construction, namely that the claimed “virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential” requires that the issuing agency has verified the “virtual representation” (and not the “credential”) to be “an official representation of the credential.” *See* EX2013 at 10-11; EX2009 ¶45.

V. VISA NEVER MET ITS BURDEN TO SHOW OBVIOUSNESS BASED ON OBORNE (GROUNDS 1-4)

A. All Claims: Osborne Did Not Teach Or Suggest An Issuing Agency Verification Of An “OVER file”

Every claim of the ’531 Patent requires 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.” *See* EX1001 at 21:24-28, 22:61-67, 23:39-43 (independent Claims 1, 15, 21). This was the same limitation the Examiner found absent from the closest prior art during prosecution. EX1007 at 20.

The Board did not address the Petition’s assertion that Osborne taught verification of the credential by an issuing agency. 486-DI/487-DI at 24-25. And

for good reason: Osborne does not show any verification of its alleged OVER files, much less verification by an issuing agency as an official representation of the credential.

Indeed, the Petition quickly pivots to obviousness, arguing that verification would be a “routine step” in Osborne’s system. 486-Pet. at 23; 487-Pet. at 24. Yet Visa cites no prior art disclosing the missing issuing agency verification limitation. Instead, it improperly relies on the common sense, or ordinary creativity, of one of skill. *Apple v. Contentguard Holdings*, IPR2015-00453, 2015 WL 4467403, at *8 (P.T.A.B. July 13, 2015). But in the wake of the Examiner finding this limitation absent from “[t]he closest prior art,” EX1007 at 20, the Petition pointing to no prior art showing this limitation gives lie to Visa’s claim that issuing agency verification was “common sense.” Further, Visa does not provide the reasoned analysis and evidentiary support necessary to fill a missing limitation, as required by the Federal Circuit in *Arendi*. Visa’s only cited support is Dr. Shamos’ conclusory and conflicting testimony, which repeats Visa’s attorney argument and is undermined by other testimony elsewhere in his declaration. Nor does Visa or Dr. Shamos address that Osborne already solved the problem of fraudulent tokens that they argue issuing agency verification would solve.

1. Osborne Did Not Disclose Issuing Agency Verification

Visa asserts that the claimed “OVER file comprising a virtual representation of the credential” is disclosed by Osborne’s “token... ‘linked to credit card information,’” which is “generate[d]” by a “token server.” 486-Pet. at 21-22; 487-Pet. at 22-23. But Visa does not show that Osborne’s token “has been verified by an issuing agency to be an official representation of the credential,” as required by the ’531 Patent. EX1001 at 21:26-28, 22:64-67, 23:43 (claims 1, 15, 21).

The ’531 Patent explains that upon receiving an OVER file generation request, the OVER engine may “contact an issuing agency datastore, such as, for example, an issuing agency database 130, to verify the information contained in the OVER File generation request and to obtain additional credential information.” EX1001 at 6:22-27. For example, the ’531 Patent describes one embodiment where a user wants an OVER file “representative of a driver’s license” where:

[t]he OVER File database 128 may contact the issuing agency database 130, such as a state DMV database, and provide the driver’s license identification number to the issuing agency database 130. The issuing agency database may respond by indicating the validity of the requested credential containing the driver’s license identification number and may provide the legal name, address, and birth date of the person associated with the driver’s license identification number.

EX1001 at 6:44-52; EX2009 ¶49.

Visa does not point to a disclosure of any such verification by an issuing agency in Osborne. 486-Pet. at 21-23; 487-Pet. at 22-24. While Visa cites Osborne’s Figure 5 as “showing [the] process” for generating a token, 486-Pet. at 21; 487-Pet. at 22, this process does not include any verification of a token, much less the claimed “issuing agency” verification, EX2009 ¶¶50-59. Instead, as shown below, Osborne moves directly from a user sending a token input form (514) to creating a token (515) without any verification step, much less the claimed “issuing agency” verification:

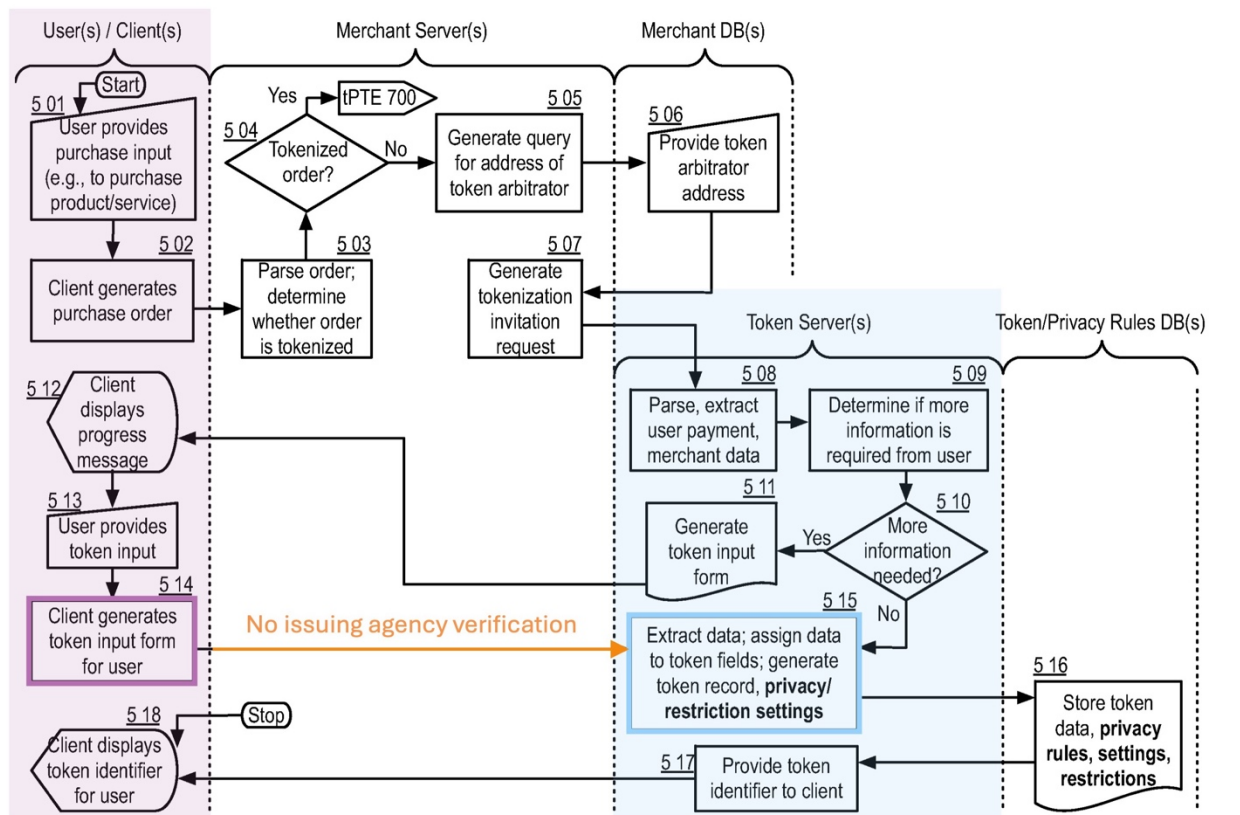


FIGURE 5

Example: Token-Based Purchase Enrollment ("TPE") component 500

EX1011 at Fig. 5 (annotated), ¶47 (“The client may generate a completed form, and provide, e.g., 514, the form to the token server (either directly or via the merchant

server). The token server may obtain the form, and parse the form to extract data fields and values from the form to generate a token data record, e.g., 515.”); EX2009 ¶¶55-58. There is simply no issuing agency verification disclosed in Osborne’s process for creating a token. EX2009 ¶¶50-59.

Visa, recognizing this hole in Osborne, argues that Osborne has an embodiment where “the agency that issued the credential”—the “issuer”—“can operate as the token server.” 486-Pet. at 22-23; 487-Pet. at 23-24. But Visa does not demonstrate that this alleged issuer-token server embodiment would operate any differently than Osborne’s standard Figure 5 process, which shows no verification step whatsoever. *See id.*; EX2009 ¶¶60-62. While Visa cites five paragraphs in Osborne as showing an “issuer” being the “token server,” 486-Pet. at 22-23 (citing EX1011 ¶¶29, 47-48, 53, 58); 487-Pet. at 23-24 (same), it does not point to any disclosure in these paragraphs of an “issuer” performing any kind of verification step, *id.*; *see also* 486-POPR/487-POPR at 22-25.

Instead of pointing to actual disclosure, Visa asserts that by an issuer “generating the token and providing it to the user to represent the credential it has issued, the issuer would be verifying it to be an official representation of the credential.” 486-Pet. at 23; 487-Pet. at 24. But Visa does not explain why an issuer-operated token server generating tokens teaches the claimed “issuing agency” verification step, much less support its position with evidence. *Id.*; EX2009 ¶¶60-62;

Icon Health v. Strava, 849 F.3d 1034, 1043 (Fed. Cir. 2017) (“Attorney argument is not evidence.”); *Zero Gravity v. Footbalance Sys.*, IPR2015-01769, 2017 WL 505951, at *8 (P.T.A.B. Feb. 3, 2017) (“Mere attorney arguments and conclusory statements that are unsupported by factual evidence have little probative value.”). Visa and Dr. Shamos point to nothing showing an issuer approving or confirming the token as an official representation of a credit card. EX2009 ¶¶62.

Visa’s argument essentially construes “verified by an issuing agency to be an official representation of the credential” to mean “issued by an issuing agency.” *See, e.g.*, 486-Pet. at 23 (“By generating the token and providing it to the user to represent the credential it has issued, the issuer would be verifying it to be an official representation of the credential.”), 62 (“A representative image provided ‘from an issuer’ would be *verified by the issuing agency to be an official representation*, as would an image produced from an actual credential, since an actual credential naturally represents itself.” (emphasis in original)); 487-Pet. at 24, 57 (same). Visa’s interpretation removes the verification step from the claim and ignores that Osborne’s token server (no matter who operates it) generates a token ***without any verification step***—which is exactly what Osborne’s Figure 5 process shows. EX1011 at Fig. 5, ¶¶47; EX2009 ¶¶60-62.

Dr. Shamos is no help either, as he provides no additional explanation or evidence and simply repeats Visa’s attorney argument verbatim. *Compare* 486-Pet.

at 22-23, 487-Pet. at 23-24 (citing EX1005 ¶240), *with* EX1005 ¶240; *Xerox Corp. v. Bytemark*, IPR2022-00624, 2022 WL 3648989, at *6 (P.T.A.B. Aug. 24, 2022) (precedential) (finding expert testimony that “merely repeats, *verbatim*, the conclusory assertion for which it is offered to support... is entitled to little weight”); *One World Techs. v. Chevron*, PGR2020-00059, 2020 WL 7222691, at *16 (P.T.A.B. Dec. 7, 2020) (Expert testimony that “merely parrots the words in the Petition... is entitled to little or no weight.”); 37 C.F.R. §42.65(a).

Visa cannot meet its burden to show that Osborne “teaches” an “issuing agency” verifying a “virtual representation... to be an official representation” with this unexplained and unsupported contention.

2. The Petition Did Not Prove That Issuing Agency Verification Was Obvious Over Osborne

Visa quickly pivots from asserting Osborne’s disclosure to arguing that it would have been obvious “for an issuer, upon generating the token, to verify that it was an official representation of the credential.” 486-Pet. at 23; 487-Pet. at 24. Despite the Examiner expressly finding this limitation was missing in “[t]he closest prior art,” EX1007 at 20, the Petition never bothers to cite any prior art disclosure of a token being verified by an issuing agency as an official representation of a credential when it is generated. 486-Pet. at 23; 487-Pet. at 24; EX1005 ¶241; EX2009 ¶84. This is plainly insufficient. *See, e.g., In re Nuvasive*, 842 F.3d 1376,

1383 (Fed. Cir. 2016) (“[T]he PTAB cannot rely solely on common knowledge or common sense to support its findings.”).

a. Visa Has Not Met Its Burden To Show That Common Sense Substitutes For This Key Claim Limitation

Instead, Visa and Dr. Shamos improperly invoke common sense to modify Osborne to fill this missing limitation. *See e.g.*, 486-Pet. at 23 (arguing verification “would be a routine step”); 487-Pet. at 24 (same); EX1005 ¶241 (same); EX2009 ¶¶83-87; *Contentguard*, 2015 WL 4467403, at *8 (equating argument that “modification[] is ‘routine’” with “stating that these changes are ‘common sense’”); *Vermeer Mfg. v. Toro Co.*, PGR2020-00081, 2021 WL 972419, at *13 (P.T.A.B. Mar. 15, 2021) (similar). But the Petition never established that using common sense is appropriate here, much less provided the reasoned analysis and evidentiary support required to do so. “[R]eferences to ‘common sense’... cannot be used as a wholesale substitute for reasoned analysis and evidentiary support, especially when dealing with a limitation missing from the prior art references specified.” *Arendi S.A.R.L. v. Apple*, 832 F.3d 1355, 1362 (Fed. Cir. 2016).

“[C]ommon sense and common knowledge have their proper place in the obviousness inquiry... ‘*if explained with sufficient reasoning.*’” *DSS Tech. v. Apple Inc.*, 885 F.3d 1367, 1374 (Fed. Cir. 2018) (quoting *Arendi*, 832 F.3d at 1361). Similar to the Petition here, Visa’s “mere recitation of the words ‘common sense’

without any support adds nothing to the obviousness equation.” *Mintz v. Dietz & Watson*, 679 F.3d 1372, 1377 (Fed. Cir. 2012); 486-Pet. at 23; 487-Pet. at 24.

The Federal Circuit cautions that “there are at least three caveats to note in applying ‘common sense’ in an obviousness analysis.” *DSS Tech.*, 885 F.3d at 1374 (quoting *Arendi*, 832 F.3d at 1361).

1. “First, common sense is typically invoked to provide a known *motivation to combine*, not to supply a missing claim limitation.” *Id.* (emphasis in original).

2. Second, the appellate court “invoke[s] common sense to fill in a *missing* limitation *only when ‘the limitation in question was unusually simple and the technology particularly straightforward.’*” *Id.* (first emphasis in original).

3. Third, the court has “repeatedly warn[ed] that references to ‘common sense’—whether to supply a motivation to combine or a missing limitation—*cannot be used as a wholesale substitute for reasoned analysis and evidentiary support*, especially when dealing with a limitation missing from the prior art references specified.” *Id.*

b. Digital Payment Systems Are Not Straightforward Technology

Here Visa does not even contend that modifying Osborne to use an officially verified electronic representation of a user’s credential was “‘unusually simple and the technology particularly straightforward’... much less provide[] support for such an allegation.” *Xerox*, 2022 WL 3648989, at *6; 486-Pet. at 23; 487-Pet. at 24; EX1001 at 1:15-53; EX2009 ¶¶63-64. Nor could it. The standard for “particularly straightforward” technology was set forth in *Perfect Web Technologies v. InfoUSA*, 587 F.3d 1324 (Fed. Cir. 2009). “There, the missing claim limitation—step D of steps A-D—was nothing more than an instruction to repeat steps A, B, and C until a particular quantity of email was sent in accordance with the claim.” *Arendi*, 832 F.3d at 1362.

By contrast, digital payment systems require devising a secure system resilient to unceasing attacks by bad actors coupled with a complex choreography among multiple parties to ensure reliable transaction management. EX1001 at 1:25-28 (“[C]urrently payment systems are highly fragmented and insecure, which creates a threat of data compromise and theft during the transfer and use of electronic commerce data.”); EX1011 ¶4 (“Engaging in card transactions requires transmission of personal information to a wide range of third-party merchants.”); *see also* EX1011 at Figs. 7A-7E (depicting a flow chart for a Token-Based Purchase Transaction

Execution system over five figures); EX1025 at 11; EX2009 ¶¶63-87. For decades, companies trying to implement digital payment methods struggled to balance the desire to create a convenient user-friendly system with the urgent need to ensure the security of the user’s information—all while keeping pace with the continuing evolution of digital communications technology and the growing sophistication of bad actors. *See supra* §II.A; EX2009 ¶¶67-71.

The Petition also overlooks that “this is *not* a case about ‘peripheral’ limitations.” *Arendi*, 832 F.3d at 1363. This limitation requiring “generating... 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,***” EX1001 at 21:24-27, determines the character of the resulting OVER file, which is used throughout the remainder of the claim, *id.* at 21:29-46 (mentioning the “OVER file” in all four subsequent limitations). This is also the key limitation the Examiner flagged during prosecution. *See* EX1007 at 20.

Invoking common sense here only courts legal error. *See, e.g., K/S Himpp v. Hear-Wear Techs.*, 751 F.3d 1362, 1365-66 (Fed. Cir. 2014) (affirming decision where “Board declined to accept a conclusory assertion from a third party about general knowledge in the art *without evidence on the record*, particularly where it is an important... limitation that is not evidently and indisputably within the common knowledge of those skilled in the art.” (emphasis in original)); *Zurn Indus. v. Sioux*

Chief Mfg., IPR2018-00973, 2018 WL 5880931, at *6 (P.T.A.B. Nov. 8, 2018) (“To the extent Petitioner asks us to fill in the missing limitation based on common sense, we decline to do so on this record, particularly where that limitation was central to the examiner’s reasoning in the Notice of Allowance.”).

c. The Petition Provides No Reasoned Analysis Or Evidence Showing Osborne’s Missing Feature Was Obvious

Visa further does not provide the “reasoned analysis and evidentiary support” necessary to fill a missing limitation with “common sense.” *DSS Tech.*, 885 F.3d at 1374; EX2009 ¶¶84-86. Instead, Visa’s entire argument is limited to a single, conclusory sentence declaring that issuer verification of a token as “an official representation of the credential... when generating the token” would have been obvious “since verifying the token would be a routine step based on the credential data received and doing so would increase confidence that the token legitimately represented the credential.” 486-Pet. at 23; 487-Pet. at 24.

But contending that a missing limitation would have been “routine” is the same as relying on “common sense” and cannot demonstrate obviousness without reasoned explanation and evidentiary support. *ContentGuard*, 2015 WL 4467403, at *8 (“We see no difference between conclusory statements that each of these modifications is ‘routine’ or a ‘logical extension’ and stating that these changes are ‘common sense,’ which, without more, is insufficient to support an obviousness

analysis.”); *Vermeer*, 2021 WL 972419, at *13 (similar); *Arendi*, 832 F.3d at 1362 (“[R]eferences to ‘common sense’... cannot be used as a wholesale substitute for reasoned analysis and evidentiary support, especially when dealing with a limitation missing from the prior art references specified.”).

Visa’s nebulous mention of “increase[d] confidence” also fails to satisfy Visa’s burden. 486-Pet. at 23; 487-Pet. at 24. Visa does not explain whose confidence would allegedly be increased, or provide evidence that “confidence that the token legitimately represented the credential” was even an issue in systems like Osborne’s. *See id.*; EX2009 ¶¶83-87. Indeed, Visa does not cite any evidence to support this conclusory assertion aside from Dr. Shamos’ parroting testimony. *Compare* 486-Pet. at 23 (citing EX1005 ¶¶240-42); 487-Pet. at 24 (same), *with* EX1005 ¶241 (Shamos: verification would “increase confidence”); *In re Zurko*, 258 F.3d 1379, 1386 (Fed. Cir. 2001) (“[T]he Board must point to some concrete evidence in the record in support of these findings.”).

d. Dr. Shamos’ Conclusory And Contradictory Testimony Provides No Evidence Of Obviousness

Dr. Shamos does not provide the required evidentiary support and reasoned explanation either, because he largely repeats Visa’s attorney argument that verification would be “routine” and “increase confidence.” *Compare* EX1005 ¶241,

with 486-Pet. at 23, 487-Pet. at 24; *DSS Tech.*, 885 F.3d at 1374; *Xerox*, 2022 WL 3648989, at *6 (“verbatim” testimony “is entitled to little weight”).

Dr. Shamos also asserts that an “issuer... would *logically* ensure that the token accurately represented the credential.” EX1005 ¶241. But reliance on the alleged “logic[]” of one of skill is essentially the same as trying to fill the missing limitation with “common sense,” which cannot demonstrate obviousness without adequate support. *ContentGuard*, 2015 WL 4467403, at *8 (no difference between statement that modification is “common sense” or “logical”).

Dr. Shamos’ only other contention is that the “existence of unofficial, forged or altered tokens in the marketplace would create problems for both issuers and users.” EX1005 ¶241. But Dr. Shamos does not explain why a skilled artisan would believe that these are problems with Osborne’s PPT system. *See id.*; EX2009 ¶¶85-86. Dr. Shamos does not explain what an unofficial, forged, or altered token is or how it could be used to exploit a vulnerability in Osborne’s PPT system. EX1005 ¶241. Thus, it is unclear how any of these could pose a “problem” for an issuer or user of Osborne’s system that would be solved by verification at the token generation step. *In re Magnum Oil Tools*, 829 F.3d 1364, 1375-76 (Fed. Cir. 2016) (burden of persuasion is on petitioner to prove unpatentability, and that burden never shifts to the patentee; that is “especially true” regarding “motivation to combine”); *DSS*

Tech., 885 F.3d at 1376 (“Dr. Hu’s... ‘conclusory statements and unspecific expert testimony’ are insufficient to support the Board’s findings.”).

Dr. Shamos himself acknowledged that unofficial, forged, or altered tokens were not a problem by the time Osborne filed his patent. He testified that the solution to this alleged problem (“a digital credential can easily be copied, forged, or altered,” EX1005 ¶118) was simply “to require the presenter of the credential to furnish additional information to prove that they are the person named in the credential,” which was done “starting in 1967 by requiring the user to enter a PIN at an ATM machine,” EX1005 ¶120. Dr. Shamos’ own testimony that the industry had already solved the alleged problem of forged tokens by authenticating identities when the credential was used in a transaction, a process that Osborne’s system already included, defeats Dr. Shamos’ pretense of any motivation to modify Osborne. EX2009 ¶86.

e. The Petition Provides No Motivation To Modify Osborne To Address A Problem Osborne Already Solved

Visa and Dr. Shamos fail to explain why a skilled artisan would be motivated to use issuer verification at the time of token generation when Osborne’s PPT system already includes authorization and payment verification at the time of the transaction, which according to Dr. Shamos, solved any hypothetical “problems” that could arise from “unofficial, forged or altered tokens.” *See DSS Tech.*, 885 F.3d

at 1376 (“Dr. Hu and the Board failed to consider that Natarajan’s multi-access protocol imposes different transmission requirements on the base station and the mobile units.”); EX2009 ¶¶88-99.

For example, Osborne describes its Token-Based Purchase Transaction Execution (tPTE) component in which in response to a token-based transaction attempt, “the token server may determine whether the user token is authenticated, e.g., 710.” EX1011 ¶69, Fig. 7A; *see also id.* ¶26 (“Thus, the system provides an authenticity shield preventing others who may know of the user’s payment token from utilizing the user’s payment token in a fraudulent transaction.”); EX2009 ¶¶92-95. If “the *user is not authenticated*, e.g., 711, option ‘No,’ the token server may generate an ‘authentication fail message,’ e.g., 712a, and initiate an error-handling routine and/or a user enrollment routine, e.g., 712b, such as the PTE 500 component” EX1011 ¶69; EX2009 ¶¶94-95. These steps are depicted in Figure 7A below:

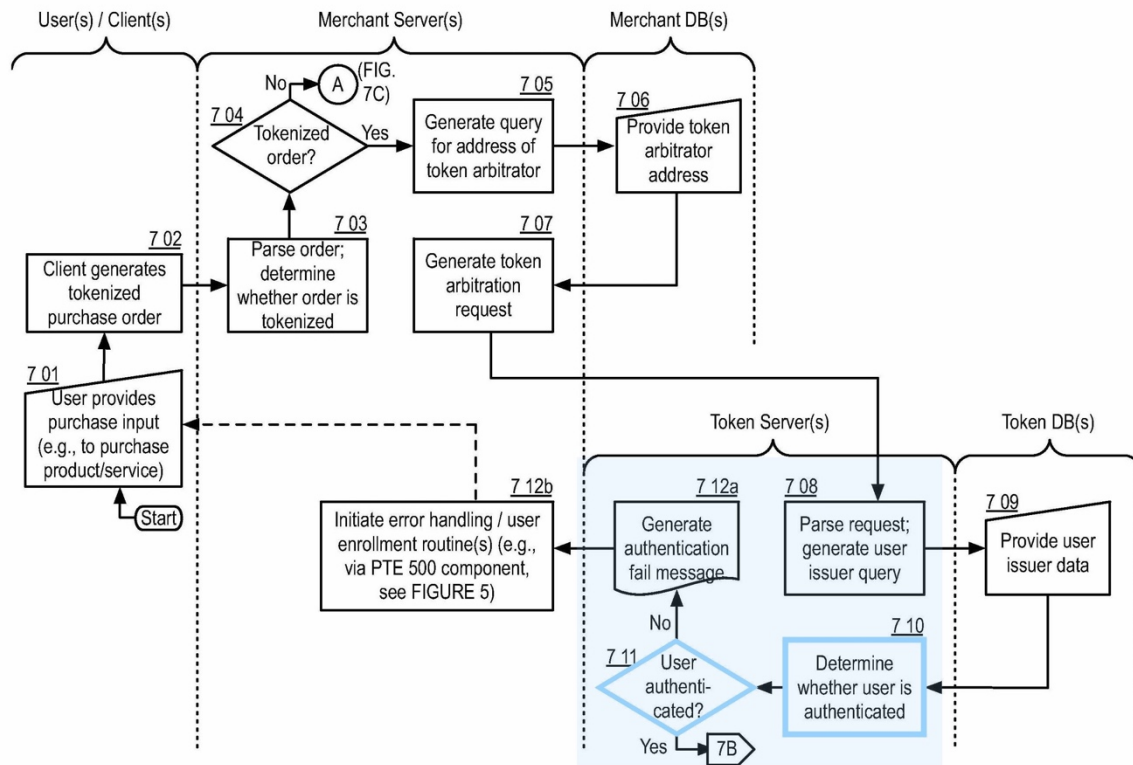


FIGURE 7A

Example: Token-Based Purchase Transaction Execution ("TPTE") component 700

EX1011 at Fig. 7A (annotated). If, as Dr. Shamos testifies, providing authentication at the time of transaction solved potential problems with digital credentials, EX1005 ¶¶118, 120, then neither Visa nor Dr. Shamos explains why this solved problem would motivate a POSITA to verify a credential at the time of generation, EX2009 ¶¶88-95.

Moreover, the Petition is silent on all of this other than stating simply “increase[d] confidence.” 486-Pet. at 23; 487-Pet. at 24. That conclusory assertion without any evidentiary support cannot possibly carry Visa’s burden, especially

when Osborne already includes an authentication step that Dr. Shamos asserts solves his hypothetical and undefined “unofficial, forged or altered tokens.”

And Visa cannot correct this failure now. *Intelligent Bio-Sys. v. Illumina Cambridge*, 821 F.3d 1359, 1369 (Fed. Cir. 2016) (“[T]he expedited nature of IPRs bring with it an obligation for petitioners to make their case in their petition to institute.”); *Dexcom v. WaveForm Techs.*, IPR2016-01680, 2018 WL 1137089, at *13 (P.T.A.B. Feb. 28, 2018) (“[E]vidence necessary to make out a prima facie case of unpatentability may not be introduced for the first time in the reply brief.”).

f. Requiring Cortex To Disprove Any Motivation To Modify Osborne Invites Legal Error

In its Institution Decision, the Board credited Dr. Shamos’ testimony and concluded, “Patent Owner fails to provide any reasoning explaining why one of ordinary skill would not have been motivated to have the issuer verify the token as Petitioner and Dr. Shamos contend.” 486-DI/487-DI at 24-25. Imposing this burden on Cortex only violates *Magnum Oil Tools*, which stated that

the Board required Magnum to rebut Petitioner McClinton’s assertions that a skilled artisan would have been motivated to combine the prior art references, ***without first requiring McClinton to provide evidence to support its assertions.*** We agree with Magnum that the Board improperly shifted the burden to it, as the patentee, to prove nonobviousness.

829 F.3d at 1377; *see also* 35 U.S.C. §316(e).

The Board’s reliance on Dr. Shamos is similarly flawed. The Board finds it “logical” for an issuer to verify the token because “such verification would increase confidence that the token legitimately represented the credential.” 486-DI/487-DI at 24. But neither Visa nor the Board explains why such confidence would improve Osborne’s system or why it would be desirable—i.e., why a skilled artisan would be motivated to pursue confidence—much less provide any *evidence* that a skilled artisan was motivated to provide such confidence or would add verification at the token generation stage to accomplish it. *See id.*; 486-Pet. at 23; 487-Pet. at 24; EX1005 ¶241; *In re Lee*, 277 F.3d 1338, 1343 (Fed. Cir. 2002) (“The examiner’s conclusory statements... do not adequately address the issue of motivation to combine.”); *Zurko*, 258 F.3d at 1386 (“[T]he Board must point to some concrete evidence in the record in support of these findings.”).

The Board next cites Dr. Shamos’ conclusory and unsupported single sentence that “unofficial, forged or altered tokens in the marketplace would create problems for both issuers and users.” 486-DI at 24 (quoting EX1005 ¶241); 487-DI at 25 (same). But, as noted above, Dr. Shamos provides no explanation for how “unofficial, forged or altered tokens” could possibly create problems in Osborne’s system, especially in view of his testimony that Osborne’s system solved these problems, nor any evidence to support the assertion that a skilled artisan was aware of such undefined problems. *DSS Tech.*, 885 F.3d at 1376 (“conclusory statements

and unspecific expert testimony” insufficient for unpatentability finding); EX2009 ¶¶88-99.

Federal Circuit precedent precludes obviousness under the circumstances presented here. As the Federal Circuit explained in *Arendi*, “[i]n cases in which ‘common sense’ is used to supply a missing limitation, as distinct from a motivation to combine, moreover, our search for a reasoned basis for resort to common sense *must be searching*.” 832 F.3d at 1363. Instead, “[t]he Board ... relied on ‘ordinary creativity’ ‘as a wholesale substitute for reasoned analysis and evidentiary support,’ and did so ‘when dealing with a limitation missing from the prior art references specified.’” *DSS Tech.*, 885 F.3d at 1377 (quoting *Arendi*, 832 F.3d at 1362). The Petition and Dr. Shamos’ testimony here are conclusory and suffer from the same deficiencies identified in *Arendi* and *DSS Technology*. Thus, the Petition’s obviousness argument for Claim 1 cannot possibly carry Visa’s burden.

g. Visa Has Not Sustained Its Burden On Its Alternate Argument

Visa’s final, alternative argument is based on “the claim requir[ing] that the credential, rather than the token, be verified by the issuer.” 486-Pet. at 23; 487-Pet. at 24. But neither the parties nor the Board have adopted such a construction. *Supra* §IV.C. Regardless, Visa and its expert have not provided a reasoned explanation or

support as to why the claim would be obvious under this non-asserted construction. *DSS Tech.*, 885 F.3d at 1374; *Arendi*, 832 F.3d at 1361-62.

Therefore, Visa has not met its burden to prove that issuing agency verification of “an OVER file” would have been obvious.

B. All Claims: The Petitions Never Establish *Prima Facie* Obviousness By Failing To Identify Osborne’s Alleged “OVER engine”

The Board may confirm patentability of all claims over the Osborne grounds because Visa and its expert have not identified the “OVER engine” in Osborne.

All claims of the ’531 Patent require an “OVER [] engine,” or apparatus performing the functions of an OVER engine. EX1001 at 21:16-18 (Claim 1), 22:55-56 (Claim 15: “OVER file generation and verification engine”), 23:27-33 (Claim 21: apparatus comprising a processor and memory configured to perform the steps of the OVER engine). For each of these claims, Visa argues Osborne “discloses the recited OVER engine” because “this [PPT] apparatus generates and verifies OVER files.” 486-Pet. at 17-18 (Claim 1 analysis), 45-46 (Claim 15 cross-referencing Claim 1); 487-Pet. at 19 (Claim 21: “[T]he processor of Osborne’s PPT apparatus, executing these stored instructions, performs the steps recited in claim 21.”).

Vaguely identifying Osborne’s “PPT apparatus” as the claimed “OVER engine” does not meet Visa’s burden. Osborne describes his entire invention as the

“Payment Privacy Tokenization Apparatuses, Methods, and Systems (hereinafter ‘PPT’).” EX1011 ¶22; *id.* at Abstract. Visa’s failure to identify the specific components of Osborne’s PPT that allegedly perform the functions of the claimed “OVER engine” does not meet its burden. 35 U.S.C. §312(a)(3). “It is of the utmost importance that... the initial petition identify ‘with particularity’ the ‘evidence that supports the grounds for the challenge to each claim.’” *Intelligent Bio-Sys.*, 821 F.3d at 1369 (quoting *id.*); 37 C.F.R. §42.104(b)(4).

Visa’s Petition musters no more certainty in identifying Osborne’s “OVER engine” than its own expert. At deposition, Dr. Shamos could not identify Osborne’s OVER engine, ultimately concluding: “Well, I can’t tell because it depends on the implementation.” EX2016 at 73:20-74:3; *see also id.* at 66:20-76:9 (Dr. Shamos unable to identify the “OVER engine” in Osborne).

Visa’s failure to specifically identify the “OVER engine” only results in the Petition improperly pointing to other components of Osborne’s PPT system to satisfy separate claim limitations with impunity. For example, Visa points to Osborne’s “merchant server” to satisfy the separate “OVER file third-party client verifying device” limitation of the claims. 486-Pet. at 25 (Claim 1: “a *third-party client verifying device* (the merchant server, alone or in conjunction with the merchant’s point-of-sale device interacting with the user’s device via NFC)” (emphasis in original)), 46-47 (Claim 15: referencing “element 1.5”); 487-Pet. at 27 (Claim 21:

“The third-party verifying device includes the merchant server and optionally the point-of-sale terminal.”).

As another example, the Board noted Visa’s assertion that Osborne’s “user device” was both “a first OVER file client device” and part of “the claimed OVER engine”:

Petitioner contends that Osborne’s “payment privacy tokenization apparatus” (PPT), which includes a “token server” or “token arbitrator,” a “merchant server,” a “merchant point-of-sale device in communication with a merchant server” (i.e., *an OVER file verifying device*), and a “user device” (i.e., a *first OVER file client device*) teaches the claimed *OVER engine*.

IPR2024-00488, Paper 7 at 25-26 (emphases in original); *see also* 486-Pet. at 19 (Claim 1: Osborne’s “client such as, but not limited to: a personal computer, mobile device...” satisfied the “OVER file storage client device” in limitation 1.2), 45-46 (Claim 15: cross-referencing limitation 1.2); 487-Pet. at 20 (Claim 21).

As the Board correctly observed, the merchant server and user device/client are also included in Osborne’s PPT apparatus as shown in Figure 4 below:

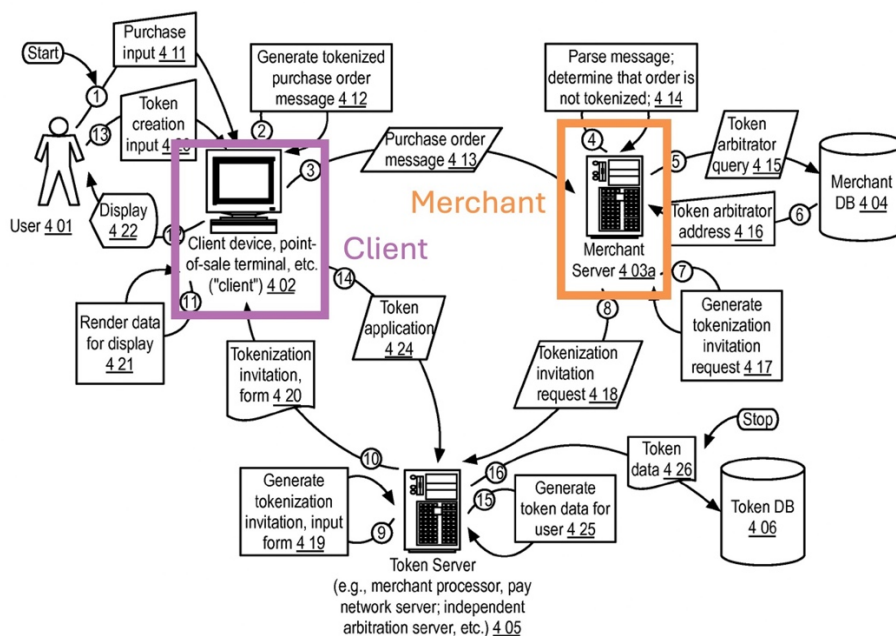


FIGURE 4

Example: Token-Based Purchase Enrollment

EX1011, Fig. 4 (annotated); *id.* ¶9 (“Fig. 4 shows a data flow diagram... in some embodiments of the PPT[.]”); *see also* EX2016 at 73:15-19 (Shamos: admitting everything in Figures 4 and 6 “other than the user” is part of the PPT apparatus).

Pointing to the same “PPT apparatus” to satisfy separate claim limitations is improper. *Kyocera Senco v. Int’l Trade Comm’n*, 22 F.4th 1369, 1382 (Fed. Cir. 2022); *Becton, Dickinson v. Tyco Healthcare*, 616 F.3d 1249, 1254 (Fed. Cir. 2010) (“Where a claim lists elements separately, the clear implication of the claim language is that those elements are distinct components of the patented invention.” (cleaned up)); *Engel Indus. v. Lockformer*, 96 F.3d 1398, 1404-05 (Fed. Cir. 1996).

Because Visa cannot remedy this error on reply and the Petitions failed to submit a *prima facie* case of obviousness by identifying Osborne’s alleged “OVER

engine,” this provides a complete basis for confirming patentability over Osborne. *Intelligent Bio-Sys.*, 821 F.3d at 1369; *Dexcom*, 2018 WL 1137089, at *13.

C. The Petition Fails To Show Obviousness Of The Dependent Claims

Even if the Board concludes that verification was obvious over Osborne, Visa nonetheless has not met its burden to show obviousness of the dependent claims discussed below.

1. Claim 2

Claim 2, depending from Claim 1, additionally requires:

- “a second OVER file generation request” “from a second OVER file storage client device of the user,”
- “generating... a second OVER file comprising a second virtual representation of the credential... that is invalid for use in the first OVER file storage client device for authenticating the user; and”
- “transmitting to the second OVER file storage client device of the user the second OVER file....”

EX1001 at 21:54-65.

By using the definite article “the,” the “second ... device of *the user*” in Claim 2 refers to the same “user” recited in Claim 1. *Wi-LAN v. Apple*, 811 F.3d 455, 462 (Fed. Cir. 2016); *Netskope v. Fortinet*, IPR2023-00457, 2023 WL 6161708, at *7 (P.T.A.B. Sept. 11, 2023). Similarly, Claim 2’s recitation of a “second OVER file

comprising a second virtual representation of *the credential*” refers to the same “credential” recited in Claim 1. *See id.*

Accordingly, Claim 2 requires a user with two devices (“first”/“second” device), each receiving a different OVER file comprising a different virtual representation (“first”/“second” OVER file comprising a “first”/“second” virtual representation) of the same credential. EX1001 at 21:54-65; EX2009 ¶¶100-02. And Claim 2 further requires that the “second OVER file” is “invalid for use in the first OVER file storage client device.” EX1001 at 21:54-65.

The Petition attempts to gloss over these added limitations with less than 1.5 pages of argument, contending they are all somehow met. 486-Pet. at 31-32; *id.* at 44-45 (Ground 3: relying on Ground 1 arguments). Despite nominally declaring that “Oborne teaches these elements,” *id.* at 31, Visa actually asserts that these limitations “would have been obvious in view of Oborne,” *id.* at 32.

The Petition does not demonstrate obviousness of Claim 2 for two independent reasons. Visa never shows it would have been obvious for Oborne to: (1) generate a “second OVER file comprising a second virtual representation” of the same “credential” for the user’s “second” device; and (2) have a “second OVER file” that is “invalid for use in the first OVER file storage client device.”

**a. Visa Does Not Show That Osborne Suggests
“generating... a second OVER file”**

Visa argues that all the “elements” of Claim 2 with “the word ‘second’” are “satisfied by a user having two devices and receiving OVER files on each device,” 486-Pet. at 31-32, but does not show that this would meet the claimed “generating ... a second OVER file comprising a second virtual representation of the credential,” EX2009 ¶¶103-09.

As an initial matter, Visa does not contend that Osborne discloses a user receiving tokens (alleged “OVER files”) on two different devices, or how its system would work in that circumstance. 486-Pet. at 32; EX2009 ¶¶105. Instead, Visa contends that applying Osborne to a user with two devices “would have been obvious” as a “POSA would have expected users to use multiple devices.” 486-Pet. at 32. Yet Visa’s Petition does not explain why one of skill would have been motivated to adapt Osborne’s system to allow a user to receive tokens on multiple devices. *Id.*; *Belden v. Berk-Tek*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (“[O]bviousness concerns whether a skilled artisan not only could have made but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention.” (emphasis in original)).

Dr. Shamos argues that a “POSITA[] would find it unnatural to be restricted to using only a single device,” EX1005 ¶253, but does not cite any support or explain

why this would have led one of skill to modify Osborne, much less how Osborne might be modified to address such a circumstance, EX2009 ¶104; EX2018. Again, Visa cannot fill in missing claim limitations using only “common sense” without a reasoned explanation and appropriate evidentiary support. *DSS Tech.*, 885 F.3d at 1374; *Arendi*, 832 F.3d at 1361-62.

Moreover, Visa does not show that a user receiving an OVER file on two devices meets the claimed “generating” a “*second* OVER file comprising a *second* virtual representation” of the same credential for the user’s second device. EX2009 ¶¶106-09. Visa completely ignores the normal and expected option (according to Dr. Shamos) that Osborne’s system would respond to a “second OVER file generation request” from a “second” device by sending the “first OVER file comprising a first virtual representation” of the credential that it had already created and stored. EX1001 at 21:47-62. In fact, Visa’s own expert, Dr. Shamos, testified that this was both the “conventional” and “logical” solution:

It was conventional to not to repeat generating a representation of a credential if the representation had previously been generated and stored. It is simply logical not to waste resources generating something that has already been generated.

EX1005 ¶55. Thus, according to Dr. Shamos, it was “simply logical” to use the first OVER file on the second device as well. *Id.* Neither Visa nor Dr. Shamos explains

why a skilled artisan would depart from Dr. Shamos’ “logical” approach here, as was necessary to carry their burden. EX2009 ¶¶108-09; *W.R. Grace v. Cochise Tech.*, IPR2023-01063, 2023 WL 8590764, at *10 (P.T.A.B. Dec. 11, 2023) (finding Petitioner failed to meet burden to show prior art disclosure “would have prompted one of ordinary skill in the art... to depart from the conventional approach”).

Visa’s Petition thus fails to show that Osborne suggested “generating... a second OVER file.”

b. Visa Does Not Prove That Osborne Suggests “a second OVER file” That Is “invalid for use” In The First Device

Relying on its argument that Osborne renders obvious a “second OVER file” for a user’s “second” device, Visa further contends that it “would also have been obvious” for “the second OVER file” to be “invalid for use in the first device.” 486-Pet. at 32. But Visa’s argument reeks of hindsight bias and does not even attempt to explain “how or why” one of skill would have further modified Osborne to meet this limitation. EX2009 ¶¶110-15; *Metalcraft of Mayville v. Toro Co.*, 848 F.3d 1358, 1367 (Fed. Cir. 2017) (“Without any explanation as to how or why the references would be combined to arrive at the claimed invention, we are left with only hindsight bias that *KSR* warns against.”); *Palo Alto Networks v. BT Ams.*, IPR2023-00888, Paper 12 at 5-6 (P.T.A.B. Apr. 1, 2024) (Petitioner bears “burden to

articulate both a *reason why*... [and] explain[] *how* [the art] would be modified to render the limitation obvious.” (emphasis in original)).

Visa relies on Osborne’s brief mention of “device fingerprinting” as a potential “additional security” measure. 486-Pet. at 32 (citing EX1011 ¶26). But Osborne’s disclosure of “device fingerprinting” is literally limited to the fact that it “may be utilized” and that “a client device of a user may be a device that is used exclusively by the user.” EX1011 ¶26. This does not teach how “device fingerprinting” would be implemented, much less for a user with two devices. EX2009 ¶111.

Visa also points to Osborne’s “client_fingerprint” field with a “MAC address” in an “example token data structure.” 486-Pet. at 32 (citing EX1011 ¶47); EX1005 ¶254 (arguing “MAC addresses... are globally unique”). But Visa does not even allege that Osborne discloses using this “client_fingerprint” to render the token “invalid for use” on a different device of the same user. 486-Pet. at 32. Indeed, as noted above, Visa does not argue that Osborne even considered the possibility of a user with two devices using Osborne’s system, much less explain how Osborne’s system would operate in that circumstance. *Id.*

Visa contends that it would be obvious “to employ Osborne’s device fingerprinting to tie a given token to a given device, such that the token for a second device would be invalid in a first device (since the device’s fingerprint would not match).” 486-Pet. at 32. But Visa does not cite any prior art showing “device

fingerprinting” being implemented in a system like Osborne’s to make a “token for a second device” of a user “invalid in a first device” of the same user. *Id.* Instead, Visa relies exclusively on Dr. Shamos’ testimony. *Id.*

Dr. Shamos’ testimony, however, cannot save Visa’s argument. He again parrots Visa’s contention that Osborne’s “device fingerprinting” would be implemented in this way without demonstrating *why* one of skill would have done so. *Compare* 486-Pet. at 32, with EX1005 ¶254; *Xerox*, 2022 WL 3648989, at *6; *Arendi*, 832 F.3d at 1366; *DSS Tech.*, 885 F.3d at 1376. Dr. Shamos’ assertion that “[t]here would be no purpose to device fingerprinting if a token could be used on any device,” EX1005 ¶254, is logically flawed and plainly incorrect.

First, Dr. Shamos’ proposed dichotomy is false in that device fingerprinting could be used to limit a token to a *set of (fingerprinted) devices* rather than to only one device or none. EX2009 ¶113. Indeed, enabling the same token to be used on *two* of the user’s devices would have allowed Osborne to follow the “conventional” and “logical” approach according to Dr. Shamos—i.e., to not “generat[e] a representation of a credential if the representation had previously been generated and stored.” EX1005 ¶55; EX2009 ¶113.

Second, yet another possibility overlooked by Dr. Shamos’ false dichotomy is that device fingerprinting could be used as one of a number of non-exclusive options for the user to be authenticated. EX2009 ¶114 (“device fingerprinting” allowing

simpler authentication on the user’s device(s), but require additional authentication on other devices). Dr. Shamos’ lack of imagination renders his testimony baseless.

Because they assumed based on hindsight that Osborne’s device fingerprinting would render a second OVER file invalid for use on a first device, neither Visa nor Dr. Shamos explains how Osborne would be modified to accomplish this result. 486-Pet. at 32; EX1005 ¶254. Visa argues that “a POSA would be motivated to employ Osborne’s device fingerprinting to tie a given token to a given device, such that the token for a second device would be invalid in a first device (since the device’s fingerprint would not match),” 486-Pet. at 32, but its conclusory assertion rests on hindsight-based premises. For example, it assumes that a second token would be generated rather than simply tying a second device to the original token, as Dr. Shamos testified would be logical. EX1005 ¶55. Visa does not explain how it arrived at its assumption, especially in view of its own expert’s testimony that creating a new token when one already exists would not be “logical.” *See id.*; EX2009 ¶¶113-15.

Visa’s burden to explain “how or why” one of skill would have further modified Osborne to meet the limitation cannot be met with such conclusory and unsupported arguments. *Metalcraft*, 848 F.3d at 1367; *Palo Alto*, Paper 12 at 5-6. Accordingly, the Petition has not demonstrated that it would have been obvious to

further modify Osborne such that a “second OVER file” was “invalid for use on the first” device of the user.

2. Claims 7 and 20

Claim 7 depends from Claim 4 and further requires a “status indicator indicat[ing] an invalid credential” and “credential information indicat[ing] a reason for the invalid credential.” EX1001 at 22:20-22. Dependent Claim 20 recites a similar limitation, EX1001 at 23:23-26, and Visa exclusively relies on its Claim 7 arguments for Claim 20. 486-Pet. at 52. Both Claims 7 and 20 fail for the same reasons. EX2009 ¶¶116-24.

Visa invokes its Claim 4 argument, contending that Osborne’s “authorization success or fail message[]” is the “credential information” and further contends that “it would be obvious for the credential information to indicate a reason for invalidity.” 486-Pet. at 36; *id.* at 34 (Claim 4).

Visa argues that “if the information provided for the credential did not match the issuer’s information, it would be routine to indicate this mismatch in a rejection response.” 486-Pet. at 36. But Visa again does not provide the “reasoned analysis and evidentiary support” necessary to demonstrate obviousness based on its common sense (“it would be routine”) rationale seeking to fill in a limitation entirely missing from the prior art. EX2009 ¶119; *DSS Tech.*, 885 F.3d at 1374; *Arendi*, 832 F.3d at 1361-62.

Dr. Shamos’ testimony contains the same conclusory assertions in the Petition and thus is also insufficient. EX1005 ¶264; *Xerox*, 2022 WL 3648989, at *6. He also cross-references to paragraph 219 of his declaration, but it discusses status indicators in Neafsey and Harris and does not address indicating “a reason for the invalid credential” or even Osborne. EX1005 ¶219; EX2009 ¶119.

Dr. Shamos also adds the conclusory and unsupported assertion that if no reason were given, that “would leave a customer confused about why the transaction did not go through.” EX1005 ¶264. But Dr. Shamos does not explain why that would be enough to motivate one of skill to modify Osborne to include a reason for the invalid credential—indeed, credit card transactions even today are routinely declined without explanation. *See id.* Dr. Shamos further does not consider the fact that a user may not want the reason for an invalid credential to be sent to the merchant, e.g., the card being over its limit, causing embarrassment. EX2009 ¶¶119-20.

Visa also contends that “Osborne expressly teaches indicating the reason for invalidation” because “an issuer response can indicate lack of funds, or indicate that a ‘number of failed authorization attempts exceeds a threshold’ by sending a ‘transaction terminated’ message.” 486-Pet. at 36 (citing EX1011 ¶72). But neither Osborne’s “authorization fails message 644” or Osborne’s “‘transaction terminated’ message, e.g., 741” “indicates a reason for the invalid credential,” as required by

Claim 7. EX1011 ¶¶61, 72; EX2009 ¶¶121-22. Visa pretending that “[e]ach of these messages indicates a reason that the credential is invalid” without explanation does not make it true. *See* 486-Pet. at 36; EX1011 ¶72.

3. Claims 8 and 29

Claim 8 depends from Claim 1 and further recites:

generating, by the OVER engine, a reference to a remotely stored credential, wherein the information associated with the credential of the user comprises the reference to the remotely stored credential.

EX1001 at 22:23-27. Claim 29 depends from Claim 23 and simply recites, “wherein the stored credential comprises a reference to a remotely stored credential.” *Id.* at 24:36-37. The Petition’s assertion that Claim 8 would have been obvious because Osborne allegedly teaches some aspects of Claim 8 is facially insufficient and does not withstand the mildest scrutiny. 486-Pet. at 37. It relies on the same argument for Claim 29. 487-Pet. at 42.

The Petition incorrectly asserts that “Osborne teaches that its systems may store *data objects* locally or in ‘remote storage facilities.’” 486-Pet. at 37 (citing EX1011 ¶133); *see also* 487-Pet. at 42 (similar). Instead, Osborne teaches that “program components” “may also be” stored in “remote storage facilities.” EX1011 ¶133. In that same paragraph, Osborne distinguishes between “program and/or database components and/or data,” indicating that Osborne was *not teaching* that

“data objects” could be stored remotely, as the Petitions assert. Thus, the Petitions’ entire premise for Claims 8 and 29 fails, as do their assertions of obviousness. Dr. Shamos’ verbatim repetition of the Petitions’ arguments is also incorrect for the same reasons, in addition to being entitled to little or no weight. *Compare* EX1005 ¶267, *with* 486-Pet. at 37; *Xerox*, 2022 WL 3648989, at *6.

Dr. Shamos adds one conclusory sentence to this analysis, asserting that the limitation was obvious “at least because it was common for tokens to be generated on a different server from the one on which the original credential were [sic] stored, at least for reasons of security.” EX1005 ¶266. First, this argument is not made in the Petition and cannot be incorporated by reference despite its citation. *See* 486-Pet. at 37 (citing EX1005 ¶240); 487-Pet. at 42 (same); *Alcon v. AMO Dev.*, IPR2021-00858, 2022 WL 17585777, at *15 (P.T.A.B. Dec. 12, 2022) (“Arguments made in a different document [other than the petition], such as an expert’s declaration, may not be incorporated-by-reference in the Petition.”); 37 C.F.R. §42.6(a)(3). Second, this single sentence cites no evidence and is conclusory at best. *Xerox*, 2022 WL 3648989, at *6 (“Dr. Jones does not cite any additional supporting evidence or provide any technical reasoning to support his statement.”).

Thus, Visa failed to show that Claims 8 and 29 would have been obvious.

4. Claims 12-13

Claim 13 multiply depends from Claims 1, 11, and 12. Claims 11-13 add requirements based on a “credential identifier.”

- [11] “...OVER file generation request comprises *a credential identifier*....”
- [12] “...comparing *the credential identifier* with one or more stored credentials.”
- [13] “...authentication message comprises the status indicator of the stored credential when *the credential identifier* matches a stored credential.”

EX1001 at 22:36-49. Using the definite article “the” shows that “the credential identifier” in Claims 12-13 refers to the same “credential identifier” that was part of the “OVER file generation request” in Claim 11. *Wi-LAN*, 811 F.3d at 462 (definite article “refers back to the same term recited earlier in the claim”). Despite the plain claim language, Visa relies on different alleged “credential identifier[s]” for Claim 11 and the later limitations in Claims 12-13.

While Visa nominally contends that Claims 11-13 are obvious, its arguments rely entirely on alleged teachings in Osborne. 486-Pet. at 38-40; *id.* at 44-45 (relying on Ground 1 arguments). Visa argues that Claim 11’s “OVER file generation request compris[ing] a credential identifier” is met by Osborne’s “token application”

including an account number. 486-Pet. at 38-39 (“Oborne teaches that the token application identifies a user credential by a credential identifier (account_num field)....”).

But for Claims 12-13, Visa switches its mapping to argue that “credential identifier” corresponds to Osborne’s “token identifier.” 486-Pet. at 39-40. In particular, Visa contends that Claim 12’s “comparing the credential identifier” with a “stored credential[]” is met by Osborne “using the *token identifier* to query a database and retrieve stored credentials (e.g., cards’ account numbers).” *Id.* at 39. Visa similarly argues that Claim 13’s “credential identifier match[ing] a stored credential” by Osborne “using the *credential identifier (token ID)* as a database query to retrieve stored account information (matching identifier to stored credentials).” *Id.* at 40.

Visa does not contend that Osborne’s token identifier is part of an “OVER file generation request” (Claim 11) or that Osborne’s account number is “compar[ed]” or “match[ed]” with a “stored credential[]” (Claims 12-13). Visa thus has not shown that Osborne renders Claims 12-13 unpatentable.

5. Claim 19

Claim 19 depends from Claim 15 and further requires “the OVER file comprises a credential image.” EX1001 at 23:21-22. Visa fails to show it would have been obvious to include an image in Osborne’s token.

Visa argues that Purves teaches “a virtual wallet ‘panel 1210 may display an image of the card (e.g., from the issuer),’ providing the customer with a helpful image representative of the credential.” 486-Pet. at 53. Visa then contends that a POSA would have found it obvious “to include a credential image as part of an OVER file also including a token as taught by Osborne and a scannable code as taught by Neafsey to provide an improved interface for users with a simple visual indication of the credentials to be invoked in a tokenized transaction.” *Id.* at 53-54. As with Visa’s asserted Stafford-Purves combination, however, Visa ignores the security concerns in providing a “credential image” to a user’s device. *Id.* at 53-54; EX2016 at 109:11-12 (testifying that providing card information to a party outside the issuer “would be a security problem. So, normally you wouldn’t do it”). And as Dr. Shamos conceded at his deposition, Purves does not disclose storing a credential image on a user’s device. EX2016 at 114:5-11. Visa’s asserted Osborne-Purves-Neafsey combination thus fails for the same reasons as its Stafford-Purves combination discussed below. *See infra* §VI.A.4.

6. Claims 23-26 and 28-33

Claims 23-26 and 28-33 require, either directly or through dependency, the “processor” of Claim 21 to further “request the credential from the issuing agency.” EX1001 at 24:9-27, 24:33-52; 487-Pet. at 34. Visa fails to carry its burden by failing to provide a reason to combine Purves’ payment account retrieval with Osborne.

Visa argues that Purves teaches the claimed “request” by “retriev[ing] the user’s ‘payment account information from the payment account issuer.’” 487-Pet. at 37 (quoting EX1013 ¶107); *see also id.* at 47-48 (relying on Ground 2 arguments). But Visa does not specifically argue that it would be obvious to combine this feature of Purves with Osborne, much less explain “how or why” one of skill would have combined the relied-on teachings in a manner that meets the claims. 487-Pet. at 34-39; *Metalcraft*, 848 F.3d at 1367; *Palo Alto*, Paper 12 at 5-6.

Instead, Visa contends that it would have been obvious “to combine Osborne and Purves... because both references are directed to similar applications.” 487-Pet. at 35. But arguing that the references discuss similar technology is not enough to demonstrate a motivation to combine. *Securus Techs. v. Glob. Tel*Link*, 701 F. App’x 971, 977 (Fed. Cir. 2017) (“[A] broad characterization of [asserted references] as both falling within the same alleged field [is insufficient] to support an obviousness conclusion.”).

Visa also generically argues that “the teachings of Purves would be recognized as useful to add new credentials to the digital wallet of Osborne’s PPT apparatus.” 487-Pet. at 35. This does not explain why the *specific* addition of Purves’ alleged “request [for] the credential from the issuing agency” would be “useful” to the *specific* embodiment in Osborne that Visa relies on for the rest of the claim. *Sisvel Int’l v. Sierra Wireless*, 82 F.4th 1355, 1364 (Fed. Cir. 2023) (affirming

nonobviousness because the “proposed combinations and rationales were expressed at such *a non-specific, high level of generality, they never made clear* to the Board what portions of the references were being combined and *why a skilled artisan would identify those particular elements for a combination*”); *ActiveVideo Networks v. Verizon Commc’ns*, 694 F.3d 1312, 1328 (Fed. Cir. 2012) (rejecting generic rationale that “fails to explain why a person of ordinary skill in the art would have combined elements from specific references *in the way the claimed invention does*” (emphasis in original)).

Dr. Shamos’ testimony does not provide any evidentiary support. *See* 487-Pet. at 35 (citing EX1005 ¶295). Aside from repeating Visa’s attorney argument, Dr. Shamos contends that the combination “would be a predictable combination of known, related technologies, to produce a predictable result (a wallet system capable of engaging in tokenized transactions and of adding new credentials as needed).” EX1005 ¶295. But just like Visa, Dr. Shamos does not explain with any specificity why one of skill would be motivated to add Purves’ alleged “request” to Osborne. EX1005 ¶¶292-95, 301-05.

Accordingly, Visa does not demonstrate Osborne and Purves render obvious the claimed “request.”

VI. VISA NEVER MET ITS BURDEN TO SHOW OBVIOUSNESS BASED ON STAFFORD (GROUNDS 5-6)

The Board correctly recognized that the Petition had not met its burden based on the Stafford (and Purves) grounds. 486-DI/487-DI at 35-41. The Board’s finding can be confirmed for any of the following four reasons:

1. Stafford does not meet the claim requirements for an “OVER file” because its IdSig1 and IdSig2 key signatures are not based on information associated with the credential;

2. Stafford never teaches issuing agency verification of those key signatures required by the claims;

3. Dr. Shamos’ admission that Purves’ card images are not stored on the user device defeats the Petition’s argument that these card images satisfy the claimed “OVER file”; and

4. The Petition provides no motivation to use Purves’ mobile-wallet card images with Stafford’s single-use encryption keys, and doing so would only introduce security risks.

A. Visa Has Not Met Its Burden To Show That Stafford Teaches Or Suggests The Claimed “OVER File”

Visa has not met its burden to show that Stafford satisfies the requirements of the claimed “OVER file,” including that Stafford’s key signatures are (1) “based on the information associated with the credential of the user”; and (2) “verified by an

issuing agency.” EX1001 at 21:24-28, 22:61-67, 23:39-43 (independent Claims 1, 15, 21). Either failure provides a complete basis to confirm patentability of all claims over Grounds 5-6.

1. Stafford’s Key Signatures Are Not “based on the information associated with the credential of the user”

Visa argues that Stafford’s “key signatures... correspond to the recited OVER files.” 486-Pet. at 61; *see also* 487-Pet. at 56 (same). It asserts that these key signatures, “IdSig1 and IdSig2 are hash values of the credential’s one-time pads” that “act[] as a virtual credential representation of the stored credential, derived based on the information associated with the credential.” *Id.*

The Institution Decision correctly rejected Visa’s argument that Stafford’s key signatures are virtual representations of a credential derived “based on the information associated with the credential.” 486-DI at 38-39; 487-DI at 39. This is because Stafford teaches that IdSig1 and IdSig2 are hash values of one-time pads IdPad and IdSecPad used to encrypt one or more credentials, and “the pads do not appear to include any information related to the credential or its contents.” *Id.*; *see also* EX1012 ¶¶88, 95, 97, 99, 103; EX2009 ¶¶131-48; EX2017.

The Board is right. Stafford’s IdSig1 and IdSig2 are not “derived based on information associated with the credential” and thus cannot meet the requirement of all independent claims that the OVER file be “based on the information associated

with the credential of the user.” 486-DI at 37; 487-DI at 37-38; EX1001 at 21:24-28, 22:63-67, 23:39-43 (Claims 1, 15, 21); EX2009 ¶¶139-48.

As Stafford teaches, and the Petition concedes, both IdSig1 and IdSig2 are hash values of Stafford’s one-time pads and are not based on information associated with the credential. EX1012 ¶¶94-103; 486-Pet. at 61; 487-Pet. at 56; EX2009 ¶¶147-48. Stafford explains that:

- The process for generating IdSig1 and IdSig2 starts with the encryption key, One Time Pad. EX1012 ¶94 (“[T]he unencrypted IdFiles... are symmetrically encrypted using *One Time Pad* or similar highly secure algorithm that provides ‘perfect secrecy’, to create IdSecFiles2.”); EX1012 at Fig. 2; EX2009 ¶143.
- “The key or pad (PadKey1) used for the *One Time Pad* is encrypted with User_priv_key1... to create *IdPad* in step 230.” EX1012 ¶95; EX2009 ¶143.
- Then, “in step 232 a hash value of *IdPad* is created, called *IdSig1*.” EX1012 ¶97; *see also* EX1012 ¶47; EX2009 ¶144.
- “Next, *IdPad* is encrypted with IdCheck_pub_key2 to generate *IdSecPad* in step 234.” EX1012 ¶99; EX2009 ¶145.
- “A hash value of *IdSecPad* is created at 236, which is referred to as *IdSig2*....” EX1012 ¶99; *see also* EX1012 ¶48; EX2009 ¶145.

Thus, Stafford teaches both IdSig1 and IdSig2 are hashes derived exclusively from the One Time Pad and are not based on any information associated with any credential in Stafford. 486-Pet. at 61 (Visa: “IdSig1 and IdSig2 are hash values of the credential’s one-time pads....”); 487-Pet. at 56 (same); EX1012 ¶¶47-48; EX2009 ¶¶147-48. All claims may be confirmed over Grounds 5-6 on this basis.

2. Stafford’s Key Signatures Are Not “verified by an issuing agency”

Even if Stafford’s IdSig1 and IdSig2 hash values were based on information associated with the credential as required by all ’531 Patent claims (and they are not), Visa further fails to show that IdSig1 and IdSig2 are “verified by an issuing agency” as required by all claims. EX2009 ¶¶149-57.

The claims specifically require verification by an “issuing agency” of “a *virtual representation* of the credential.” EX1001 at 21:24-28, 22:61-67, 23:39-43 (Claims 1, 15, 21). Visa contends that Stafford’s “hash value” key signatures are virtual representations of a credential, yet presents no argument or evidence showing that Stafford’s hash values were verified by an issuing agency. 486-Pet. at 61; 487-Pet. at 56.

Instead, Visa argues that “Stafford teaches that its encrypted credentials may be verified by the issuer.” *Id.* But the claims require “a virtual representation of the credential that has been verified by an issuing agency.” EX1001 at 21:25-26, 22:63-

65, 23:39-41 (Claims 1, 5, 21); *see also* 486-DI at 13 (holding claims require virtual representation to be verified); 487-DI at 12-13 (same). Indeed, none of the paragraphs cited in Visa’s Petition discuss Stafford’s hash values being verified, much less by an issuing agency. *See* 486-Pet. at 61-62 (citing EX1012 ¶¶62, 65, 67); 487-Pet. at 56-57 (same); 486-POPR/487-POPR at 35-36; EX2009 ¶¶153-57. Stafford does not disclose this limitation.

3. Purves Also Did Not Teach Or Suggest The Claimed “virtual representation of the credential”

Visa also argues Purves’ teaching of card images provides the required “verifi[cation] by the issuing agency.” 486-Pet. at 61-62; 487-Pet. at 56-57. Visa’s argument fails for either of two reasons: (1) Dr. Shamos admits that Purves’ user device never stores the card images on the user device, and thus cannot meet the claim requirements for a virtual representation has been verified by the issuing agency; and (2) Purves does not teach using card images for verification and thus fails to provide the asserted “verifi[cation] by the issuing agency.”

a. Dr. Shamos’ Admission That Purves Never Stores The Card Images Shows They Do Not Satisfy the Claimed Requirements Of The “virtual representation” In The Claimed “OVER file”

To satisfy the requirements of the virtual representation that has been verified by the issuing agency, Visa asserts that “Purves teaches that a user device (e.g., a device implementing a digital wallet) may be sent an image of a credential such as

a credit card, to conveniently represent a real credential.” 486-Pet. at 62; 487-Pet. at 57. But Dr. Shamos conceded at his deposition that is simply false:

A. I’m not seeing a disclosure in Purves in which the material that is sent in 2025 is stored locally on the user’s device.

Q. And by the material sent in 2025, you mean the account information and card image displayed in step 2325?

A. Right.

EX2016 at 114:5-11. Thus, as Dr. Shamos confirmed, Purves does not disclose storing card images (or account information) locally on a user device. *Id.* That is because Purves instead stores the account information and card images in a virtual wallet on a wallet server. EX2016 at 111:15-22; EX1013 ¶122, Fig. 23b (depicting “Save” occurring on Wallet Server 2301); EX2009 ¶162.

Because Purves does not disclose storing images or credit card information on a user device, it cannot satisfy the claim requirements for the virtual representation verified by an issuing agency, which is part of the claimed OVER file. EX2009 ¶162. According to all claims, the OVER file containing the virtual representation must be “transmit[ted] to the OVER file storage client device of the user.” EX1001 at 21:29-30 (Claim 1), 22:61-62 (Claim 15: “receiving, at the OVER file storage client device of the user, an OVER file”), 23:44-45 (Claim 21: “transmit, to the OVER file storage client device of the user, the OVER file”). After being sent to the user device, the claims require some variation of a “scan associated with the OVER

file on the OVER file stor[ag]e client device of the user.” EX1001 at 21:34-36 (Claim 1), 23:1-3 (Claim 15: “displaying a portion of the OVER file to an OVER file third-party client verifying device to authenticate the user”), 23:50-51 (Claim 21: similar to Claim 1).

Absent the card image on the user device, Purves cannot possibly teach these claim requirements for a virtual representation that has been verified by an issuing agency. EX2009 ¶162. Indeed, Purves’ user device cannot be an ***OVER file storage*** client device of the user at all if it does not ***store*** the alleged OVER file comprising a virtual representation. *Id.* Thus, the Petition’s citation to Purves, even if combined with Stafford, does not remedy the defects in Stafford.

b. Purves Does Not Teach Using Card Images For Verification

Additionally, Visa cannot show that Purves’ card images satisfy the requirements of a “virtual representation of the credential.”

Board’s construction. The Board construed “OVER file” to mean “a virtual representation of one or more credentials, to be used for verification of those credentials.” 486-DI/487-DI at 9; *supra* §IV.A. But Purves only taught using card images to assist a consumer in enrolling in, or using, a virtual wallet—not for any verification. *E.g.*, EX1013 ¶¶39 (“retriev[ing]” card images “to facilitate the selection of payment accounts for addition to the virtual wallet” during enrollment),

102 (discussing a “window 2001 for linking payment accounts to a virtual wallet”),
114 (using card images to help consumer “select which accounts to link to their
virtual wallet”); EX2009 ¶162.

Even Purves’ mention of a consumer “verify[ing] the authenticity of the
payment account being added” shows that the card image is used by the consumer
to confirm the account being enrolled in a virtual wallet, not a third party seeking to
verify a user’s credential. EX1013 ¶39. None of the seven paragraphs from Purves
cited by Visa show Purves’ card images being used for anything other than assisting
consumers in enrolling or using a virtual wallet. 486-Pet. at 62 (citing EX1013 ¶¶85,
102, 108-09, 111-12, 122); 487-Pet. at 57 (same). Purves does not satisfy the
requirements of the claimed “virtual representation of a credential” under the
Board’s construction of “OVER file.”

Visa’s construction. Visa further doesn’t show Purves’ card images satisfy the
claimed “virtual representation” under its own construction of “OVER file.” The
Petition construes “OVER file” as “a file comprising an image of (or associated with)
the credential... [or] a file comprising a token....” 486-Pet. at 13; 487-Pet. at 12.
Because each of the claims requires that the OVER file comprise “a virtual
representation of the credential that has been verified by an issuing agency to be an
official representation of the credential,” EX1001 at 21:25-27, 22:63-65, 23:39-41
(Claims 1, 15, 21), Visa’s construction equates “an image of (or associated with) the

credential... [or] a token” with the claimed “virtual representation.” As explained in the preceding subsection VI.A.3.a, Purves does not store card images, account information, or a token on a user device, and thus cannot satisfy all of the other claim requirements for the claimed “virtual representation” in the claimed “OVER file,” such as “transmitting” an OVER file comprising a virtual representation “to the OVER file storage client device of the user” and “a scan associated with the OVER file on the OVER file stor[ag]e client device of the user.” EX1001 at 21:29-31, 34-36 (Claim 1), 22:61-62 (Claim 15: “receiving, at the OVER file storage client device of the user, an OVER file”), 23:1-3 (Claim 15: “displaying a portion of the OVER file to an OVER file third-party client verifying device to authenticate the user;”), 23:44-45, 50-51 (Claim 21 similar to Claim 1); EX2009 ¶162.

Visa’s citation to Dr. Shamos’ testimony, 486-Pet. at 62 (citing EX1005 ¶366), 487-Pet. at 57 (same), does not close the gap because Dr. Shamos’ conclusory testimony merely repeats Visa’s attorney argument without any further explanation or evidence and should be given no weight. *Compare id.*, with EX1005 ¶366; *Xerox*, 2022 WL 3648989, at *6. Dr. Shamos’ admissions that Purves’ user device does not store card images only confirms Purves’ deficiencies. *Supra* §VI.A.3.a; EX2016 at 112:7-114:11.

Because Stafford and Purves, alone or in combination, do not teach the claimed “OVER file” or the claimed “virtual representation,” Visa failed to show

“the claimed invention as a whole would have been obvious.” 35 U.S.C. §103; *Litton Indus. v. Solid State Sys.*, 755 F.2d 158, 164 (Fed. Cir. 1985); *Absolute Dental Servs. v. Watson Guide IP*, IPR2023-00177, 2023 WL 5047049, at *4 (P.T.A.B. May 4, 2023) (citing *Litton*).

4. Visa’s Petition Does Not Establish A Motivation To Modify Stafford With Card Images or QR Codes From Purves

Finally, as the Board identified at institution, Visa’s Petition does not “set forth a sufficiently persuasive rationale to combine Stafford and Purves,” 486-DI/487-DI at 40, for two more reasons: (1) using Purves’ mobile wallet features with Stafford’s single-use keys makes no sense; and (2) the combination would only expose security risks.

a. There Is No Reason To Use Purves’ Card Images To Identify Stafford’s Single-Use Keys

Visa does not show that one of skill would have been motivated to combine Purves’ card images from its virtual wallet system with Stafford’s single-use key signatures. Visa contends it would have been obvious to use Purves’ “images representing a credential” in Stafford “to remind users which credential the key signature represents” and allow “quick selection from among a plurality of options available on the user’s device.” 486-Pet. at 62; 487-Pet. at 57 (same). This combination is nonsensical. EX2009 ¶¶158-61.

The Board correctly observed: “Stafford teaches the use of one-time key signatures, while Purves is directed to a virtual wallet with multiple payment accounts.” 486-DI/487-DI at 40. Indeed, Stafford’s single-use key signatures based on a “one-time pad” were only created *after* the user had “select[ed] files or information for release” and “determin[ed] who pays for the service.” EX1012 ¶¶84, 88, 93, 95, Fig. 2; 486-POPR/487-POPR at 39-40; EX2009 ¶¶163-64. The Petition does not explain why Purves’ credential images would be useful *after* the user has selected the credential(s) for release. 486-Pet. at 62; 487-Pet. at 57; EX1012 ¶¶74, 84; EX2009 ¶¶163-64.

Because the Petition has not shown that Stafford’s single-use key signatures were used multiple times, it further does not demonstrate how Purves’ card images would aid in selecting key signatures that are never reused. *Cisco Sys. v. Centripetal Networks*, IPR2018-01655, 2019 WL 2004230, at *8 (P.T.A.B. May 6, 2019) (rejecting motivation when “it is unclear why or how” the proposed benefit “would be useful or advantageous”); EX1012 ¶142 (“This form of ‘release’ [using pass codes] is not as secure as the previous embodiments [using hash values], since data can be transmitted multiple times.”); EX2009 ¶164.

b. Using Purves’ Card Images or QR Codes Would Introduce Security Risks in Stafford’s Secure System

Separately, Visa ignores the security risk of sending card images or QR codes, which would open vulnerabilities in Stafford’s system and reveal or suggest the contents of Stafford’s encrypted payloads, defeating the purpose of using Stafford’s key signatures in the first place. EX2009 ¶¶165-70. The Federal Circuit has long held there is no motivation to modify the prior art in such a way to make it “inoperable for its intended purpose.” *In re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1984); *Redline Detection v. Star Envirotech*, 811 F.3d 435, 453 (Fed. Cir. 2015) (no motivation to combine where proposed modification “can damage closed EVAP systems with volatile compounds”); *Streck v. Ravgen*, IPR2021-01577, Paper 62 at 87 (P.T.A.B. Apr. 18, 2023) (modified method that “could damage the cffDNA analyte in the sample itself, frustrating its detection and analysis” demonstrates no motivation to combine).

Stafford addressed the safe handling of sensitive documents and proposed using “key signatures” to address this issue. EX1012 ¶75 (“Preferably sensitive information can only be released securely, that is, it can only be released after confirmation by the entity....”); *id.* ¶81 (“Sensitive data is not able to be released without the purchase of key signatures.”); EX2009 ¶165. Stafford proposed a multitude of safety measures as part of this key signature release process to protect

this sensitive information, including encryption, digital signatures, and calculation of hash values. EX1012 ¶81 (“Advantageously, embodiments of a key signature purchase process involves multiple controls to ensure that the release of sensitive information is intentional, secure and ensures data is delivered to the intended recipient.”); *id.* ¶¶93-106 (describing the process for preparing sensitive information for release, including encryption and calculation of hash values); 486-DI/487-DI at 40 (noting Stafford’s use of “extensive encryption ... to protect specific documents”).

But Visa’s proposed modification to add card images and QR codes to Stafford introduces security vulnerabilities that would only defeat the purpose of using Stafford’s key signature-based security system. *See* 486-DI/487-DI at 40 (“[W]e question the rationale to add elements of Purves which could compromise the security of the key signature.”); EX2009 ¶¶165-70.

Dr. Shamos’ ridiculous proposal of sending a “real image of the credential” (like that shown below) with Stafford’s key signatures, EX1005 ¶367, would allow attackers to easily intercept and steal valuable cardholder information, EX2009 ¶166.



Further, Visa proposes something neither Stafford nor Purves taught—storing card images on a user device. EX2016 at 114:5-11 (Dr. Shamos: Purves doesn’t disclose storing card images or account information on a user device); EX2009 ¶162; 486-Pet. at 61 (asserting based on Stafford that “[a] *hash value* thus acts as a virtual credential representation of the stored credential”); 487-Pet. at 56 (same). Visa’s unexplained leap to add card images to Stafford’s hash values is further weakened by the fact that Purves and Stafford do not teach it, necessitating a reasoned explanation for how a skilled artisan would arrive at such an arrangement. *Univ. of Strathclyde v. Clear-Vu Lighting*, 17 F.4th 155, 161 (Fed. Cir. 2021) (“Given neither Ashkenazi nor Nitzan teaches or suggests inactivation of *any* bacteria *without* using a photosensitizer, we fail to see why a skilled artisan would opt to entirely omit a photosensitizer when combining these references.” (emphasis in original)).

Even if the system “obscured confidential information,” 486-Pet. at 62; 487-Pet. at 57, adding Purves’ card images to Stafford would create an undesirable

and unnecessary risk, as the Board pointed out. 486-DI/487-DI at 40 (“[T]he addition of an image of the user’s credential because, even with some obscured confidential information, this addition may add some risk to the secure handling of the key signature.”); EX2009 ¶¶167-70. Obscuring or omitting the account information from the card image still allows attackers to recover, or brute-force guess, the account information, or otherwise use it as a springboard to identity theft. EX2009 ¶¶167-70. Stafford disclosed that for “sensitive files, a highly secure symmetric or similar encryption process e.g. a one time pad, is used.” EX1012 ¶88. Visa offers no explanation for how its proposed bypass of Stafford’s security protocol by including card images can be reconciled with Stafford’s teachings.

The Board also pointed out that Stafford’s safe handling of sensitive user information is further threatened by Visa’s proposed addition of QR codes. 486-DI/487-DI at 40 (“QR encoding the key signature would entail the additional storage of QR-encoded key signature data, with associated additional risk to key signature security.”). Visa and Dr. Shamos propose “us[ing] a QR code to encode Stafford’s key signature... [to] allow the user to more easily transmit the key signature to a third party using a QR code scan.” 486-Pet. at 63 (citing EX1005 ¶369); 487-Pet. at 58 (citing same). The Board’s finding is correct because Dr. Shamos’ proposal manages to be both unworkable and insecure. EX2009 ¶¶171-79.

Stafford says nothing about QR codes, and generating them would only practically be performed by Stafford's system because of the extra processing steps and hassle involved. EX2009 ¶¶173-74. Stafford teaches that the user "can choose to either [1] copy IdSig1 [or IdSig2] from the display or [2] have it sent to him/herself in an email" where "the system will encrypt IdSig1 with User_pub_key1 prior to sending." EX1012 ¶¶97, 99. Neither option would work with a QR code. A user sending an unencrypted QR code to the recipient would provide direct access to the key signatures, defeating Stafford's email encryption security protocol. *Id.*; EX2009 ¶176. If the QR code was encrypted, the user could not present it to the recipient without also revealing the user's private decryption key, which would introduce a different security vulnerability in Stafford. EX2009 ¶176.

Visa's Petition does not even acknowledge the security flaws incorporated by its proposed modifications, much less explain why one of skill would still make the combination in spite of them. 486-Pet. at 54-56, 61-63; 487-Pet. at 48-51, 56-58; EX2009 ¶¶174-79. Certainly Dr. Stafford's claim that his QR proposal would "allow the user to more easily transmit the key signature to a third party" withstands no scrutiny. EX1005 ¶369; EX2009 ¶¶174-77. Further, Dr. Shamos' repetition of Visa's attorney argument does not sustain Visa's burden, and endorsing Visa's proposed security flaws only renders his opinions preposterous. *Compare* 486-Pet. at 54-56, 61-63, 487-Pet. at 48-51, 56-58, *with* EX1005 ¶¶350-57, 366.

For any and all of these reasons, Visa failed to show that the combination of Stafford and Purves renders the claims obvious.

VII. CONCLUSION

For any of the foregoing reasons, Cortex respectfully requests the Board confirm patentability of all claims of the '531 Patent.

ARMOND WILSON LLP

Dated: October 24, 2024

By: /Michelle E. Armond/
Michelle E. Armond (Reg. No. 53,954)
Douglas R. Wilson (Reg. No. 54,542)
Patrick Maloney (Reg. No. 67,247)
Yue Han (Reg. No. 80,950)
Attorneys for Cortex MCP, Inc.

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(d), the undersigned certifies that foregoing **PATENT OWNER’S RESPONSE** exclusive of the parts exempted as provided in 37 C.F.R. § 42.24, contains 13,989 words and therefore complies with the type-volume limitations of 37 C.F.R. § 42.24.

ARMOND WILSON LLP

Dated: October 24, 2024

By: /Michelle E. Armond/
Michelle E. Armond (Reg. No. 53,954)
Douglas R. Wilson (Reg. No. 54,542)
Patrick Maloney (Reg. No. 67,247)
Yue Han (Reg. No. 80,950)
Attorneys for Cortex MCP, Inc.

CERTIFICATE OF SERVICE

The undersigned certifies that pursuant to 37 C.F.R. § 42.6(e), a true copy of the foregoing **PATENT OWNER’S RESPONSE** and **EXHIBITS 2009-2024** are being served electronically on October 24, 2024 to the following lead and backup counsel for Petitioner to the following email addresses:

Matthew A. Argenti
margenti@wsgr.com

Michael T. Rosato
mrosato@wsgr.com

Patrick M. Medley
pmedley@wsgr.com

Joseph M. Baillargeon
jbailargeon@wsgr.com

ARMOND WILSON LLP

Dated: October 24, 2024

By: /Michelle E. Armond/
Michelle E. Armond (Reg. No. 53,954)
Douglas R. Wilson (Reg. No. 54,542)
Patrick Maloney (Reg. No. 67,247)
Yue Han (Reg. No. 80,950)
Attorneys for Cortex MCP, Inc.