UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

APPLE INC.,
Petitioner

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner

_____

Case: IPR2024-00330
U.S. Patent No. 10,713,656

_____

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I. INTRODUCTION 1

II. BACKGROUND 1

A. THE '656 PATENT (EX. 1001) 1

B. PETITIONER'S ASSERTED PRIOR ART 6

1. Stone (Ex. 1008) 6

2. Hoyos (Ex. 1013) 8

3. FFIEC Guidance (Ex.1037) 9

4. Varghese (Ex. 1010) 10

5. Borovsky (Ex. 1041) 13

C. PERSON OF ORDINARY SKILL IN THE ART 14

D. CLAIM CONSTRUCTION 14

III. ARGUMENT 15

A. GROUND 1: THE COMBINATION OF STONE, HOYOS, AND VARGHESE DOES NOT RENDER THE CHALLENGED CLAIMS OBVIOUS. 15

1. Stone in combination with Hoyos and Varghese does not render the independent claims obvious. 15

a) Petitioner fails to establish that a POSITA would have combined Stone with Hoyos and Varghese and would have had a reasonable expectation of success in doing so. 16

(1) Petitioner's conclusory explanation for the motivation to combine is insufficient. 16

(2) Stone is not analogous art. 20

(3) Stone, Hoyos, and Varghese teach away from each other. 23

b) Stone-Hoyos-Varghese does not disclose limitation [1.2]. 32

c) Stone-Hoyos-Varghese does not disclose Limitation [1.9]. 38

2. Stone in combination with Hoyos and Varghese does not render the dependent claims obvious. 41

a) Claims 5 and 14 do not disclose or render obvious "wherein the transaction icon includes a graphical representation of payment form."… 41

b) Claims 8 and 17 do not disclose or render obvious "wherein the virtual likeness comprises an avatar selected by the account holder." 42

B. GROUND 2: THE COMBINATION OF STONE AND THE FFIEC GUIDANCE DOES NOT RENDER THE CHALLENGED CLAIMS OBVIOUS. 42

1. Stone-FFIEC Guidance does not render the independent claims obvious. 43

a) Stone-FFIEC Guidance does not disclose limitation [1.2].....43

b) Stone-FFIEC Guidance does not disclose Limitation [1.9]. 44

c) Petitioner fails to establish that a POSITA would have been motivated to combine Stone with the FFIEC Guidance and would have had a reasonable expectation of success in doing so. 44

(1) Petitioner's conclusory explanation for the motivation to combine Stone and the FFIEC Guidance is insufficient. 44

(2) Stone is not analogous art. 47

2. Stone-FFIEC Guidance does not render the dependent claims obvious. ...47

C. GROUND 3: THE COMBINATION OF STONE IN VIEW OF HOYOS, VARGHESE, AND BOROVSKY DOES NOT RENDER THE CHALLENGED CLAIMS OBVIOUS. 48

D. GROUND 4: THE COMBINATION OF STONE IN VIEW OF FFIEC GUIDANCE AND BOROVSKY DOES NOT RENDER THE CHALLENGED CLAIMS OBVIOUS. 49

IV. CONCLUSION.....51

TABLE OF AUTHORITIES

Page(s)

CASES

Airbus S.A.S. v. Firepass Corp.,
941 F.3d 1374 (Fed. Cir. 2019) 21

Fresenius Med. Care Holdings, Inc. v. Baxter Intern., Inc.,
No. C 03-1431 SBA, 2006 WL 1343648, at *22 (N.D. Cal. May 16, 2006) 21

In re Bigio,
381 F.3d 1320 (Fed. Cir. 2004) 21

In re Clay,
966 F.2d 656 (Fed. Cir. 1992) 20, 23

In re Ethicon, Inc.,
844 F.3d 1344 (Fed. Cir. 2017) 20

In re GPAC Inc.,
57 F.3d 1573 (Fed. Cir. 1995) 20

In re Urbanski,
809 F.3d 1237 (Fed. Cir. 2016) 23, 29

KSR Intern Co., v. Telefex Inc,
550 U.S. 398 (2007) 19

Medichem, S.A. v. Rolabo, S.L.,
437 F.3d 1157 (Fed Cir. 2006) 27

NTP, Inc. v. Research in Motion, Ltd.,
418 F.3d 1282 (Fed. Cir. 2005) 40

Phillips v. AWH Corp.,
415 F.3d 1303 (Fed. Cir. 2005) (en banc) 14

Procter & Gamble Co. v. Team Techs., Inc.,
No. 1:12-CV-552, 2014 WL 12656554 (S.D. Ohio July 3, 2014) 21

Samsung Elecs. Co., Ltd. v. Infobridge Pte. Ltd.,
929 F.3d 1363 (Fed. Cir. 2019) 46

Sanofi- Aventis Deutschland GmbH v. Mylan Pharms. Inc.,
66 F.4th 1373 (Fed. Cir. 2023) 20

South-Tek Systems, LLC v. Engineered Corrosion Solutions, LLC,
748 Fed. Appx. 1003 (Fed. Cir. 2018) 25

Tec Air, Inc. v. Denso Mfg. Mich. Inc.,
192 F.3d 1353 (Fed. Cir. 1999) 23

TQ Delta, LLC v. CISCO Sys., Inc.,
942 F.3d 1352 (Fed. Cir. 2019) 16

Unwired Planet, LLC v. Google Inc.,
841 F.3d 995 (Fed. Cir. 2016) 20

Virtek Vision Int'l ULC v. Assembly Guidance Sys., Inc.,
No. 2022-1998, 2024 WL 1292734 (Fed. Cir. Mar. 27, 2024) 19, 47

Warner-Lambert Co. v. Apotex Corp.,
316 F.3d 1348 (Fed. Cir. 2003) 40

Winner Int'l Royalty Corp. v. Wang,
202 F.3d 1340 (Fed. Cir. 2000) 27

STATUTES

35 U.S.C. §103(a) 6, 15

OTHER AUTHORITIES

37 C.F.R. §42.10(b) 55

37 C.F.R. §42.24 54

37 C.F.R. §42.24(b)(1) 54

37 C.F.R. §42.100(b) 14

TABLE OF EXHIBITS

Exhibit	Description
2001	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 14 (Defendant's Rule 12(b)(6) Motion to Dismiss the Complaint for Failure to State a Claim Under 35 U.S.C. §101) (W.D. Tex. May 24, 2023)
2002	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 30 (Plaintiff's Response to Defendant's Rule 12(b)(6) Motion to Dismiss the Complaint for Failure to State a Claim Under 35 U.S.C. §101) (W.D. Tex. June 1, 2023)
2003	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 31 (Defendant's Reply Brief In Support of Motion to Dismiss for Failure to State Claim Under 35 U.S.C. §101) (W.D. Tex. June 28, 2023).
2004	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 64 (Defendant's Opposed Motion to Stay Pending Transfer) (W.D. Tex. November 28, 2023)
2005	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 37 (Defendant's Opposed Motion to Transfer (redacted)) (W.D. Tex. July 26, 2023)
2006	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 66 (Carbyne's Response to Motion to Stay Pending Transfer) (W.D. Tex. December 5, 2023)
2007	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 50(Carbyne's Response to Motion to Transfer Venue) (W.D. Tex. October 27, 2023)
2008	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 55 (Apple's Reply In Support of Its Motion to Transfer Venue) (W.D. Tex. November 10, 2023)

2009	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 60 (Carbyne's Surreply in Response to Motion to Transfer Venue) (W.D. Tex. November 16, 2023)
2010	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 42 (Apple's Opening Claim Construction Brief) (W.D. Tex. October 4, 2023)
2011	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 49 (Carbyne's Response to Apple's Proposed Claim Construction) (W.D. Tex. October 25, 2023)
2012	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 54 (Apple's Reply Claim Construction Brief) (W.D. Tex. November 8, 2023)
2013	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 62 (Carbyne's Sur-Reply to Apple's Claim Construction Brief) (W.D. Tex. November 22, 2023)
2014	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 69 (Minute Entry re Markman Hearing and Motion to Transfer Venue) (W.D. Tex. December 12, 2023)
2015	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 73 (Apple's Motion to Stay Pending The Court's Written Order on Transfer) (W.D. Tex. January 17, 2024)
2016	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 79 (Carbyne's Response to Motion to Stay Pending Written Order on Transfer) (W.D. Tex. January 24, 2024)
2017	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 80 (Apple's Reply in Support of Motion to Stay Pending Court's Written Order on Transfer) (W.D. Tex. January 24, 2024)
2018	*In Re Apple*, Case No. 2024-111, Dkt 2 (Apple's Petition for Writ of Mandamus) (Fed. Cir. February 1, 2024)

2019	*In Re Apple,* Case No. 2024-111, Dkt. 13 (Carbyne's Response to Writ of Mandamus) (Fed. Cir. February 20, 2024)
2020	*In Re Apple Inc.*, Case No. 2024-111, Dkt 15 (Apple's Reply In Support of Petition for Writ of Mandamus) (Fed. Cir. February 27,
2021	*In Re Apple Inc.*, Case No. 2024-111, Dkt 18 (Order Denying Writ of Mandamus) (Fed. Cir., March 18, 2024)
2022	United States Patent and Trademark Office Memorandum Dated June 21, 2022 re: Interim Procedure for Discretionary Denials in AIA post-grant proceedings with Parallel District Court Litigation
2023	*Cloud of change, LLC v. Lightspeed POS Inc.,* Case NO. 6:21-cv-0102 Order Denying Lightspeed POS Inc's Opposed Motion to Stay Pending Resolution of *Inter Partes* Review (W.D. Tex. Dated May 15, 2023)
2024	*Sonrai Memory Limited v. LG Electronics, Inc.* 2022 WL 2307475 (W.D. Tex. June 27, 2022)
2025	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Apple's Amended Preliminary Invalidity Contentions (W.D. Tex. October 6, 2023) (excerpts)
2026	Email Correspondence From Counsel Of Petitioner To Counsel of Patent Owner re *Sotera* Stipulations and *Carbyne Biometrics, LLC v. Apple Inc.*, 1:23-cv-0032 (W.D. Tex.)
2027	Email Correspondence From Counsel Of Petitioner To The Board re *Sotera* Stipulations for IPRs IPR2024-00329, -00330, -00331, -00332, -00333, -00334 and-00507
2028	U.S. Patent No. 5,164,992 ("Turk Patent")
2031	CV of Dr. Michael Goodrich
2032	Declaration of Dr. Michael Goodrich
2033	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 155 (Apple Inc.'s Final Election of Asserted Prior Art) (W.D. Tex. October 23, 2024)

I. INTRODUCTION

At Petitioner Apple Inc.'s request, on July 30, 2024, the Patent Trial and Appeal Board ("Board") instituted *inter partes* review of claims 1-19 ("Challenged Claims") of U.S. Patent No. 10,713,656 ("the '656 Patent"). Carbyne Biometrics, LLC ("Patent Owner") respectfully disagrees with Petitioners' arguments and the Board's Decision. As explained in detail below, the Challenged Claims of the '656 Patent are not rendered obvious by the cited references, and their patentability should be affirmed.

II. BACKGROUND

A. The '656 Patent (Ex. 1001)

The '656 Patent is titled "Method, Medium, and System for Reducing Fraud," and claims priority from a provisional application filed on May 6, 2010. The '656 Patent provides systems and methods for preventing or reducing fraud in electronic financial transactions. *See* Ex. 1001 at abstract. As the '656 Patent observes, there are two main reasons why even an otherwise honest person would refrain from committing fraud: (1) associated feelings of guilt and (2) the risk of getting caught. *Id.* at 4:24-4:26; Ex. 2032 ¶ 30.

Electronic payment fraud presents "an ongoing problem" that is "particularly devastating" because the electronic transaction medium removes the physical barriers of a typical financial transaction and, in the process, neutralizes these

primary fraud deterrents. *Id.* at 1:22-1:32, 4:24-4:26; Ex. 2032 ¶ 31.

The electronic transaction medium does so, first, by lowering the risk that a would-be fraudster will be caught, or at least lowers the fraudster's perception of this risk, by removing the need for physical access to the victim's wallet or credit card. *See id.* 1:28-1:30; Ex. 2032 ¶ 31. Second, removing the physical access requirement also dehumanizes the transaction and alleviates the potential feelings of guilt associated with perpetrating a fraud. *See id.* 5:10-5:12 ("The more human the victim is made to be, the more guilty a fraudster might feel when perpetrating a fraud."). Put another way, a faceless, electronic transaction makes it easier for the fraudster to go through with the fraud. *See id.* 5:8-5:34, 6:10-6:23, 6:52-6:64; Ex. 2032 ¶ 31.

The '656 Patent seeks to curb electronic payment fraud by providing novel systems and methods by bolstering the two fraud deterrents that the electronic medium mitigates. *See* 4:24-4:26. First, the '656 Patent's claimed invention increases a potential fraudster's feelings of guilt by providing an improved graphic user interface that includes a virtual likeness of the face of an account holder whose account is engaged in an electronic transaction. *See id.* at 5:8-5:34; Ex. 2032 ¶ 32. Forcing a potential fraudster to complete a transaction while looking at a photo or other virtual likeness of the victim's face (or the potential recipient of illicit funds in a peer-to-peer cash transfer, *see id.* at 11:6-11:10) humanizes the transaction by

emphasizing the identity of the victim or account holder who will be impacted by the fraudulent transaction. *Id.* at 5:23-5:25. The figures below from the ’656 Patent provide examples of a transaction interface that includes the virtual likeness of an account holder as claimed by the ’656 Patent.

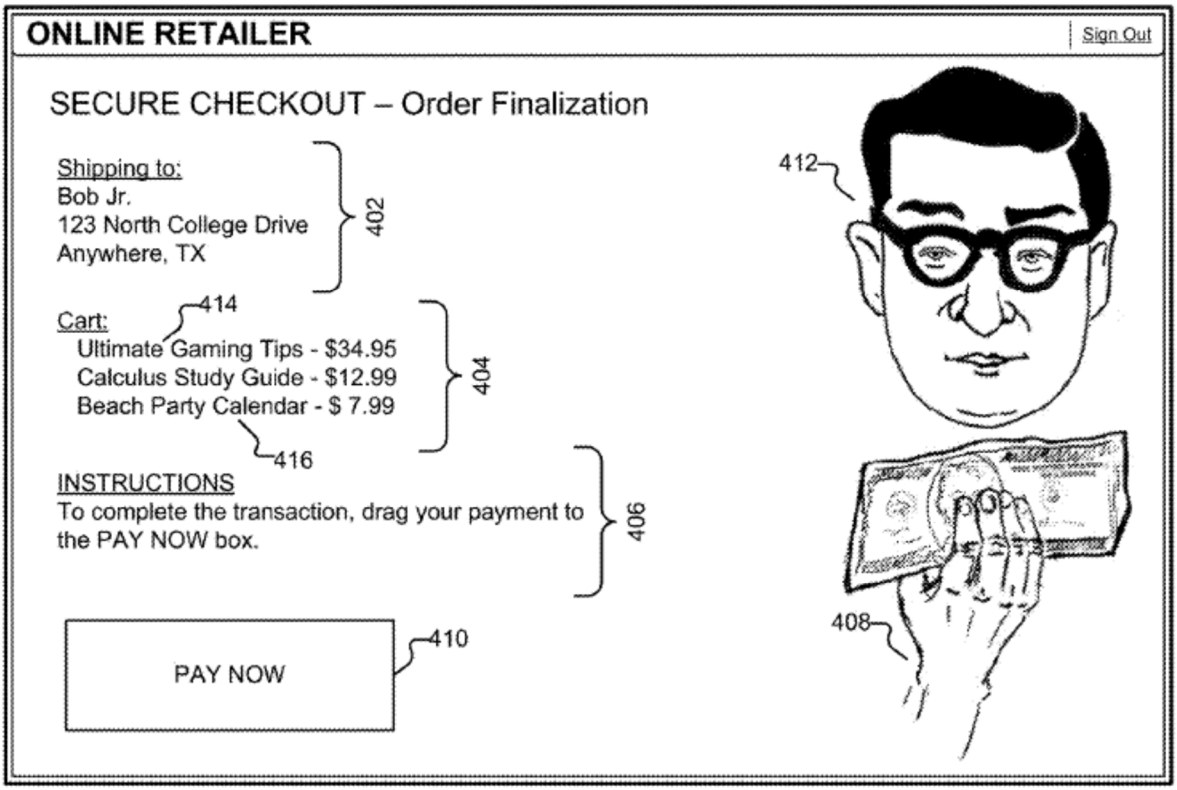


FIG. 4

Ex. 1001 at Fig. 4.

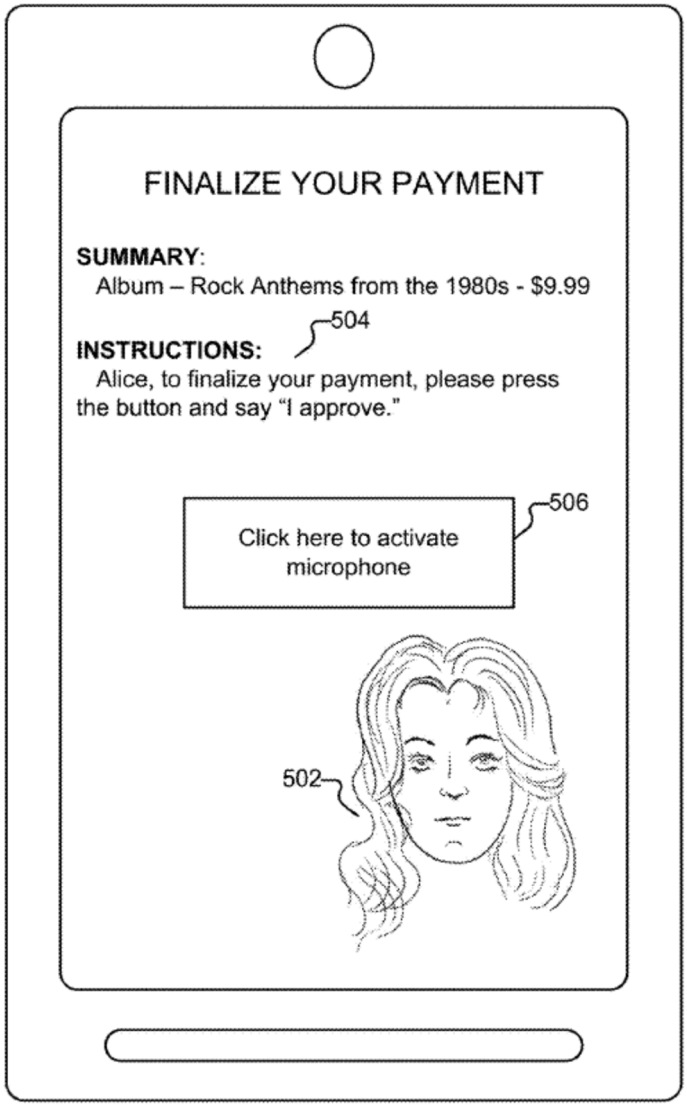


FIG. 6

Ex. 1001 at Fig. 6.

The '656 Patent's claimed systems and methods also increase the fraudster's risk of being caught—real or perceived—by employing biometric authentication techniques as part of a fraud detection analysis to determine that a user is alive. *See, e.g.*, Ex.1001, cl. 1. Specifically, the '656 Patent's claimed authentication process is

as follows. The user interacts with a transaction icon in an interface containing a virtual likeness of the face of an account holder. *Id.* The user's biometric information is captured and fraud detection analysis is performed to determine that the user is alive, based at least in part on an analysis of the biometric information collected from the user. *See id.* The electronic transaction is then completed based at least in part on both the user interaction with the transaction icon in the interface and the fraud detection analysis. *See id*.

The collected biometric information can include images of the user or an audio recording. *Id.* at 8:51-9:6; Ex. 2032 ¶ 34. For the collection of images, techniques for confirming the object captured in the images is alive (e.g., by taking multiple photographs in rapid succession) "can be employed to help make sure that the fraudster isn't using camera 112 to photograph a printed picture of the legitimate user." *Id.* at 8:61-66. "The application of various rules, such as requiring that a face be detected in the captured image or that a certain amount of flesh tone be present in the picture can also be implemented." *Id.* 8:66-9:2. "Similar rules can be applied to other types of capture, such as requiring that a GPS be turned on prior to a transaction taking place, or requiring that provided audio conform to general rules that define what human utterances sound like." *Id.* 9:2-9:6.

In sum, the '656 Patent provides a novel approach to preventing fraud in electronic transactions by coupling an interface incorporating the virtual likeness

of an account holder to inspire feelings of guilt in a potential fraudster with biometric authentication techniques, specifically those to determine whether the user is alive, that increase the likelihood (real or perceived) that the fraud will be detected. Ex. 2032 ¶ 35.

B. Petitioner's Asserted Prior Art

The table below lists Petitioner's obviousness grounds followed by descriptions of the individual references.

Ground	Claims	Basis
1	1, 4-10, and 13-19	§103(a) over Stone in view of Hoyos and Varghese
2	1, 4-10, and 13-19	§103(a) over Stone in view of FFIEC Guidance
3	2-3 and 11-12	§103(a) over Stone in view of Hoyos, Varghese, and Borovsky
4	2-3 and 11-12	§103(a) over Stone in view of FFIEC Guidance, and Borovsky

1. Stone (Ex. 1008)

What Petitioner identifies as the "Stone reference" is U.S. Patent Pub. No. 2010/0042535, titled "Currency Display" and assigned on its face to eBay. *See* Ex. 1008. Stone discloses systems and methods for electronic visual displays of currency. *Id.* [0002], [0006]; Ex. 2032 ¶ 37. Stone provides for an interface that displays a visual representation of the amount of currency that is subject to an electronic transaction. *Id.* at [0016]. As Stone explains, providing a visual representation of the amount in a transaction reinforces the value of the amount of

money in the transaction and provides the user with a "more visually rich interface." *Id.* An aspect of the system disclosed by Stone is that it enables a user's device to detect and use the currency of the country where the device is located. *Id.* at [0026]. For example, if the user is a U.S. citizen traveling in South Korea, the disclosed user display will display South Korean won instead of U.S. dollars. *Id.* at [0026-30]. This feature allows a user in a foreign land to understand how much he or she is willing, or unwilling, to pay for something when bartering with local merchants. *Id.* at [0030]; Ex. 2032 ¶ 37.

The display described in Stone can also include more than just a representation of currency. *Id.* at [0021]. Some embodiments of the display can include the name and picture of the recipient in a peer-to-peer funds transfer or the user's funding source and account balance before a transaction is initiated. *Id.* at [0024].

But at its core, Stone's primary focus is providing a "more visually rich interface" that gives the user a visual representation of the amount and denomination of currency subject to a transaction, particularly where foreign currencies are involved. *See id.* at [0016], [0026]; Ex. 2032 ¶ 39.

Stone is not concerned with electronic payment fraud or how to deter it. In fact, Stone is not at all concerned with actually processing transactions, improving transaction processing, or user authentication. *See, e.g.*, Stone at [0023] ("Note that transferring funds via a mobile phone is known, such as through PayPal in San Jose,

Calif. Thus, details of how funds are transferred are not described here."); Ex. 2032 ¶ 40.

2. Hoyos (Ex. 1013)

Hoyos discloses systems and methods for biometric authentication in financial transactions. Ex. 1013 at [0002]. In one aspect, Hoyos discloses a method for authenticating financial transactions by acquiring biometric data from a person, calculating the probability of liveness of the person and probability of a match between the person and known biometric information. *Id.* at [0017]. Examples of the biometric inputs include photos capturing the subject's face and eyes or readings of finger and palm temperature. *Id.* at [0021]. In certain embodiments, the authentication decision is calculated using the collected biometric information to determine the probability of a match and probability of a live person based on a mathematical formula. *Id.* at [0016]-[22]; Ex. 2032 ¶ 41.

While Hoyos describes techniques for biometric authentication, it does not suggest coupling these techniques with an improved digital interface. Nor does Hoyos even mention digital interfaces as being relevant to its claimed authentication techniques. Hoyos' proposed claims and specification focus mainly on the above-described probability calculations used for authenticating a user. Hoyos also does not disclose employing its methods or systems in a client-server environment, but rather is focused on providing local authentication on a client device. *See, e.g.*,

Hoyos at cl. 4; Ex. 2032 ¶ 44.

3. FFIEC Guidance (Ex. 1037)

Petitioner's next reference is guidance published by the Federal Financial Institutions Examination Council (FFIEC). Ex. 1037 at 1. The FFIEC is a formal interagency body of five banking regulators established in 1979 and "empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions." *Id.* In 2005, the FFIEC issued "guidance" for "Authentication in an Internet Banking Environment" ("FFIEC Guidance" or the "Guidance"). *See id.* The Guidance "addresses why financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services." *Id* 1. The Guidance suggests that single-factor authentication (such as typed passwords) is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. *Id.* The Guidance mentions high-level techniques and methodologies for multifactor authentication that fall into three broad categories: something a person knows (password or PIN), something a person has (a physical token or card), or something a person is (most commonly biometrics). *Id.* at 2; Ex. 2032 ¶ 45.

Concerning biometrics, the FFIEC Guidance provides a basic description of

fingerprint and facial recognition techniques and the benefits of employing these methods. But the Guidance stops short of "endors[ing] any particular technology" or explaining how to implement any techniques, specifically as part of a digital interface. Ex. 1037 at 1. The Guidance mentions that "various biometric techniques and identifiers are being developed and tested, these include: fingerprint recognition, face recognition, voice recognition, keystroke recognition, handwriting recognition, finger and hand geometry, retinal scan, and iris scan." *Id.*at 10. Of these techniques, the FFIEC states that fingerprint and face recognition are gaining acceptance, *see id.*, but the FFIEC Guidance does not state that these techniques or any biometric technique was well known or universally applied to secure electronic or online transactions. Ex. 2032 ¶ 46. The Guidance also does not discuss improvements or upgrades to digital displays in electronic transactions. Ex. 1037 at 9-11.

4. Varghese (Ex. 1010)

Varghese generally relates to "systems and methods for providing protection against identity theft over a computer network." Ex. 1010 at [0002]. It discloses multi-factor authentication for electronic transactions that uses a rules engine to score the transaction based on different criteria, including biometrics (voiceprint) and device "location fingerprint." *Id.* at Fig. 14. Varghese describes both pre- and post-authentication procedures. *Id.* at [0090]; *see also id.* at Table 3. For "pre-authentication, the most common user request is a login request to access an

application or system." *Id.* at [0074]. "[R]equests usually handled by post-authentication services include, e.g., transaction requests involving large amounts of money." *Id.* at [0074]; *see also id.* at [0099]; Ex. 2032 ¶ 47.

The systems and methods Varghese discloses separate authentication into two phases: pre- and post-authentication. Pre-authentication is employed for actions such as login requests and considers identifying information of the device originating the request or information about the identity of the user. *Id.* at [0065]. Post-authentication is applied for transaction authentication requests, such as transaction requests for large amounts of money. *Id.* Post-authentication described by Varghese authenticates an individual transaction by considering historic transaction information for the user device and workflow history. *Id.*; Ex. 2032 ¶ 48.

Varghese identifies available security-relevant information related to a user request (the "request attributes") as falling into related "criteria." *Id.* at [0089]. For pre- and post-authentication, different criteria are available, or of differing importance, depending on which authentication phase is being implemented. *Id.* In pre-authentication, a user is seeking to log in to an application, so the user's transaction history is unavailable, so it would not be used at this phase. *Id.*; Ex. 2032 ¶ 49. But for post-authentication, when a user is making a transaction request (e.g., a transaction request for large amounts of money), criteria for initial authentication, such as location information for the user device or the device IP address, are typically

not relevant, and the user's transaction history is more relevant. *Id.*

Table 3 from Varghese presents a list of characteristics that can be used during pre-authentication and post-authentication. Petitioner's Grounds 1 and 2 rely on Varghese as disclosing the "location" limitations of the Challenged Claims. Pet. 39-45, 65-68; Ex. 2032 ¶ 50. As Table 3 (reproduced below) shows, location information is considered in pre-authentication—for user login requests. "Location information characterizes the location of the device from which a request originates." Ex. 1010 at [0072]. "Location can most easily be estimated from the device's IP address and the hierarchy of networks linking the device to the internet." *Id.* at [0093].

TABLE 3

Example of Request Attributes		
Pre-authentication	Location information	City, State, Country information and confidence factors
		Connection type
		Connection speed
		IP address, routing type, and hop times
		Internet service provider flag
		Autonomous system number
		Carrier name
		Top-level domain
		Second-level domain
		Registering organization
		A list of anonymizing proxies
		Hostnames and routers
	Device information	Secure Cookies
		Flash Cookies
		Digitally signed device
		Device & display Characteristics:
		Operating System characteristics
		Browser Characteristics
Post-authentication	User information	User identifications
		Valid or not valid user
		Authentication status
	Transaction information	Key Value Pairs:
		Support multiples
		Keys can be defined using Regular Expressions
		Values can be defined in ranges
		Pages accessed
		Time spent on page
		Transactions sequences

5. Borovsky (Ex. 1041)

Borovsky (U.S. Patent Pub. US 2010/0317335) is titled "Systems and Methods for Remotely Configuring a Mobile Device." Borovsky claims priority to U.S. Patent Appl. No. 12/483,149 filed June 11, 2009. *See* Ex. 1041. Borovsky generally relates to systems and methods for remotely configuring a mobile device. *Id.* at [0001]. The system and methods disclosed by Borovsky for remotely configuring a mobile phone using servers that store and remotely update configuration information for the mobile device. *See, e.g.*, Ex. 1041 at cls. 1, 7, 19; *See* Ex. 2032 ¶ 51. Borovsky provides for a remote computer that includes a user interface for managing configuration information for the user's mobile device. *Id.* at [0010]. The user enters management information via the user interface presented at the remote computer and, subsequently, a management system updates configuration information at a database based on the management information. *Id.* The configuration information can include contact information for viewing or updating contacts of the user stored in the mobile device. *Id.* at cl. 3. The user interface displayable at the remote host computer may comprise a contacts interface that can enable a user to enter contact management information. *See, e.g.*, *id.* at cl. 6. The contact management information may include display names corresponding to the user's contacts, phone numbers for the contacts, addresses for the contacts, or photos corresponding to contacts of the user. *See, e.g.*, *id.* at cl. 7.

C. Person of Ordinary Skill in the Art

Petitioner asserts that a person of ordinary skill in the art ("POSITA") at the time of the '656 Patent's invention would have had "a bachelor's degree in electrical engineering, computer engineering, computer science, or a related field, and at least two years of experience in the research, design, development, and/or testing of biometric authentication techniques, and related firmware and software, or the equivalent, with additional education substituting for experience and vice versa." Institution Decision (Paper 10) at 20 (quoting Pet. 4). The Board adopted Petitioner's description of a POSITA "except for the language 'at least' that qualifies the experience level and allows the experience level to encompass an expert's level of skill." Institution Decision at 21. For the purposes of this proceeding, Patent Owner and its expert have applied this level of ordinary skill in the art, as clarified in the Board's Institution Decision. *See* Ex. 2032 ¶¶ 25-28.

D. Claim Construction

The Board gives claim terms their ordinary and customary meaning as understood by a POSITA at the time of the invention in light of the patent's specification. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (en banc); 37 C.F.R. § 42.100(b) (applying *Phillips* standard to petitions filed on or after Nov. 13, 2018). Patent Owner accepts Petitioner's position that none of the claim terms of the '656 Patent require construction. *See* Pet. at 5. Patent Owner and its

expert have therefore given all claim terms their plain and ordinary meaning as understood by a POSITA at the time of the invention in light of the patent's specification.

III. ARGUMENT

A. Ground 1: The Combination of Stone, Hoyos, and Varghese Does Not Render the Challenged Claims Obvious.

Petitioner's first invalidity ground asserts that independent claims 1, 10, and 19 and dependent claims 4-9, 13-18 of the '656 Patent are obvious under 35 U.S.C. §103(a) over Stone in view of Hoyos and Varghese. As explained below, the Stone-Hoyos-Varghese combination does not render any of the Challenged Claims obvious. *See* Ex. 2032 ¶¶ 54-90.

1. Stone in combination with Hoyos and Varghese does not render the independent claims obvious.

Petitioner fails to show that the '656 Patent's independent claims 1, 10, and 19 are rendered obvious by the Stone-Hoyos-Varghese combination. First, Petitioner fails to establish that a POSITA would have combined Stone with Hoyos and Varghese resulting in the claims of the '656 Patent and would have had a reasonable expectation of success in doing so. Ex. 2032 ¶¶ 55-78. Second, the Stone-Hoyos-Varghese combination does not disclose storage of biometric information in a data store, wherein the biometric information is associated with an account of the account holder as required by the '656 Patent's independent claims. Ex. 2032 ¶¶ 79-85.

Finally, Stone-Hoyos-Varghese does not disclose "a memory coupled to the processor." as required by the '656 Patent's independent claims. Ex. 2032 ¶¶ 86-87.

a) Petitioner fails to establish that a POSITA would have combined Stone with Hoyos and Varghese and would have had a reasonable expectation of success in doing so.

Petitioner fails to establish that a POSITA would have combined Stone with Hoyos with a reasonable likelihood of success that would result in the claims of the '656 Patent. First, Petitioner's explanation for the alleged motivation to combine is conclusory. Ex. 2032 ¶¶ 55-62. Stone is also not analogous art to the '656 Patent, which itself is sufficient to establish a lack of motivation to combine. Ex. 2032 ¶¶ 63-66. Finally, Stone and Hoyos teach away from each other in materials ways that would have dissuaded a POSITA from combining their teachings to reach the '656 Patent's claims. Ex. 2032 ¶¶ 67-78.

(1) Petitioner's conclusory explanation for the motivation to combine is insufficient.

Petitioner's "explanations" for why a POSITA would have combined Stone and Hoyos are conclusory. "[C]onclusory assertion[s] with no explanation [are] inadequate to support a finding that there would have been a motivation to combine." *TQ Delta, LLC v. CISCO Sys., Inc.*, 942 F.3d 1352, 1356 (Fed. Cir. 2019). Petitioner's stated reasons supporting the Stone-Hoyos-Varghese combination do not provide a justification for *why* a POSITA would have combined

their teachings, specifically Stone and Hoyos, in a way that results in the '656 Patent's claims. Petitioner's explanation for why a POSITA would have combined Stone and Hoyos can be summarized as follows: "[I]t was well-known that financial transactions of Stone had a need for authentication including fraud detection (e.g., with higher levels of security for higher-risk transactions)." Pet. at 16. And "[a] POSITA would have been motivated to implement Hoyos' spoofing- resistant biometric authentication for fraud detection in the system of Stone for 'improved deterrent against attempted fraudulent transactions, and decreased rejection of valid customers.'" *Id.*

These assertions do not explain *why* a POSITA would have combined the references. Stone does not identify electronic payment fraud as a problem needing to be solved. Stone never mentions fraud, nor does it discuss any techniques for preventing fraud, like those described in Hoyos. Stone discloses an enhanced currency display. *See* Stone at [0002] and [0016]. It is not concerned with the actual processing of transactions, *see* Stone at [0023], so a POSITA would not have been motivated to apply Hoyos's authentication techniques to Stone's teachings. Ex. 2032 ¶¶ 57-58.

While Stone states that user identifier 418 "may include attributes related to the user, such as personal information (e.g., a user name, password, photograph image, biometric id, address, phone number, etc.) and banking information (e.g.,

banking institution, credit card issuer, user account numbers, security information, etc.), *see* Stone at [0045], Stone does not state that the user identifier is used for performing some form of authentication or fraud detection, specifically biometric-based fraud detection. Ex. 2032 ¶¶ 58-60.

Nothing in Stone substantiates that the "biometric id" or "security information" is used for transaction authentication. Ex. 2032 ¶ 60. Further evidencing that Stone is concerned with improving the user interface and not authentication or fraud detection is the fact that in reference to the actual transfer of funds, Stone states: "Note that transferring funds via a mobile phone is known, such as through PayPal in San Jose, Calif. Thus, details of how funds are transferred are not described herein." Stone at [0023]. Declining to explain how funds are transferred, much less providing ways to improve this process, such as ways to reduce fraud, further proves that Stone is not concerned with fraud detection or the processing of electronic transactions.

Hoyos, for its part, also contains nothing to suggest a POSITA would apply its teachings to Stone. Hoyos has a limited focus—improving known biometric matching techniques by incorporating a method to determine the probability that the subject is alive. Ex. 1013 at [0016]-[0022]. Hoyos is not concerned with improving a user display, specifically an electronic currency display (like that of Stone), or improving a user's experience based on providing a richer interface (like

Stone). Nothing in Hoyos would lead a POSITA to combine its biometric authentication methods with an interactive interface, particularly a currency display like the one Stone provides. Ex. 2032 ¶¶ 57-61.

At bottom, Petitioner's alleged motivation to combine the references in Ground 1 is this: electronic payment fraud was a known problem, and the '656 Patent's independent claims consist of elements disclosed in Stone and Hoyos. *See* Pet. at 17-21. But this argument fails. Stone, again, was not concerned with processing or improving the processing of electronic transactions. And even if it were, known elements and a known problem without more are insufficient to establish a motivation to combine. Ex. 2032 ¶¶ 60-62. *See Virtek Vision Int'l ULC v. Assembly Guidance Sys., Inc.*, No. 2022-1998, 2024 WL 1292734, at *4 (Fed. Cir. Mar. 27, 2024) (finding no motivation to combine where limitations were "known" in the prior art). In short, Petitioner's Ground 1 applies the same hindsight bias that the Supreme Court and Federal Circuit have routinely rejected. *See KSR Intern Co., v. Telefex Inc*, 550 U.S. 398, 421 (2007) (warning against a "temptation to read into the prior art the teachings of the invention in issue" and instructing courts to "'guard against slipping into use of hindsight'" (quoting *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 36 (1996))). The Board should thus reject Petitioner's purported motivation to combine.

(2) Stone is not analogous art.

Petitioner's alleged motivation to combine also fails because Stone is not analogous art. The analogous art test is a "threshold" question in an obviousness analysis. *See, e.g.*, *Clay*, 966 F.2d at 658; *In re GPAC Inc.*, 57 F.3d 1573, 1577 (Fed. Cir. 1995) (analogous art inquiry is a "threshold issue"). "Generally, a skilled artisan would only have been motivated to combine analogous art." *In re Ethicon, Inc.*, 844 F.3d 1344, 1349 (Fed. Cir. 2017). The Petitioner bears the burden of establishing that a reference is analogous art. *Sanofi- Aventis Deutschland GmbH v. Mylan Pharms. Inc.*, 66 F.4th 1373, 1377 (Fed. Cir. 2023). Under the relevant test, "[p]rior art is analogous where either (1) 'the art is from the same field of endeavor, regardless of the problem addressed' or (2) even if the reference is not within the same field of endeavor, 'the reference still is reasonably pertinent to the particular problem with which the inventor is involved.'" *In re Ethicon, Inc.*, 844 F.3d 1344, 1349 (Fed. Cir. 2017) (quoting *In re Clay*, 966 F.2d 656, 658–59 (Fed. Cir. 1992)).

While the field of endeavor is "not limited to the specific point of novelty, the narrowest possible conception of the field, or the particular focus within a given field," *Unwired Planet, LLC v. Google Inc.*, 841 F.3d 995, 1001 (Fed. Cir. 2016), the field of endeavor cannot be defined "too broadly" such that it would be beyond what a POSITA would reasonably be expected to look for to find a solution to the

problem facing the inventor. *See, e.g.*, *Fresenius Med. Care Holdings, Inc. v. Baxter Intern., Inc.*, No. C 03-1431 SBA, 2006 WL 1343648, at *22 (N.D. Cal. May 16, 2006) (finding petitioner failed to establish same field of endeavor was "multi-parameter medical machines" where the challenged patent defined the field of endeavor as hemodialysis and asserted prior art was cardiopulmonary bypass materials); *Procter & Gamble Co. v. Team Techs., Inc.*, No. 1:12-CV-552, 2014 WL 12656554, at *25 (S.D. Ohio July 3, 2014) (finding patents-in-suit and prior art not in same field of endeavor where patents were "directed to application of a delivery system for treating the teeth" and prior art was directed to "keeping substances off the teeth").

Petitioner cannot show that Stone satisfies either element of this test. First, Stone is not in the same field of endeavor as the '656 Patent. Ex. 2032 ¶ 64. To determine the appropriate field of endeavor, the Board refers to explanations of the invention's subject matter in the patent application, including the embodiments, function, and structure of the claimed invention. *In re Bigio*, 381 F.3d 1320, 1325-26 (Fed. Cir. 2004). The background of the invention of the '656 Patent states that the claimed invention relates to improved techniques to prevent and detect fraud, particularly within electronic transactions. *See Airbus S.A.S. v. Firepass Corp.*, 941 F.3d 1374, 1380 (Fed. Cir. 2019) ("[S]tatements in the Background of the Invention section of the applicant's specification may be relied upon to delineate the field of

endeavor.") (citations and quotations omitted). The '656 Patent's claims are also solely focused on detecting and preventing fraud—by increasing feelings of guilt and the likelihood a perpetrator will be caught—as are the specification and the disclosed embodiments. *See generally* Ex. 1001; Ex. 2032 ¶ 64-65. Stone is only concerned with providing an improved currency display. *See* Stone at Abstract. It "relates to electronic visual displays, and in particular, to such displays that show a visual representation of financial instruments." Stone at [0002]. And a primary goal of Stone's claimed invention is to provide a "more visually rich interface." *Id.* at [0016]. It is not in the field of electronic fraud prevention. In fact, Stone never discusses fraud. Ex. 2032 ¶¶ 64-65.

Even if Petitioner contends the relevant field of endeavor is electronic financial transactions, this is not correct. As noted, Stone is not concerned with the actual processing of financial transactions or improving the processing of financial transactions. *See* Stone at [0023]. To the extent Stone mentions financial transactions, this is tangential to Stone's primary purpose—improving a user display. Ex. 2032 ¶ 66.

As for the second prong, Stone is not pertinent to the problem that the '656 Patent is concerned with solving—electronic payment fraud. "A reference is reasonably pertinent if . . . it is one which, because of the matter with which it deals, logically would have commended itself to an inventor's attention in considering his

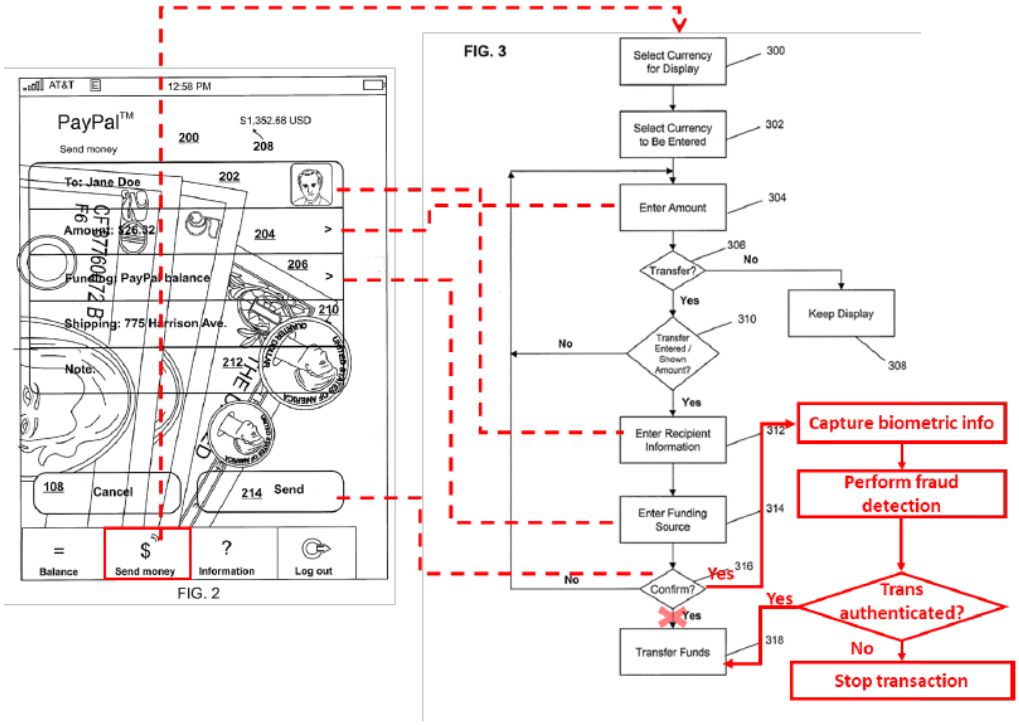
problem." *In re Clay,* 966 F.2d 656, 659 (Fed. Cir. 1992). "If a reference disclosure has the same purpose as the claimed invention, the reference relates to the same problem." *Id*. As just explained, the driving focus of the '656 Patent's claims is addressing the problem of electronic payment fraud. *See, e.g.*, Ex. 1001 at cl.1. Stone is not concerned with payment processing and does not even recognize payment fraud as a problem needing to be solved. Stone is therefore not analogous art to the '656 Patent, and this provides an independent basis to reject Petitioner's Ground 1.

(3) Stone, Hoyos, and Varghese teach away from each other.

"There is no suggestion to combine, however, if a reference teaches away from its combination with another source." *Tec Air, Inc. v. Denso Mfg. Mich. Inc.*, 192 F.3d 1353, 1360 (Fed. Cir. 1999). "A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant." *In re Urbanski*, 809 F.3d 1237, 1244 (Fed. Cir. 2016). Here, Stone and Hoyos teach away from each other in material ways such that a POSITA would not have been motivated to combine them.

The figure below illustrates Petitioner's Stone-Hoyos-Varghese electronic transaction model. The Stone interface is on the left (Fig. 2); the transaction flow

chart from Stone is to the right (Fig. 3), and the biometric "authentication process" from Hoyos is inserted into the flowchart represented by the red text on the far right.



Example of Stone-Hoyos
(annotated based on APPL-1008, FIGS. 2 and 3)

Pet. at 37.

As Dr. Goodrich notes, there are several problems with Petitioner's Stone-Hoyos transaction model. First, Stone and Hoyos teach away from each other and are incompatible because they are directed to different computing environments. Stone requires a client-server structure, *see* Ex. 1008 at [0040]-[0048] and Fig. 4, and Hoyos's disclosed authentication methods are employed locally on the device, with no mention of a server structure. *See, e.g.*, Hoyos cl. 4; *see also id.* at [0016]-[0022]; Ex. 2032 ¶ 68.

While Petitioner suggests that biometric authentication can be performed using either a server or client device, *see* Pet. 21, Stone provides no basis for applying Hoyos's authentication techniques locally because Stone discloses only a client-server structure for implementing its currency display. *See* Stone at [0045]-[0048] and Fig. 4. Stone discloses that the payment server maintains the user accounts, account information, and payment applications. *See id.* So for the system of Stone to perform a transaction, communication with the server is required. Ex. 2032 ¶ 69.

Employing local biometric authentication within Stone's client-server structure also does not make sense to a POSITA. Ex. 2032 ¶ 70. For one, this would be redundant. *South-Tek Systems, LLC v. Engineered Corrosion Solutions, LLC*, 748 Fed. Appx. 1003, 1006 (Fed. Cir. 2018) (finding lack of motivation to combine where resulting feature will be merely redundant to what the prior art device already had). As Stone Figure 2 shows, the user's account balance (208) is displayed on the interface *before* the user completes the transaction. Displaying an account balance would require some communication with the payment server where the user's account information must be stored, *see* [0047]-[0048] and Fig. 4, well before the end of the transaction where Petitioner inserts the Hoyos "authentication process." Inserting the Hoyos client-only authentication process as the final step before completing the transaction would then require on-device authentication *after* the

device has already transferred information in communication with payment server 408, which is redundant. Ex. 2032 ¶¶ 70-71.

Requiring local authentication in addition to requiring communication with a server to associate a user with their account and obtain necessary account information would also increase latency within the transaction, which undermines a primary goal of Hoyos (transaction speed) to address a problem that Stone does not even identify as a concern (electronic payment fraud), *see* Ex.1013, [0009], [0011], and would unnecessarily tie up resources on the user device that the client-server structure is meant to free up. Ex. 2032 ¶ 71.

A POSITA also would not have been motivated to implement the aliveness determination and matching techniques from Hoyos on a client-server structure. Doing so would undermine Hoyos's stated goals of improving speed, accuracy, and security of biometric authentication. Petitioner's expert, Dr. Jones, concedes as much by listing a series of benefits derived from local authentication as Hoyos discloses. These benefits include

> **reduced latency** (e.g., by minimizing communication delays between the user device and network server), **offline analysis capabilities** (allowing for analysis even when the user device is offline or has limited connectivity), **enhanced privacy** (by reducing the amount of data that needs to be transmitted to the server and minimizing potential privacy concerns), **efficient resource utilization** (helping distributing the processing load to the user device), **customization for device characteristics** (enhancing fraud detection by considering user device specific characteristics and capabilities), improved security (where a

> malicious actor intends to compromise the user device system), and **reduced server load for cost savings and improved scalability** (especially where the system has a large user base).

Ex. 1003 at ¶ 68.

While it may be true that a "given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine." *See Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed Cir. 2006). The "benefits, both lost and gained, should be weighed against one another." *Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 n.8 (Fed. Cir. 2000). Here, every one of these benefits provided by local authentication, like that envisioned by Hoyos, is undermined by employing a server structure. Latency is increased due to the time communicating with the server. There would be no offline capability. Privacy would not be improved, given the possibility of a data breach of the server where a user's biometric information would be stored. Resources would not be efficiently used as processing power on the device would be sacrificed. Ex. 2032 ¶¶ 71-73.

Ultimately, whether the references are not in the same field, not directed at the same problem, or simply not compatible, a POSITA would not have been motivated to combine Stone and Hoyos. Ex. 2032 ¶¶ 55-73.

A POSITA would also not have been motivated to combine Varghese with Stone and Hoyos. Ex. 2032 ¶¶ 74-78. First, Varghese amplifies the disconnect between Stone and Hoyos regarding the server and client distinction. Varghese, like

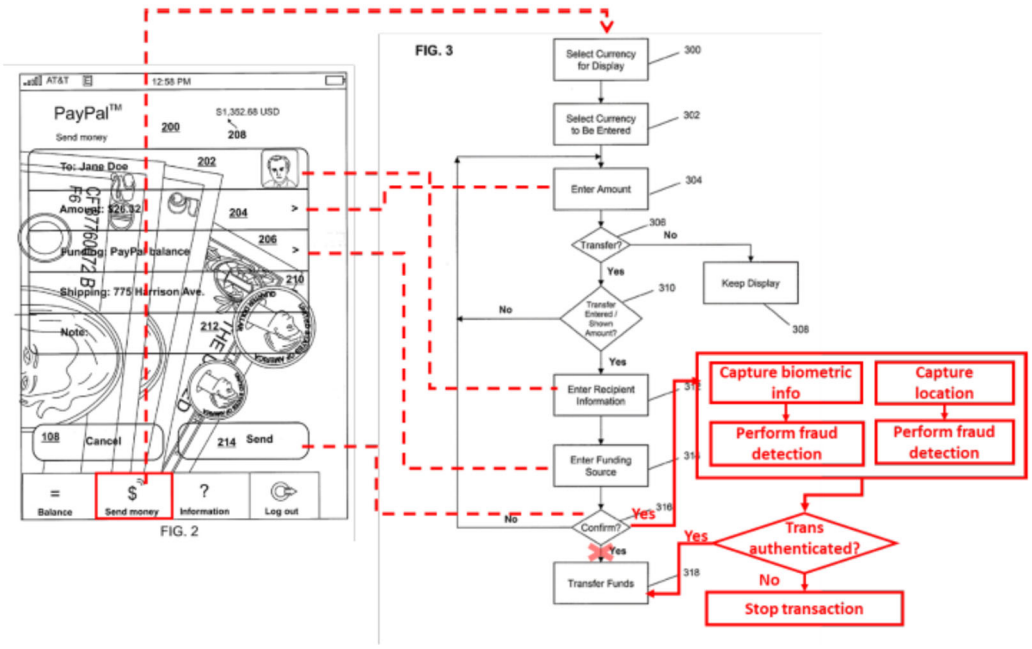
Stone, envisions a client-server structure. *See* Ex. 1010 at [0005-06]; Ex. 2032 ¶ 74. User authentication in Varghese involves information transferred from the client to the server. So for the reasons explained above in the discussion of the disparate structures of Stone and Hoyos, it would not make sense to combine techniques performed using a client-server structure (Varghese) with techniques performed only on a client device (Hoyos) to achieve the fraud analysis provided for in the '656 Patent's claims. Ex. 2032 ¶ 74.

Moreover, one of the goals of Varghese is to provide a "purely software based solution to identify theft that does not require hardware devices to be issued and maintained." Ex. 1010 at [0022]. The system envisioned by Varghese is centered on "device-based fraud monitoring" that includes "a repository of information for identifying legitimate and fraudulent users based on a more reliable and robust fingerprinting of the user device that can be integrated with other repositories of security tracking information." Varghese at [0017] and [0021]; Ex. 2032 ¶¶ 75-76. Varghese recognizes that such systems and methods were "currently lacking in the art" at the time. *Id.* at [0016]. The software-only goal of Varghese requires implementation through a client-server structure. Ex. 2032 ¶¶ 75-76. Varghese is also concerned with using information from the user's device itself rather than the user for fraud detection, *see* Varghese at [0017] and [0021]-[0022], and not concerned with implementing or improving sensor-based biometrics, such as

fingerprints and facial biometrics, on the user device that require *hardware* implementations (e.g., fingerprint scanners and forward-facing cameras). *See* Ex. 2032 ¶ 75 (citing Ex. 1013 at Fig. 2, [0018-19], [0034-36] (using camera to collect images of user for biometric authentication), [0022] (noting probability of biometric match can be calculated by "iris recognition, fingerprint image recognition, finger vein image recognition, or palm vein image recognition").

The hardware-based biometrics collection and authentication techniques described in Hoyos do not support Varghese's stated goal of providing a "purely software based solution to identify theft" (i.e., fraud detection), so a POSITA would not have been motivated to look to Hoyos to improve or alter the system disclosed by Varghese, specifically to reach the claimed solution of the '656 Patent claims. Ex. 2032 ¶ 76; *see In re Urbanski*, 809 F.3d at 1244 (finding reference teaches away where a POSITA "would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant").

Petitioner has also not established that a POSITA would have been motivated to add Varghese's collection of location information to the transaction flow laid out in Stone, particularly at the final confirmation stage. Ex. 2032 ¶ 77.



Example of Stone-Hoyos-Varghese
(annotated based on APPL-1008, FIGS. 2 and 3)

Pet. at 23.

Varghese specifically teaches against applying a location check as one of the final steps of the '656 Patent's claimed fraud detection analysis. Varghese discloses a multifactor authentication framework divided into pre-authentication and post-authentication stages. Ex. 1010 at [0074] and [0090]. Pre-authentication deals with collection of information related to the user and the user's device to authenticate a user logging into a web application—focusing heavily on information collected from the user's device (e.g., device fingerprint that involves collection of IP address information, among other things.) *Id.* at [0074]. A user login is not depicted in Petitioner's combined transaction model shown above. But it would undoubtedly

occur at a stage before the first step listed in the flowchart of Stone Fig. 3, as well as before the interface in Stone Fig. 2 would be presented to a user.

But perhaps most problematic for Petitioner, Varghese teaches that post-authentication is for completing monetary *electronic transactions*, which are authenticated using a user's transaction history and historic workflow. Ex. 1010 at [0065] ("User workflow sequences are authenticated (referred to herein as 'post-authentication') using a user's transaction history."). And "when a user is engaged in requesting transactions [post-authentication], criteria related to initial authentication [e.g., pre-authentication location data] are usually less important." Ex. 1010 at [0089]; Ex. 2032 ¶ 78. Based on Varghese's teaching, a POSITA would not have been motivated to collect location data (a pre-authentication technique for user login requests) to authenticate an *electronic transaction* [post-authentication request], particularly as the last step of a transaction as Petitioner claims.

b) Stone-Hoyos-Varghese does not disclose limitation [1.2].[1]

Limitation [1.2] is "receive biometric information associated with an account holder; store, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder." Pet. 31 (citing '656 Patent claim 1). Petitioner contends that "Stone describes receiving from an account holder (user 409), biometric information (to be stored as 'biometric id') associated with the account holder (user 409); and storing the biometric information as 'biometric id' in a data store (storage component 508) of user device 404, where the stored 'biometric id' is a user attribute of user identifier 418 associated with an account (account 422) of the account holder (user 409)." Pet. 31 (citing Ex. 1008 at [0045]).

But Petitioner fails to show that Stone discloses biometric information that is associated with an account of the account holder as limitation [1.2] requires. Ex. 2032 ¶¶ 79-85. Petitioner points to Figures 4 and 5 of Stone and the related descriptions in the specification as disclosing limitation [1.2]. Both figures are

[1] Limitation [1.2] is substantially similar to limitations [10.1] and [19.1]. Patent Owner's arguments with respect to limitation [1.2] thus equally apply to limitations [10.1] and [19.1].

reproduced below for reference. First, for the claim element "receive biometric information associated with an account holder" Petitioner points to the user identifier 418, which "may include attributes related to the user, such as personal information (e.g.,…biometric id)." *See* Pet. 31 (citing Ex. 1008 at [0045]). Petitioner states the user's (i.e., account holder's) "biometric id" is stored in a data store (storage component 508) of the user's device 404, in a data store (storage component 508) of user device 404, where the stored "biometric id" is a user attribute of user identifier 418 associated with an account (account 422) of the account holder (user 409)." Pet. 31 (citing Ex. 1008 at [0045]). However, Stone does not disclose any association of a user identified 418 with a user's account 422 that occurs on the user's device 404. Any association that may occur of a user identifier with a user account occurs on the payment server 408, not a data store on the user device. Ex. 2032 ¶¶ 81-85.

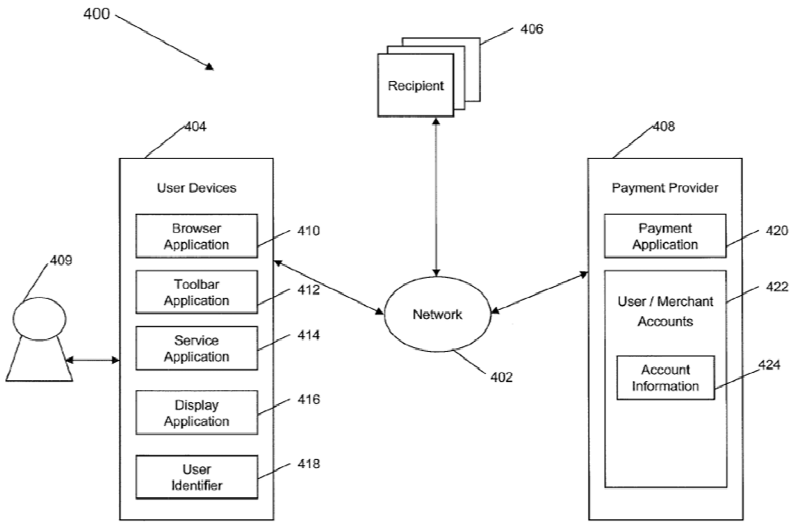


FIG. 4

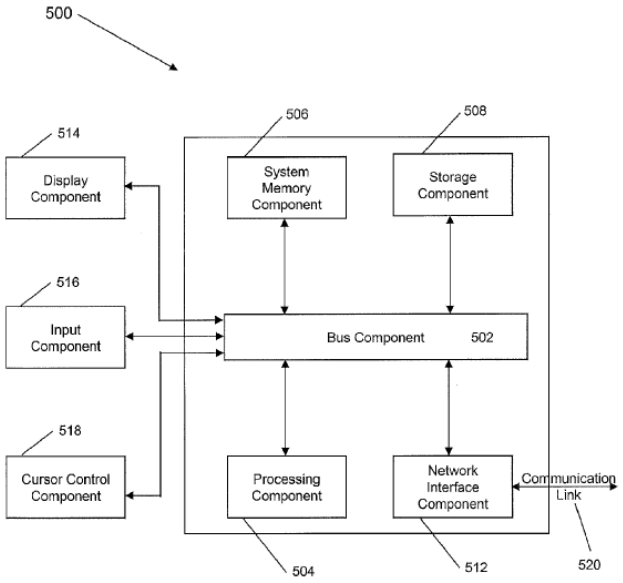
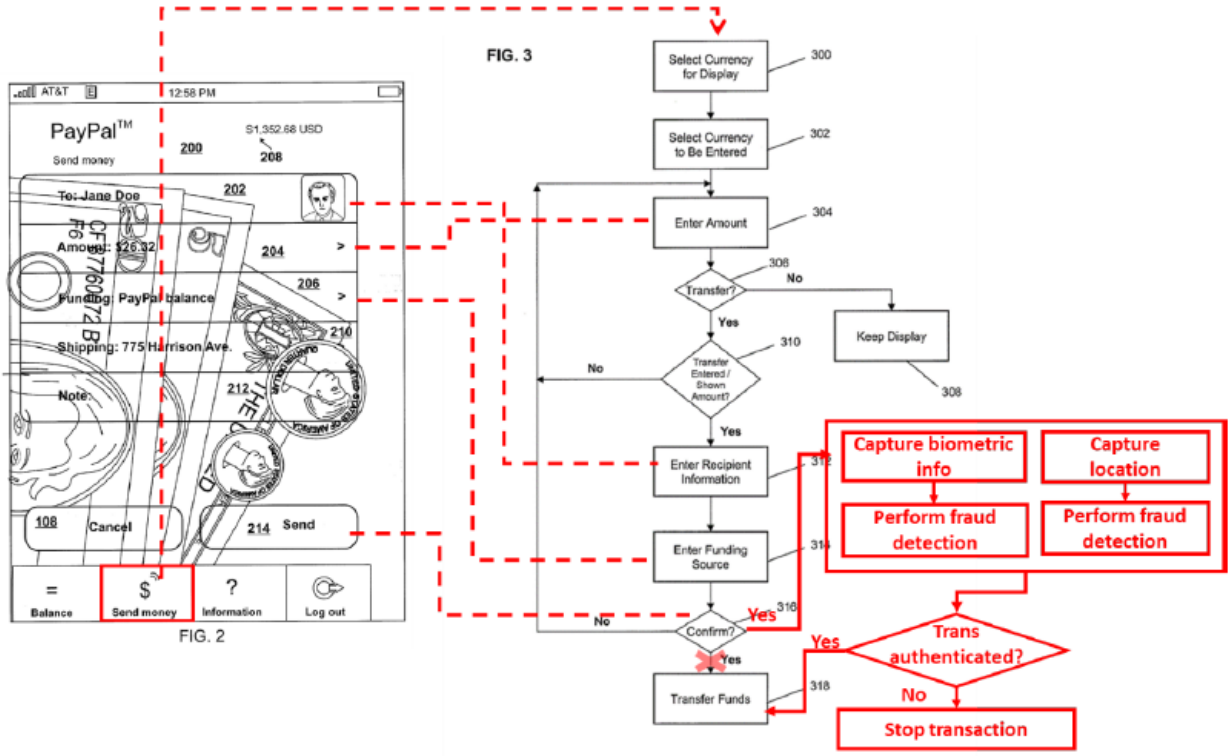


FIG. 5

Moreover, the payment server cannot disclose the "association" element of the claim because the "association" must occur *within* the data store after the biometric information is stored. *See* limitation [1.2] ("store, *in* a data store, the received biometric information, *wherein* the biometric information is associated with an account of an account holder" (emphasis added)); Ex. 2032 ¶ 82. Stone describes the "association" of user identifier 418 (e.g., biometric id) with an account as occurring in the payment server: "user identifier 418 may be passed request to payment provider server with a user money transfer 408**,** and user identifier 418 may be used by payment provider server 408 to associate user 409 with a particular user account maintained by payment provider server 408." Ex. 1008 at [0045]. Stone

provides no other disclosure for "associating" a user identifier with an account other than within the payment provider server.



Example of Stone-Hoyos-Varghese

(annotated based on APPL-1008, FIGS. 2 and 3)

Pet. at 23.

Even if Petitioner were to suggest that the association step occurring in the payment provider server discloses limitation [1.2], this would conflict with the '656 Patent's claimed transaction flow. Ex. 2032 ¶¶ 83-85. The independent claims of the '656 Patent include a timing requirement for the transaction flow as shown below.

> **[1.6]** ***subsequent to receiving the indication of the action taken by the user***, capture contextual information associated with the electronic

> transaction, the captured contextual information comprising captured biometric information and location data associated with the user;
>
> **[1.7.1]** perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises:
>
> > **[1.7.2]** performing a comparison based at least in part on the stored biometric information and the captured biometric information; and
> >
> > **[1.7.3]** determining, based at least in part on the captured biometric information, that the user is alive; and
>
> **[1.8]** based at least in part on both the user interaction with the transaction icon rendered in the interface and performing the fraud detection analysis, complete the electronic transaction; and

See Pet. "Listing of Challenged Claims" at vii-viii; Ex. 1001 at cl.1.

The "capture" of "biometric information and location data associated with the user," and "fraud detection analysis" comprising "performing a comparison based at least in part on the stored biometric information and the captured biometric information" must occur *after* the account holder's biometric information is stored and associated with the account of the account holder in limitation [1.2]. Ex. 2032 ¶ 84. Otherwise, there is no stored biometric information to be used for comparison. But Stone only discloses possibly associating the biometric id with a user's account "with a user money transfer request to the payment provider server," Ex. 1008 at [0045], i.e., after the user has completed the "confirm" step 316 in the graphic above. Ex. 2032 ¶ 84. So not only does this conflict with the '656 Patent's claimed

transaction, Stone's failure to disclose stored biometric information associated with a user prior to the time a transaction request is submitted to the server emphasizes that a POSITA would not have sought to implement Hoyos's (local) authentication techniques *after* Stone's "confirmation" step as the '656 Patent's claims require. This further proves that Petitioner's Ground 1 is rooted in hindsight bias. *Id.* at ¶¶ 82-84.

Finally, Petitioner contends that "to the extent Stone does not explicitly describe "biometric id" as the reference biometric information for comparison in authentication, Hoyos expressly describes receiving and storing biometric information during enrollment, and the stored biometric information is used for comparison with subsequent captured biometric data during transaction authentication." Pet. 33 (citing Ex. 1003, ¶94; Ex. 1013 ("Hoyos") at [0003]). But Hoyos does not disclose receiving, storing, and associating with an account biometric information in a data store in the exact manner claimed by the '656 Patent's limitation [1.2]. Ex. 2032 ¶ 85. The portion of Hoyos that Petitioner cites as disclosing limitation [1.2] is a generic description of the biometric matching technology known in the prior art at the time the Hoyos application was filed. *See* Pet. 33 (citing Hoyos at [0003] ("Biometric identification and authentication systems…are known to be useful for [] **comparing** biometric data acquired from an individual to **stored sets of biometric data of known "enrolled" individuals**")).

Not only is this not a disclosure of limitation [1.2], but a POSITA would not have been motivated to combine Hoyos's local authentication with Stone's client-server structure, particularly in terms of the "association" step that occurs on the payment server 408 in Stone. *See* Ex. 2032 ¶¶ 79-85.

c) Stone-Hoyos-Varghese does not disclose Limitation [1.9].

Limitation [1.9] recites "a memory coupled to the processor and configured to provide the processor with instructions." Petitioner contends that "Stone discloses a memory (e.g., system memory component 506 of FIG. 5) coupled to a processor 504 in each device of the system, and the memory is configured to provide the processor with instructions for various processes for an electronic transaction." Pet. 51. However, Petitioner fails to identify in Stone "a memory coupled to the processor and configured to provide the processor with instructions," as required by claim 1 of the '656 Patent. *See* Ex. 2032 ¶¶ 86-87.

The embodiment of system 500 depicted in Figure 5 of Stone may be a part of a cell phone, personal computer, and/or a network server. *See* Stone at [0049]. Stone states that "system 500 performs specific operations by processor 504 executing one or more sequences of one or more instructions contained in the system memory component 506." Stone at [0050].

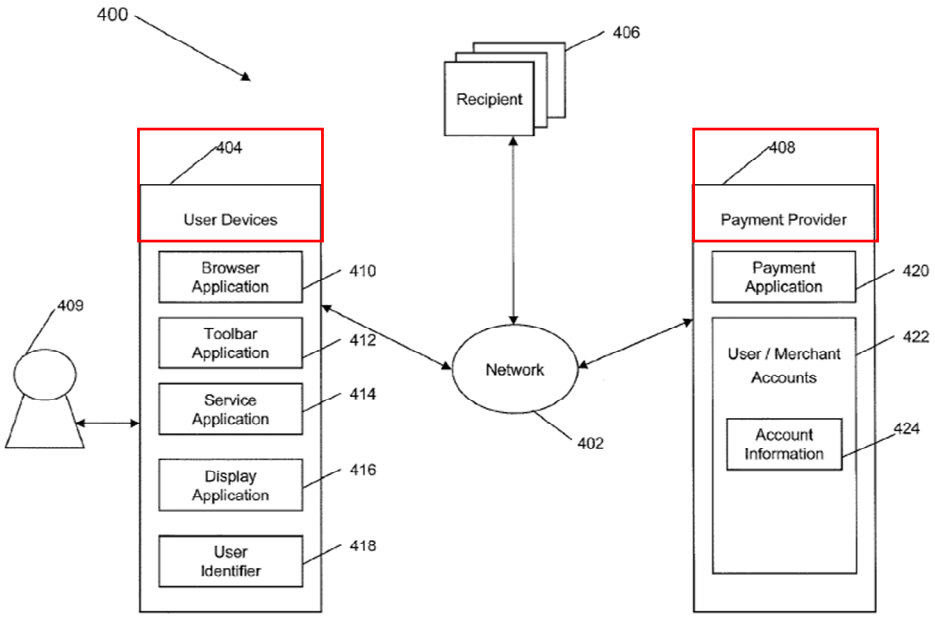

400
406
Recipient
404
User Devices
408
Payment Provider
Browser Application
410
Payment Application
420
409
Toolbar Application
412
User / Merchant Accounts
422
Network
Service Application
414
Account Information
424
402
Display Application
416
User Identifier
418

FIG. 4

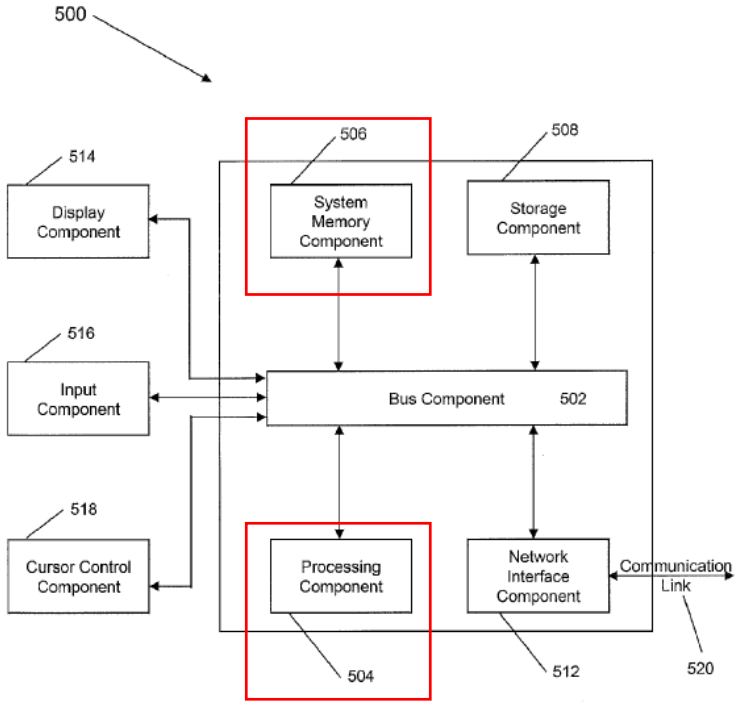

500
506
508
514
System Memory Component
Storage Component
Display Component
516
Input Component
Bus Component
502
518
Cursor Control Component
Processing Component
Network Interface Component
Communication Link
504
512
520

FIG. 5

For the disclosure of "a processor" in limitation [1.1], Petitioner identifies in Stone "processor 504 in user device 404 alone, or in combination with other processors including the processor 504 of other devices" as being "configured to perform processes for a transaction." Pet. 29-30; Ex. 2032 ¶ 87. Based on the antecedent basis rule, "the processor" in limitation [1.9] refers to the processor identified in limitation [1.1], which performs the other claim limitations in claim 1. *See NTP, Inc. v. Research in Motion, Ltd.*, 418 F.3d 1282, 1306 (Fed. Cir. 2005) (noting use of "a" followed by use of "the" indicates reference to the same "destination processor"); *Warner-Lambert Co. v. Apotex Corp.*, 316 F.3d 1348, 1356 (Fed. Cir. 2003) ("[I]t is a rule of law well established that the definite article 'the' particularizes the subject which it precedes.").

For the storing and "association" of the biometric information with the account of the account holder required by limitation [1.2], this is done by the payment server 408 as described in the analysis of that limitation. *See* III.A.1.b. As limitation [1.9] requires "a memory coupled to the processor," for Stone to disclose limitation [1.9] under Petitioner's theory, the "memory" must be at least coupled to the payment server 408 since the payment server must perform the association step. Ex. 2032 ¶ 87. But since Petitioner only identifies the "processor" for limitation [1.1] as the processor on user device 404, Petitioner fails to identify "a memory coupled to *the* processor" as limitation [1.9] requires. *Id.*

2. Stone in combination with Hoyos and Varghese does not render the dependent claims obvious.

Petitioner has not shown that Stone-Hoyos-Varghese renders obvious independent claims 1, 10, and 19. Because the dependent Challenged Claims depend from these independent claims, Stone-Hoyos-Varghese does not render obvious any of the dependent Challenged Claims 4-9 and 13-18 for the same reasons Stone-Hoyos-Varghese does not render obvious the independent claims. Stone-Hoyos-Varghese does not disclose the dependent limitations of claims 5, 8, 14, and 17. Ex. 2032 ¶¶ 88-90.

a) Stone in combination with Hoyos and Varghese does not disclose or render obvious "wherein the transaction icon includes a graphical representation of payment form" in claims 5 and 14.

Dependent claims 5 and 14 require the system of claim 1 (for claim 5) and the method of claim 10 (for claim 14) "wherein the transaction icon comprises a graphical representation of a payment form." Neither Stone nor Hoyos discloses that a transaction icon can be a payment form. Rather, Petitioner states simply that "a POSITA would have been motivated to implement the funding source selection using a form of payment icon (e.g., 'the specific card, such as a PayPal card, Visa, MC, AMEX') for improved visual presentation." Pet. at 53-54. But Petitioner provides no explanation why this would be obvious without working backward from claim 4 of the '656 Patent using hindsight.

b) Stone in combination with Hoyos and Varghese does not disclose or render obvious "wherein the virtual likeness comprises an avatar selected by the account holder" in claims 8 and 17.

Dependent claims 8 and 17 require the system of claim 1 (for claim 8) and the method of claim 9 (for claim 17) "wherein the virtual likeness of the face of the recipient comprises an avatar of the recipient." Stone-Hoyos-Varghese does not disclose the use of an avatar to represent an account holder. Ex. 2032 ¶ 90. Petitioner, instead, merely states that an "avatar is a well-known alternative of a picture for a user icon renders this element obvious." Pet. at 56. But that a claim element is well known does not render it obvious. Besides being "well known," Petitioner provides no justification why it would be obvious to use an avatar for an electronic payment system to reach the invention of the '656 Patent's claims 8 and 17, other than hindsight bias. Ex. 2032 ¶ 90.

B. Ground 2: The Combination of Stone and the FFIEC Guidance Does Not Render the Challenged Claims Obvious.

Petitioner asserts that Stone in view of the FFIEC Guidance renders obvious independent claims 1, 10, and 19 and dependent claims 4-9 and 13-18 of the '656 Patent. As explained below the Stone-FFIEC Guidance combination does not render the Challenged Claims obvious. Ex. 2032 ¶¶ 91-100.

1. Stone-FFIEC Guidance does not render the independent claims obvious.

Petitioner fails to show that the ’656 Patent’s independent claims 1, 10, and 19 are invalid for at least three reasons. First, Petitioner fails to establish that a POSITA would have combined Stone with the FFIEC Guidance resulting in the claims of the ’656 Patent and would have had a reasonable expectation of success in doing so. Ex. 2032 ¶¶ 93-99. Second, Stone-FFIEC Guidance does not disclose storage of biometric information in a data store, wherein the biometric information is associated with an account of the account holder as required by the ’656 Patent’s independent claims. *Id.* at ¶ 92. Finally, Stone-FFIEC Guidance does not disclose “a memory coupled to the processor” as required by the ’656 Patent’s independent claims. *Id.*

a) Stone-FFIEC Guidance does not disclose limitation [1.2].

For limitation [1.2], Petitioner’s Ground 2 relies on the same elements of Stone it relied on in Ground 1 as disclosing this limitation. Stone-FFIEC Guidance therefore fails to render obvious limitation [1.2] for the same reasons explained for Ground 1 above. Ex. 2032 ¶ 92.

b) Stone-FFIEC Guidance does not disclose Limitation [1.9].

For the limitations requiring "a memory coupled to the processor and configured to provide the processor with instructions," Petitioner's Ground 2 relies on the same elements of Stone it relied on in Ground 1 as disclosing this limitation. The Stone-FFIEC Guidance therefore fails to render obvious limitation [1.9] for the same reasons explained for Ground 1 above. Ex. 2032 ¶ 92.

c) Petitioner fails to establish that a POSITA would have been motivated to combine Stone with the FFIEC Guidance and would have had a reasonable expectation of success in doing so.

Petitioner fails to establish that a POSITA would have combined Stone with the FFIEC Guidance with a reasonable likelihood of success that would result in the claims of the '656 Patent. The Petitioner's explanation for the alleged motivation to combine is conclusory. Ex. 2032 ¶¶ 94-99. Additionally, Stone is not analogous art to the '656 Patent, which itself is sufficient to establish a lack of motivation to combine. Ex. 2032 ¶ 93.

(1) Petitioner's conclusory explanation for the motivation to combine Stone and the FFIEC Guidance is insufficient.

Like with Stone-Hoyos-Varghese, Petitioner's alleged motivation to combine Stone and the FFIEC Guidance is also conclusory. Ex. 2032 ¶¶ 94-99. It consists of four paragraphs that recite functionality and give boilerplate statements. *See* Pet. at

62-63. For example, Petitioner states that a POSITA would have understood based on the Guidance that multifactor authentication can reduce fraud and improve customer protection. *Id.* at 63.

Based on this understanding, Petitioner then states that "a POSITA would have been motivated to apply Guidance's teaching of multifactor, real-time, contextual-based and risk-based authentication in Stone for the benefits of improved security and boosted customer confidence for service providers, and the additional benefits of FFIEC compliance for federal supervised financial institutions." Pet. 62; Ex. 2032 ¶ 95.

Petitioner's assertions are conclusory and provide no actual explanation for *why* a POSITA would have combined Stone and the Guidance. Petitioner presumes that Stone had a need for authentication for fraud detection. But Stone is not concerned with security of transactions. It is concerned with providing an improved display for the user and a "richer interface" that provides a currency display. Ex. 1008 at [0016]. Stone also does not view fraud as a problem that needs to be addressed, with increased security, nor does it even mention electronic payment fraud. *See supra* III.A.1.c. In fact, it is telling that whenever Petitioner states the proposition that Stone had a need for fraud detection, Petitioner never once cites the Stone reference. *See, e.g.*, Pet. at 63.

The FFIEC Guidance is also not concerned with the goals and purpose of Stone's disclosures. The Guidance is not concerned with conveying amounts of funds or visual representations of currency or providing a digital interface. It simply discusses biometrics and security in broad, general terms. Ex. 1037 at 1-2, 9-11. The Guidance also never discusses using multifactor or biometric authentication with a digital interface, or combining these components in an ordered manner like the claims of the '656 Patent. Ex. 2023 ¶¶ 96-97.

A POSITA also would not have combined Stone with the FFIEC Guidance because the Guidance is outside a POSITA's area of interest as defined by Petitioner. A reference is considered publicly accessible if "persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it." *Samsung Elecs. Co., Ltd. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1369 (Fed. Cir. 2019). Petitioner has defined a POSITA as one holding "a bachelor's degree in electrical engineering, computer engineering, computer science, or a related field, and at least two years of experience in the research, design, development, and/or testing of biometric authentication techniques, and related firmware and software, or the equivalent." *See* Section II.C. An engineer fitting this description and exercising reasonable diligence would not have been inclined to look to high-level and non-technical regulatory guidance directed to the banking industry to develop precise technical solutions for electronic fraud. Ex. 2023 ¶ 98.

Petitioner's argument, again, amounts to hindsight combination of these references to reach the limitations of the '656 Patent's independent claims without giving anything more than perfunctory statements for why a POSITA would have combined them. *See* Pet. at 62-63; Ex. 2023 ¶¶ 94-99. Pointing out that a patent's limitations were simply known across multiple prior art references does not establish a motivation to combine. *See Virtek Vision Int'l ULC*, 2024 WL 1292734, at *4 (finding no motivation to combine where limitations were "known" in the prior art). Rather, the Stone-Guidance combination was constructed in hindsight by taking the '656 Patent's claims and working backward to pull limitations from unrelated prior art references.

(2) Stone is not analogous art.

For the reasons explained in the discussion of Ground 1, Stone is not analogous art to the '656 Patent, so a POSITA would not have been motivated to combine it with the FFIEC Guidance to reach the claims of the '656 Patent. Ex. 2032 ¶ 93.

2. Stone-FFIEC Guidance does not render the dependent claims obvious.

Petitioner has not shown that the Stone-FFIEC Guidance renders obvious independent claims 1, 10, and 19. Because the dependent Challenged Claims depend from these independent claims, Stone-FFIEC Guidance does not render obvious any

of the dependent Challenged Claims for the same reasons this combination does not render the independent claims obvious. Further, Stone-FFIEC Guidance does not disclose the dependent limitations of claims 5, 8, 14, and 17 for the same reasons explained in Ground 1. Ex. 2032 ¶ 100.

C. Ground 3: The Combination of Stone in View of Hoyos, Varghese, and Borovsky Does Not Render the Challenged Claims Obvious.

Petitioner asserts that Stone in view of the Hoyos, Varghese, and Borovsky renders obvious dependent claims 2-3 and 11-12 of the ’656 Patent. As Petitioner states, the claim analysis for Ground 3 relies on the same analysis and evidence provided for Ground 1 (Stone-Hoyos-Varghese), except where additional analysis is provided for the dependent limitations for the respective claims. Because claims 2-3 and 11-12 depend from independent claims, Stone-Hoyos-Varghese-Borovsky does not render obvious any of these dependent claims for the same reasons that Stone-Hoyos-Varghese does not render the independent claims obvious. Ex. 2032 ¶¶ 101-02.

It would also not have been obvious to combine Stone and Borovsky as Petitioner argues. Petitioner states that “Stone has the need to obtain for display on the user device, pictures of other users connected to a network with the user.” Pet. 78; Ex. 1003 at ¶ 278. Petitioner further states that “[f]acing the need of Stone, a POSITA would have been motivated apply Borovsky’s teaching of providing

contact photo obtained from social network sites for user device contact display as icons for network-connected users on user device, especially in the case that the other user did not profile a profile icon, for the benefits of enhanced user experience with helpful visuals, increased transaction confidence and efficient identification." *Id.* But Petitioner does not state why a social networking site would be the obvious source for obtaining a user photo in Stone. Ex. 2032 ¶ 102. For example, Stone does not discuss using social networks to populate any information for the disclosed interface. The source of information is all directly provided by the user (e.g. user identifier 418) and/or banking or credit card information from the payment server 408. *See* Ex. 1008 at [0020], [0036], [0045-48]. Nothing in Stone suggests introducing another third-party server to Stone's existing client-server. The only motivation for doing would be conceived in hindsight working backward from the '656 Patent's claims.

D. Ground 4: The Combination of Stone in View of FFIEC Guidance and Borovsky Does Not Render the Challenged Claims Obvious.

Petitioner asserts that Stone in view of the FFIEC Guidance and Borovsky renders obvious dependent claims 2-3 and 11-12 of the '656 Patent. As Petitioner states, the claim analysis for Ground 4 relies on the same analysis and evidence provided for Ground 2 (Stone-Guidance), except where additional analysis is provided for the dependent limitations for the respective claims. Because claims 2-

3 and 11-12 depend from independent claims, Stone-FFIEC Guidance-Borovsky does not render obvious any of these dependent claims for the same reasons that Stone-FFIEC Guidance does not render the independent claims obvious. Ex. 2032 ¶¶ 101-02.

It would also not have been obvious to combine Stone and Borovsky as Petitioner claims. Petitioner states that "Stone has the need to obtain for display on the user device, pictures of other users connected to a network with the user." Pet. 78; Ex. 1003 at ¶ 278. Petitioner further states that "[f]acing the need of Stone, a POSITA would have been motivated apply Borovsky's teaching of providing contact photo obtained from social network sites for user device contact display as icons for network-connected users on user device, especially in the case that the other user did not profile a profile icon, for the benefits of enhanced user experience with helpful visuals, increased transaction confidence and efficient identification." *Id.* But Petitioner does not state why a social networking site would be the obvious source for obtaining a user photo in Stone. Ex. 2032 ¶ 102. For example, Stone does not discuss using social networks to populate any information for the disclosed interface. *Id.* The source of information is all directly provided by the user (e.g. user identifier 418) and/or banking or credit card information from the payment server 408. *See* Ex. 1008 at [0020], [0036], [0045-48]. Nothing in Stone suggests introducing another third-party server to Stone's existing client-server. The only

motivation for doing would be conceived in hindsight working backward from the '656 Patent's claims. Ex. 2032 ¶¶ 101-02.

For the reasons explained in Ground 3, it would also not have been obvious to combine Stone and Borovsky as Petitioner claims.

IV. PETITIONER'S VIOLATION OF *SOTERA* STIPULATION

Petitioner submitted a *Sotera* stipulation in this proceeding in hopes that the Board would institute this IPR, despite the parallel Texas district court litigation that was in its advanced stages at that time. Ex. 1048 at 1; *see* Exs. 2001-2021. Specifically, Petitioner stipulated as follows:

> Petitioner Apple Inc. ("Apple") hereby stipulates that if the Patent Trial and Appeal Board (PTAB) institutes the IPR based on the grounds identified below [ground 1—Stone and Hoyos; ground 2—Stone, Hoyos, and Varghese; and ground 3—Stone and the Guidance], then it (i) will not pursue the grounds identified below in the Parallel District Court Litigation [the Texas case] and (ii) ***will not pursue any other ground that reasonably could have been raised during the IPR (should it be instituted) in the Parallel District Court Litigation.***

Ex. 1048 at 1 (emphasis added).

Based on Petitioner's *Sotera* stipulation, the Board instituted this IPR, "declin[ing] to exercise [its] discretion under § 314(a) to deny institution in view of the Texas case." *See* Institution Decision (Paper 10) at 17-19 (citing Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (June 21, 2022) at 3, 7, 9).

Despite its *Sotera* stipulation, Petitioner now asserts nine obviousness grounds in the parallel Texas district court litigation, all of which consist of printed publication references, or references materially identical to the printed publications, that reasonably could have been raised in this IPR. *See* Ex. 2033 (Apple Inc.'s Final Election of Asserted Prior Art). In raising these grounds, Petitioner has gone back on its stipulation to the Board (and to Patent Owner) that Petitioner made to secure institution of this IPR. Petitioner's violation of its stipulation may result in "potentially conflicting decisions and duplicative efforts between the district court and the PTAB"—the precise harm the *Sotera* procedure is meant to avoid.

V. CONCLUSION

For the reasons provided above, Patent Owner respectfully requests that the Board find all claims of the '656 Patent valid.

Dated: October 24, 2024

Respectfully submitted,

/s/Richard A. Kamprath
Richard A. Kamprath
Reg. No. 65,320
rkamprath@mckoolsmith.com
Bradley Jarrett (*pro hac vice*)
bjarrett@mckoolsmith.com
McKool Smith, P.C.
300 Crescent Court, Suite 1500
Dallas, Texas 75201
Telephone: (214) 978-4000
Facsimile: (214) 978-4044

George Fishback

Reg. No. 76,345
gfishback@mckoolsmith.com
McKool Smith, P.C.
303 Colorado Street, Suite 2100
Austin, Texas 78701
Telephone: (512) 692-8700
Facsimile: (512) 692-8744

Counsel for Patent Owner, Carbyne Biometrics, LLC

CERTIFICATION OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned **PATENT OWNER'S RESPONSE** specified in 37 C.F.R. §42.24 have 10,556 words, in compliance with the 14,000 word limit set forth in 37 C.F.R. §42.24(b)(1). This word count was prepared using Microsoft Word 2010.

Dated: October 24, 2024

Respectfully submitted,

/s/Richard A. Kamprath
Richard A. Kamprath
Reg. No. 65,320

CERTIFICATION OF SERVICE

The undersigned hereby certifies that a copy of this **PATENT OWNER'S RESPONSE PURSUANT TO 37 C.F.R. § 42.10(b)** has been served on Petitioner via email on the following counsel of record for Petitioner:

David W. O'Brien
David.obrien.ipr@haynesboone.com

Kelly Gehrke Lyle
Kelly.lyle@haynesboone.com

Hong Shi
Hong.shi.ipr@haynesboone.com

Dated: October 24, 2024

Respectfully submitted,

/s/Richard A. Kamprath
Richard A. Kamprath
Reg. No. 65,320