

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner

Case No. IPR2024-00331
Patent No. 11,526,886

PATENT OWNER'S NOTICE OF APPEAL

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Pursuant to 35 U.S.C. §§ 141-142 and 319, 37 C.F.R. §§ 90.2-90.3, Federal Rule of Appellate Procedure 15, and Federal Circuit Rule 15, Patent Owner Carbyne Biometrics, LLC (“Carbyne”) hereby provides notice that it appeals to the United States Court of Appeals for the Federal Circuit from the Final Written Decision of the Patent Trial and Appeal Board (the “Board”) entered on July 14, 2025 (Paper 26,), and from all underlying findings, determinations, rulings, opinions, orders, issues, and decisions regarding the *inter partes* review of United States Patent No. 11,526,886 B1 (“the ’886 Patent”). This Notice of Appeal and petition for review of the Final Written Decision are timely under 37 C.F.R. § 90.3(a)(1), having been filed within 63 days of the Order Denying Request for Director’s Review.

For the limited purpose of providing the Director with the information requested in 37 C.F.R. § 90.2(a)(3)(ii) and Federal Rule of Appellate Procedure 15(a)(2)(C), issues on appeal may include but are not limited to the Board’s factual findings and conclusions of law, the Board’s determinations of the unpatentability of claims and any finding or determination supporting or relating to such determinations of unpatentability, including but not limited to obviousness issues, the scope of the alleged prior art, Board findings that conflict with the evidence of record and are not supported by substantial evidence, as well as all other issues decided adversely to Patent Owner in any orders, decisions, rulings and/or opinions, further including but not limited to: (i) the Board’s interpretation of the alleged prior

art; (ii) the Board's determination that claims 1-12, 14-18, and 20-23 of the '886 patent were shown to be anticipated and/or obvious under 35 U.S.C. § 103(a), and are thus unpatentable; (iii) the Board's legal errors in undertaking its obviousness analyses; (iv) the Board's motivation to combine analyses; (v) the Board's findings that conflict with the evidence of record or are otherwise unsupported by substantial evidence; (vi) the Board's failure to consider evidence of record (including testimonial and documentary) fully and properly; and (vii) any other findings or determinations supporting or relating to these issues as well as all other issues decided adversely to Patent Owner in any orders, decisions, rulings, or opinions in this proceeding.

Patent Owner reserves the right to challenge any finding or determination supporting or relating to the issues above and reserves the right to address any issues that may arise on appeal or that Petitioner may raise on appeal.

Simultaneously with this submission, Patent Owner is filing a true and correct copy of this Notice of Appeal with the Director of the United States Patent and Trademark Office as well as a true and correct copy of the same, along with the required filing fee, with the Clerk of the United States Court of Appeals for the Federal Circuit as set forth in the accompanying Certificate of Filing.

Dated: September 15, 2025

Respectfully submitted,

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

Attorney for Patent Owner,
Carbyne Biometrics, LLC

CERTIFICATE OF FILING

The undersigned hereby certifies that, in addition to being electronically filed, a true and correct copy of the above-captioned **PATENT OWNER'S NOTICE OF APPEAL** is being submitted via email to the Director on September 15, 2025, at the following email address:

Director of the United States Patent and Trademark Office
c/o Office of the General Counsel, 10B20
United States Patent and Trademark Office
efileSO@uspto.gov

The undersigned also hereby certifies that a true and correct copy of the above-captioned PATENT OWNER'S NOTICE OF APPEAL and the filing fee is being filed via CM/ECF with the Clerk's Office of the United States Court of Appeals for the Federal Circuit on September 15, 2025.

Respectfully submitted,

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

Attorney for Patent Owner, Carbyne
Biometrics, LLC

CERTIFICATION OF SERVICE

The undersigned hereby certifies that a copy of this **PATENT OWNER'S NOTICE OF APPEAL** 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: September 15, 2025

Respectfully submitted,

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

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner.

IPR2024-00331
Patent 11,526,886 B1

Before JAMESON LEE, ARTHUR M. PESLAK, and
STEVEN M. AMUNDSON, *Administrative Patent Judges*.

AMUNDSON, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

Apple Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1–12, 14–18, and 20–23 in U.S. Patent No. 11,526,886 B1 (“the ’886 patent”) (Exhibit 1001) under 35 U.S.C. §§ 311–319. Paper 2 (“Pet.”). Carbyne Biometrics, LLC (“Patent Owner”) filed a Preliminary Response. Paper 7 (“Prelim. Resp.”). Further, after receiving Board authorization to address certain issues, Petitioner filed a Preliminary Reply, and Patent Owner filed a Preliminary Sur-reply. *See* Paper 8 (“Prelim. Reply”); Paper 9 (“Prelim. Sur-reply”); Ex. 3001.

In the Institution Decision, we instituted review based on all challenged claims and all challenges included in the Petition. Paper 10 (“Inst. Dec.”).

We have jurisdiction under 35 U.S.C. § 6. We issue this Final Written Decision under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons explained below, Petitioner has shown by a preponderance of the evidence that claims 1–12, 14–18, and 20–23 in the ’886 patent are unpatentable. *See* 35 U.S.C. § 316(e) (2024).

II. BACKGROUND

A. Procedural History

After we instituted review, Patent Owner filed a Response to the Petition. Paper 17 (“Resp.”). Petitioner filed a Reply to Patent Owner’s Response. Paper 19 (“Reply”). Patent Owner filed a Sur-reply to Petitioner’s Reply. Paper 20 (“Sur-reply”).

In May 2025, we held an oral hearing. The record includes the hearing transcript. Paper 28 (“Tr.”).

B. Real Parties in Interest

Petitioner identifies itself as the sole real party in interest. Pet. 1.
Patent Owner identifies itself as the sole real party in interest. Paper 3, 2.
The parties do not raise any issue about real parties in interest.

C. Related Matters

Petitioner and Patent Owner identify the following civil action as a related matter: *Carbyne Biometrics, LLC v. Apple Inc.*, No. 1:23-cv-00324 (W.D. Tex. filed March 24, 2023). Pet. 1; Paper 3, 2.

D. The '886 Patent (Exhibit 1001)

The '886 patent, titled “Method, Medium, and System for Reducing Fraud,” issued on December 13, 2022, from an application filed on June 4, 2020. Ex. 1001, codes (22), (45), (54). The patent identifies that application as the latest application in a series of continuation applications with the initial application filed on May 3, 2011. *Id.* at 1:7–20, code (63).

The '886 patent describes fraudulent electronic transactions as “an ongoing problem.” Ex. 1001, 1:29. According to the patent, “[e]lectronic fraud can be particularly devastating because the perpetrator does not need physical access to a victim’s credit card (or other resource) to perform the fraud.” *Id.* at 1:34–37.

The '886 patent's Figure 1 (reproduced below) depicts an example of an electronic environment where fraudulent transactions may occur:

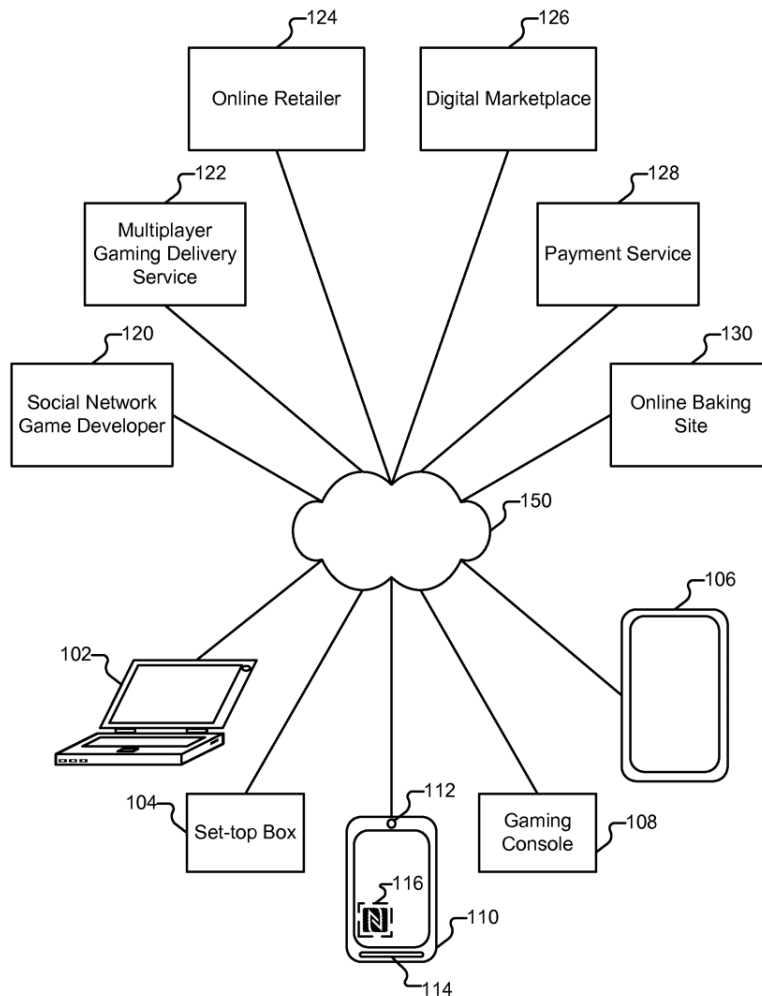


FIG. 1

Figure 1 illustrates an example of an electronic environment where “users of clients 102–110 engage in transactions involving various service providers 120–130 via one or more networks (represented herein as a single network cloud 150).” Ex. 1001, 1:46–47, 2:40–41, 2:51–54, Fig. 1. In Figure 1, the clients include laptop computer 102, set-top box 104, tablet computer 106, gaming console 108, and mobile telephone 110. *See id.* at 2:66–4:14, 13:33–34, Fig. 1. Mobile telephone 110 includes front-facing camera 112,

microphone 114, and near-field-communication (NFC) chip 116. *Id.* at 3:64–67, 13:33–34, Fig. 1.

As an example of a fraudulent transaction, “[a] family member of the laptop owner purchases a magazine from retailer 124, using laptop 102, without the laptop owner’s permission.” Ex. 1001, 3:4–7. As another example of a fraudulent transaction, “[s]tored within set-top box 104 is the credit card information of the individual renting the movies,” and “[a] roommate of the individual uses device 104 to rent a movie without the individual’s permission.” *Id.* at 3:13–16. As yet another example of a fraudulent transaction, “[a] daughter uses device 110 to send a premium SMS (e.g., to contribute money to a disaster relief fund) or to download for-pay applications from digital marketplace 126 without her mother’s permission.” *Id.* at 3:56–60.

“In each of the above examples of fraudulent transactions, the would-be perpetrators (also referred to herein as ‘fraudsters’) are family members, friends, colleagues, or persons that otherwise have some personal relation with the victim.” Ex. 1001, 4:15–18. The fraudsters “are probably not hardened criminals, but regular people who fall for the temptation.” *Id.* at 4:19–20. Yet the “otherwise honest fraudsters” still commit fraudulent transactions. *Id.* at 4:25–27.

To reduce fraudulent transactions, the ’886 patent discloses techniques for:

- (1) “increasing the guilt felt by fraudsters when they are about to commit a fraudulent transaction”; and
- (2) “increasing the likelihood (either real or as perceived by the fraudster) that the fraudulent act will be detected.”

Ex. 1001, 4:52–59; *see id.* at 7:55–59. The techniques “can be used with devices and services that are not protected by passwords, or where passwords are commonly shared.” *Id.* at 2:41–44.

The ’886 patent explains that the amount of money involved in an electronic financial transaction may seem “less concrete” than the same amount of tangible currency. *See* Ex. 1001, 5:6–11. Specifically, “physical cash is a concrete, tangible item while a digital payment for a digital good is a more abstract concept.” *Id.* at 4:39–41. The “more concrete the value of a transaction is,” however, “the more guilty a fraudster might feel when perpetrating the fraud.” *Id.* at 5:4–6. “Feelings of guilt for engaging in fraudulent transactions can be increased both by making a given transaction more concrete, and by emphasizing the victim’s identity.” *Id.* at 5:27–29.

The '886 patent's Figure 4 (reproduced below) depicts an interface for an electronic device that seeks to make a given transaction more concrete and emphasize the victim's identity:

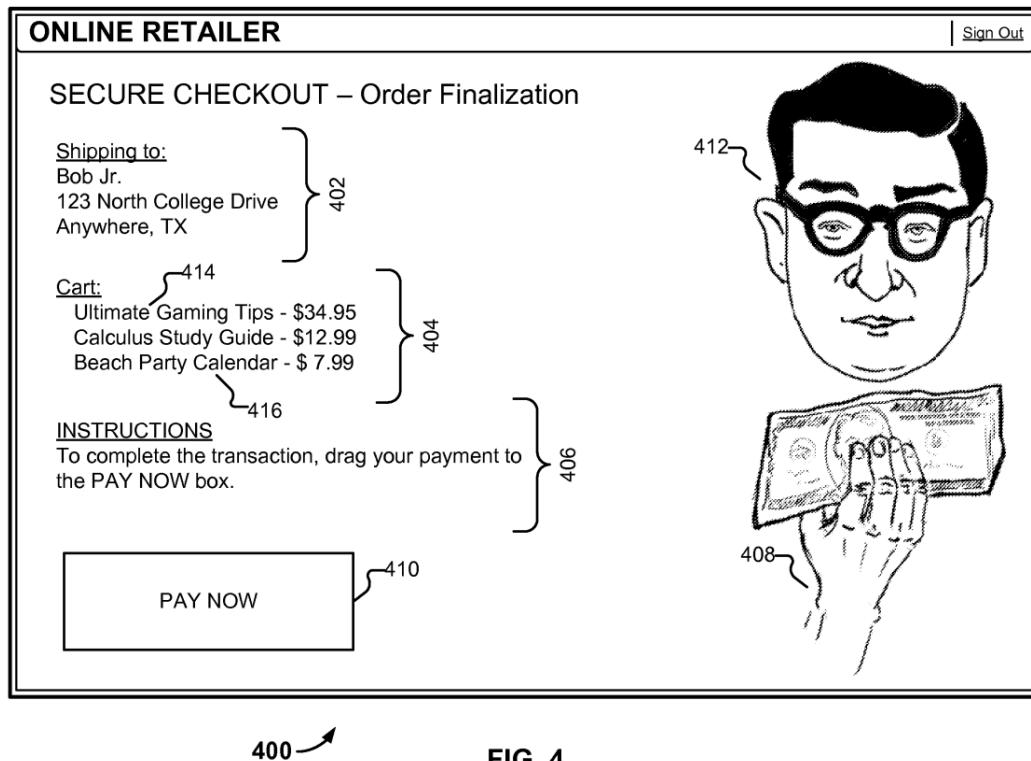


Figure 4 “illustrates an embodiment of an interface” as “rendered in a browser application of a personal computer.” Ex. 1001, 1:52, 6:29–31, Fig. 4. In particular, “Bob has specifically told Bob Jr. that it is ok for Bob Jr. to purchase schoolbooks using Bob’s account with online retailer 124” in Figure 1, and the Figure 4 interface is “shown to Bob Jr. during a checkout process.” *Id.* at 5:36–38, 6:29–32, Fig. 4.

The Figure 4 interface includes the following display elements:

- (1) region 402 showing Bob Jr.’s shipping address;
- (2) region 404 showing the contents of Bob Jr.’s shopping cart;
- (3) region 406 showing instructions for completing the transaction;

- (4) hand 408 holding money;
- (5) payment box 410 labeled “pay now”; and
- (6) an image of Bob’s face 412.

Ex. 1001, 6:37–41, 6:57–58, 11:2–3, Fig. 4.

The “amount of money held by the hand” may correspond to the “amount of money implicated by the transaction.” Ex. 1001, 10:34–36. Other transaction icons “can also be used, such as those depicting only the money” without a hand. *Id.* at 10:44–45.

As region 404 shows, “Bob Jr. has added a calculus study guide to his cart, but has also added some additional items that do not relate to his studies,” i.e., a computer game guide 414 and a calendar of beach parties 416. Ex. 1001, 6:18–20, Fig. 4.

To complete the transaction, “Bob Jr. must click on hand 408 and drag it to region 410 of the interface,” i.e., Bob Jr. must “drag[] money away from his father and present[] it as payment for the items in his cart.” Ex. 1001, 6:40–41, 6:58–60, Fig. 4. Because “Bob Jr. has included items in his cart for which his father has not authorized payment, having to drag the money away from his father may cause Bob Jr. to reconsider whether he wants to purchase items 414 and 416.” *Id.* at 6:66–7:2.

If the electronic device includes “a built-in finger scanner or other biometric equipment that allows the automatic capture of biometric information of the user performing the transaction, that biometric information can also be used for audit purposes.” Ex. 1001, 6:50–54; *see id.* at 9:24–28. “Such biometric information may be partial (e.g., the size or shape of a fingerprint) or more complete (e.g., a fingerprint).” *Id.* at 6:54–56.

The '886 patent's Figure 6 (reproduced below) depicts an interface for an electronic device:

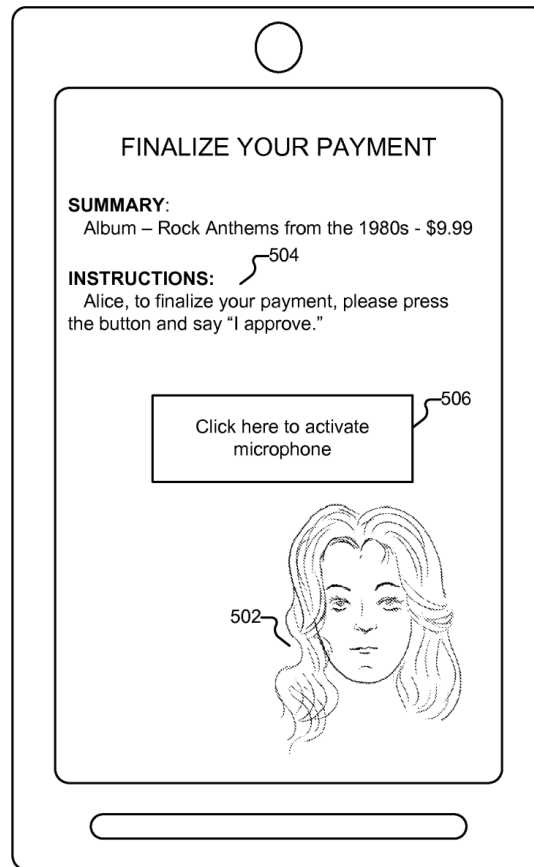


FIG. 6

Figure 6 “illustrates an embodiment of an interface” as rendered on mobile telephone 110 during a checkout process for Alice. Ex. 1001, 1:56, 7:60–63, Fig. 6. Previously, as part of an enrollment process, “Alice was asked to photograph herself, and to provide a short voice sample.” *Id.* at 7:64–66.

“As part of the checkout process, Alice is shown the image she provided at registration (502).” Ex. 1001, 7:66–8:1. The checkout process provides “instructions (504) for Alice (by name) on how to complete the transaction.” *Id.* at 8:1–3. Specifically, Alice is asked to “click on box 506 to activate the microphone 112 of device 110” and then asked to “repeat the

phrase she selected at registration,” “state a particular word or set of words appearing on the screen (such as ‘I agree’ or an arbitrary string),” or “otherwise provide an audio recording.” *Id.* at 8:3–8. “Alice’s voice is recorded after she activates the microphone of device 110 by selecting box 506.” *Id.* at 10:13–15.

In some embodiments, the newly recorded voice sample is “immediately played back to the purchaser, along with a message, such as, ‘If you would still like to proceed, press 1.’” Ex. 1001, 8:10–13. In some embodiments, the newly recorded voice sample is compared to the previously recorded voice sample to determine if the two samples sufficiently match, e.g., “as determined by a Fast Fourier Transform or other appropriate technique.” *Id.* at 8:13–18. If the two samples do not match “within some tolerance,” the newly recorded voice sample “can be stored for a period of time (e.g., in case a dispute arises), an alert can be sent to Alice, an alert can be sent to a carrier, and/or other appropriate actions can be taken.” *Id.* at 8:19–23.

As an example of fraud deterrence with the Figure 6 interface, if Alice’s daughter attempts to purchase “music on device 110 without Alice’s permission,” Alice’s daughter “may feel guilt after seeing her mother’s image, and/or will be deterred from making the purchase with the belief that her mother will be alerted that her daughter has made an unauthorized purchase.” Ex. 1001, 8:49–55.

The '886 patent's Figure 7 (reproduced below) depicts an interface for an electronic device:

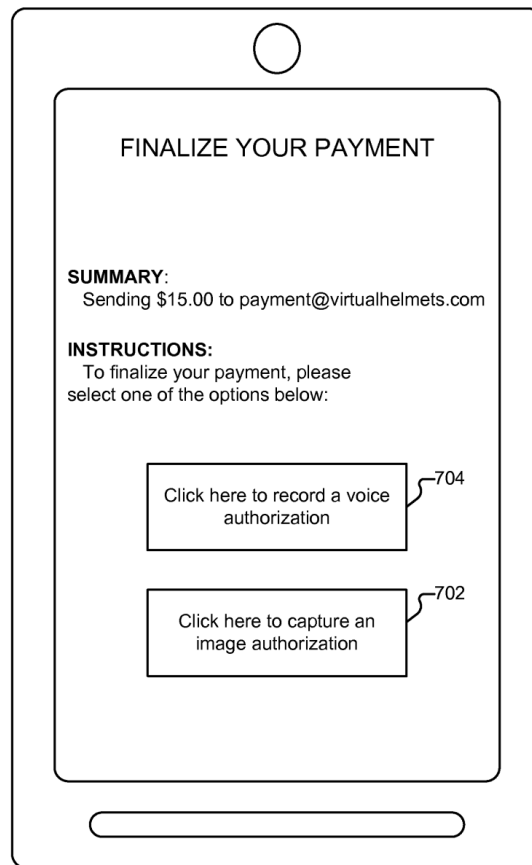


FIG. 7

Figure 7 “illustrates an embodiment of an interface” as rendered on mobile telephone 110 during a checkout process. Ex. 1001, 1:57, 8:56–58, Fig. 7.

To “complete a transaction for digital goods” with the Figure 7 interface, “the purchaser is given a choice of either providing an audio sample (by selecting box 704), or providing a photograph (by selecting box 702).” Ex. 1001, 8:58–62, Fig. 7. “If the purchaser selects box 702, the purchaser will be asked to photograph himself or otherwise provide a form of photographic authorization.” *Id.* at 8:62–64.

Techniques for “confirming that the object being photographed 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.” Ex. 1001, 8:66–9:4.

Also, a “photograph can be stored (either on the device or with a party such as a carrier or with site 120) for some period of time in case a dispute arises.” Ex. 1001, 9:13–15. In some embodiments, “no action is taken, but a fraudulent purchaser will be lead [sic] to believe that they will be caught if they engage in a fraudulent transaction.” *Id.* at 9:15–18. “Other contextual information can also be captured (or threatened to be captured) and analyzed, if applicable.” *Id.* at 9:18–20.

E. The Challenged Claims

The ’886 patent includes 23 claims. Ex. 1001, 14:2–16:38. Petitioner challenges the following claims:

- independent claim 1 for a “system”;
- claims 2–5, 12, and 14–17 that depend directly or indirectly from claim 1;
- independent claim 6 for a “method”;
- claims 7–10, 18, and 20–23 that depend directly or indirectly from claim 6; and
- independent claim 11 for a “computer program product embodied in a non-transitory computer readable storage medium.”

Pet. 5–6, 14–91.

Claim 1 exemplifies the challenged claims and reads as follows (with formatting added for clarity and with bracketed numbers added for reference purposes):¹

1. [1.0] A system, comprising:
 - [1.1] one or more processors configured to:
 - [1.2.1] render, in one or more interfaces, a virtual likeness of a face associated with an account holder,
 - [1.2.2] wherein the virtual likeness of the face was selected by the account holder as part of an enrollment;
 - [1.3.1] subsequent to an interaction by a user with an icon rendered in the one or more interfaces:
 - [1.3.1] capture contextual information comprising location data usable to determine a physical location associated with the user; and
 - [1.3.2] capture a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images; and
 - [1.4.1] facilitate a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed based at least in part on:
 - [1.4.1] the physical location associated with the user determined using the captured location data; and
 - [1.4.2] an analysis of the set of captured biometric information comprising a determination of whether the user is alive based at least in part on an analysis of the set of images captured using the camera; and

¹ We use the same reference numbers that Petitioner uses to identify the claim language. *See* Pet. vii–viii (Listing of Challenged Claims).

[1.5] a memory coupled to the one or more processors
and configured to provide the processor with instructions.

Ex. 1001, 14:2–27.

F. The Asserted References

For its challenges, Petitioner relies on the following references:

Name	Reference	Exhibit
Stone	US 2010/0042535 A1, published February 18, 2010 (based on an application filed August 15, 2008)	1008
Varghese	US 2006/0282660 A1, published December 14, 2006 (based on an application filed April 28, 2006)	1010
Hoyos	US 2010/0014720 A1, published January 21, 2010 (based on an application filed October 2, 2007)	1013
Campbell	Joseph P. Campbell, Jr., <i>Speaker Recognition: A Tutorial</i> , Proceedings of the IEEE, Vol. 85, No. 9, 1437–62 (September 1997) ²	1033
Guidance	Federal Financial Institutions Examination Council (FFIEC) Guidance, <i>Authentication in an Internet Banking Environment</i> , 1–14 (October 2005)	1037

Pet. 5–6, 14–91.

Petitioner asserts that:

- (1) Stone and Hoyos qualify as prior art “under at least §§ 102(a) and 102(e)”;
- (2) Varghese and Campbell qualify as prior art “under § 102(b)”;
- (3) the Guidance qualifies as prior art “under at least § 102(b).”

² The acronym “IEEE” stands for “Institute of Electrical and Electronics Engineers.”

Pet. 6; *see* 35 U.S.C. § 102(a), (b), (e) (2006).³

Patent Owner disputes that Stone and the Guidance qualify as prior art. *See* Resp. 15, 18–22, 40, 42–43; Sur-reply 4; Tr. 110:24–113:11. In particular, Patent Owner contends that “Stone is not analogous art.” Resp. 18–19, 40, 43; Sur-reply 4; *see* Resp. 15, 19–22; *infra* § III.D.4(c).

Regarding the Guidance, Patent Owner asserts that an ordinarily skilled artisan “exercising reasonable diligence would not have been inclined to look to” the Guidance. Resp. 42. Patent Owner does not dispute that Varghese, Hoyos, and Campbell qualify as prior art. *See, e.g.*, Resp. 14–37, 44; Sur-reply 2–23, 26.

For the reasons explained in the patentability analysis below, we determine that Stone is analogous art. *See infra* § III.D.4(d). Because we do not reach the challenges based on Stone and the Guidance, we do not address whether the Guidance is analogous art. *See infra* § III.E.

G. The Asserted Challenges to Patentability

Petitioner asserts the following challenges to patentability:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–12, 14–18, 20–23	103(a)	Stone, Hoyos, Varghese
1–12, 14–18, 20–23	103(a)	Stone, Guidance
15–17, 21–23	103(a)	Stone, Hoyos, Varghese, Campbell
15–17, 21–23	103(a)	Stone, Guidance, Campbell

³ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284 (2011), amended 35 U.S.C. § 102 and § 103 effective March 16, 2013. Because the effective filing date of the challenged claims predates the AIA’s amendments to § 102 and § 103, this decision refers to the pre-AIA versions of § 102 and § 103.

Pet. 5–6, 14–91.

H. Testimonial Evidence

To support its challenges, Petitioner relies on (1) the Declaration of Creed Jones, Ph.D. (Exhibit 1003) submitted with the Petition and (2) the Declaration of Creed Jones, Ph.D. (Exhibit 1056) submitted with the Reply. Dr. Jones states that he has “been retained by counsel for [Petitioner] as a technical expert.” Ex. 1003 ¶ 1. Dr. Jones also states that he has “a Ph.D. degree in Computer Engineering from Virginia Polytechnic Institute” and “a M.S. degree in Electrical and Computer Engineering and a B.S. degree in Electrical Engineering from Oakland University.” *Id.* ¶ 6.

To support its positions, Patent Owner relies on the Declaration of Dr. Michael T. Goodrich (Exhibit 2032). Dr. Goodrich states that he has “been retained by Patent Owner” as “an independent expert consultant in this proceeding.” Ex. 2032 ¶ 1. Dr. Goodrich also states that he obtained “a PhD in Computer Sciences from Purdue University in 1987” and “a B.A. in Mathematics and Computer Science from Calvin College, which is now known as Calvin University, in 1983.” *Id.* ¶ 7.

Additionally, Petitioner submits deposition testimony from the following:

- Dr. Jones, i.e., Exhibit 1049 (Oct. 11, 2024, Jones Dep. Tr. in IPR2024-00329, IPR2024-00330, and IPR2024-00331); and
- Dr. Goodrich, i.e., Exhibit 1050 (Jan. 7, 2025, Goodrich Dep. Tr. in IPR2024-00329, IPR2024-00330, and IPR2024-00331) and Exhibit 1053 (Jan. 8, 2025, Goodrich Dep. Tr. in IPR2024-00332 and IPR2024-00334).

I. Burden

In an *inter partes* review, a petitioner bears the burden of persuasion to prove “unpatentability by a preponderance of the evidence.” *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (quoting 35 U.S.C. § 316(e)); *see* 37 C.F.R. § 42.1(d) (2024).

III. PATENTABILITY ANALYSIS

A. Legal Principles: Obviousness

A patent may not be obtained “if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” 35 U.S.C. § 103(a) (2006). An obviousness analysis involves underlying factual inquiries including (1) the scope and content of the prior art; (2) differences between the claimed invention and the prior art; (3) the level of ordinary skill in the art; and (4) where in evidence, objective indicia of nonobviousness, such as commercial success, long-felt but unsolved needs, and failure of others.⁴ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18, 35–36 (1966); *Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1047–48 (Fed. Cir. 2016) (en banc). When evaluating a combination of references, an obviousness analysis should address “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007).

We analyze the obviousness issues according to these principles.

⁴ The parties do not address objective indicia of nonobviousness. *See, e.g.*, Pet. 14–91; Resp. 1–6, 14–44.

B. Level of Ordinary Skill in the Art

Factors pertinent to determining the level of ordinary skill in the art include (1) the educational level of the inventor; (2) the type of problems encountered in the art; (3) prior-art solutions to those problems; (4) the rapidity with which innovations are made; (5) the sophistication of the technology; and (6) the educational level of workers active in the field. *Envtl. Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696–97 (Fed. Cir. 1983). Not all factors may exist in every case, and one or more of these or other factors may predominate in a particular case. *Id.* These factors are not exhaustive, but merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007). Moreover, the prior art itself may reflect an appropriate skill level. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

Petitioner asserts that a person of ordinary skill in the art at the time of the alleged 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.” Pet. 4. Petitioner also asserts that “a person with less formal education but more experience, or more formal education but less experience, could have also met the relevant standard” for an ordinarily skilled artisan. *Id.* Dr. Jones’s testimony supports Petitioner’s assertions. *See* Ex. 1003 ¶¶ 19–20.

In the Institution Decision, we adopted Petitioner’s description of an ordinarily skilled artisan except for the language “at least” that qualifies the

experience level and allows the experience level to encompass an expert's level of skill. Inst. Dec. 21. We explained that except for the language “at least” that qualifies the experience level, “Petitioner’s description of an ordinarily skilled artisan comports with the technology and claims of the ’886 patent as well as the asserted references.” *Id.* (citing Ex. 1003 ¶ 20).

In the Response, Patent Owner notes that for “the purposes of this proceeding,” Patent Owner and Dr. Goodrich have applied the level of ordinary skill adopted by the Board in the Institution Decision. Resp. 13; *see* Ex. 2032 ¶ 27.

In the Reply, Petitioner notes that it applied the level of ordinary skill adopted by the Board in the Institution Decision and that Dr. Jones’s “analysis in the original declaration [Exhibit 1003] remains the same.” Reply 1 (citing Ex. 1056 ¶ 2).

Accordingly, for the purposes of this Final Written Decision, we apply the level of ordinary skill that we adopted in the Institution Decision. *See* Inst. Dec. 21.

C. Claim Construction

We construe claim terms “using the same claim construction standard” that district courts use to construe claim terms in civil actions for patent infringement. *See* 37 C.F.R. § 42.100(b). Under that standard, claim terms “are given their ordinary and customary meaning, which is the meaning the term would have to a person of ordinary skill in the art at the time of the invention.” *Power Integrations, Inc. v. Fairchild Semiconductor Int’l, Inc.*, 904 F.3d 965, 971 (Fed. Cir. 2018) (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc)). The meaning of claim terms may be determined by “look[ing] principally to the intrinsic evidence

of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).

Petitioner contends that “no claim term requires express construction.” Pet. 4.

Patent Owner “accepts Petitioner’s position that none of the claim terms” of the ’886 patent “require construction.” Resp. 13. Patent Owner notes that it and Dr. Goodrich have “given all claim terms their plain and ordinary meaning as understood by” an ordinarily skilled artisan “in light of the patent’s specification.” *Id.* at 13–14.

“[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.” *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999); see *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). We determine that no claim term requires an explicit construction to decide whether Petitioner has shown by a preponderance of the evidence that claims 1–12, 14–18, and 20–23 are unpatentable under § 103(a).

In the patentability analysis below, however, we address a claim-construction issue raised with respect to limitation 1.5 regarding the indefinite article “a” in the claim language “a memory.” See *infra* § III.D.6(i)(iii). We do so to provide better context to explain the issue and our resolution of the issue.

*D. Alleged Obviousness over Stone, Hoyos,
and Varghese: Claims 1–12, 14–18, and 20–23*

Petitioner contends that claims 1–12, 14–18, and 20–23 are unpatentable under § 103(a) because the claims would have been obvious over Stone, Hoyos, and Varghese. *See* Pet. 5, 14–67; Reply 2–20. Patent Owner disputes Petitioner’s contentions. *See* Resp. 14–37; Sur-reply 2–23.

Below, we provide overviews of Stone, Hoyos, and Varghese. Then, we consider the obviousness issues. For the reasons explained below, we agree with Petitioner that claims 1–12, 14–18, and 20–23 are unpatentable under § 103(a) because the claims would have been obvious over Stone, Hoyos, and Varghese.

1. OVERVIEW OF STONE (EXHIBIT 1008)

Stone is a U.S. patent application publication titled “Currency Display,” filed on August 15, 2008, and published on February 18, 2010. Ex. 1008, codes (12), (22), (43), (54). Stone states that the “invention relates to electronic visual displays, and in particular, to such displays that show a visual representation of financial instruments.” *Id.* ¶ 2; *see id.* ¶¶ 6–8, code (57).

When a user desires to transfer funds electronically, the user selects a type of currency and enters an amount into “a device with a display screen,” such as “a mobile phone, laptop computer, PDA, or personal computer.” Ex. 1008 ¶¶ 6, 16, 22; *see id.* ¶ 42. Then, the display will show the “actual currency representing the amount entered by the user” in the background of the display. *Id.* ¶¶ 6, 16, code (57). The foreground of the display may include “recipient name, amount, funding source, shipping address, etc.” *Id.* ¶ 7.

For instance, “if the user enters \$33.26 in U.S. dollars, the display will show one U.S. twenty dollar bill, one U.S. ten dollar bill, three U.S. one dollar bills, one U.S. quarter, and one U.S. penny.” Ex. 1008 ¶ 16; *see id.* ¶¶ 6, 23. “This gives the user a visual representation of the amount, which reinforces the value of the amount and provides the user with a more visually rich interface.” *Id.* ¶ 16.

The “actual currency can be based on the sender’s account, the recipient’s account, or the recipient’s selection, either real currency or personalized non-legal currency.” Ex. 1008 ¶ 8; *see id.* ¶ 39. Further, “the user may select or create his own currency for display, such as casino chips, gold bars, personalized currency with the user’s photo, etc.” *Id.* ¶ 7; *see id.* ¶¶ 19, 27–28, 39. “One example may be the user’s image or any other selected image on U.S. currency (or any other country currency).” *Id.* ¶ 28.

The recipient’s device may have “the same or similar graphics that show when funds are transferred to the recipient’s account by displaying actual currency.” Ex. 1008 ¶ 8; *see id.* ¶¶ 39, 46. For instance, the recipient’s device may show “the actual currency fading into the display, suddenly appearing on the display, moving into the display and then into an icon representing a receiving source, or any other suitable graphic or animation.” *Id.* ¶ 39.

Stone's Figure 2 (reproduced below) depicts a display on an electronic device:

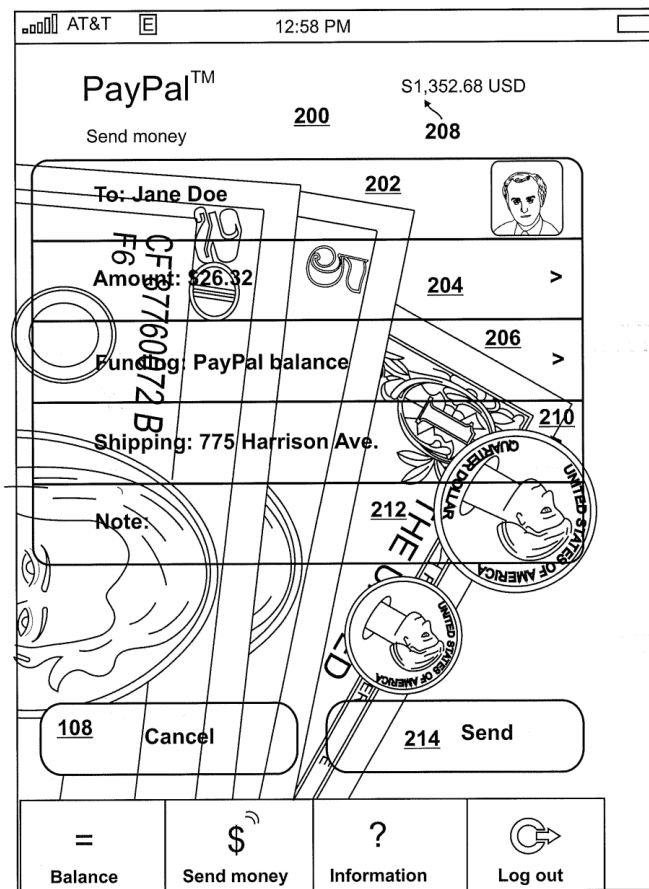


FIG. 2

Figure 2 illustrates display 200 on an electronic device including the following display elements:

- (1) name box 202 “indicating the recipient of funds”;
- (2) a “picture of the recipient” in name box 202;
- (3) funds box 204 “indicating the amount of funds to be transferred”;
- (4) funding source box 206 “indicating the source or account where the user’s funds will be transferred from”;
- (5) balance area 208 “indicating the current balance of the funding account”;

- (6) address box 210 “indicating the address of the recipient”;
- (7) “note box 212 for the user to type in any notes to the recipient”;
- (8) “send button 214 to transfer the funds [as] noted in [funds] box 204”;
- (9) “cancel button 108”;
- (10) additional buttons labeled “= Balance,” “\$ Send money,” “? Information,” and “Log out” at the bottom of the display; and
- (11) the “actual currency representing the amount entered by the user” in the background of the display.

Ex. 1008 ¶¶ 11, 16, 23–24, Fig. 2.

To transfer the funds, “the user may simply drag the currency to the other user’s icon.” Ex. 1008 ¶ 20, claim 12; *see id.* ¶ 36. Alternatively, the user may tap “an appropriate button” on the display. *Id.* ¶ 35; *see id.* ¶ 4.

After “the user decides to send the funds,” the display may indicate this with “some movement of the actual currency.” Ex. 1008 ¶ 25, Fig. 2. For example, the actual currency may “simply disappear,” “slowly fade away,” or “move off the display,” such as “a lateral movement to the right.” *Id.* ¶¶ 25, 37, Fig. 2.

Stone's Figure 3 (reproduced below) depicts a flowchart for a financial transaction:

FIG. 3

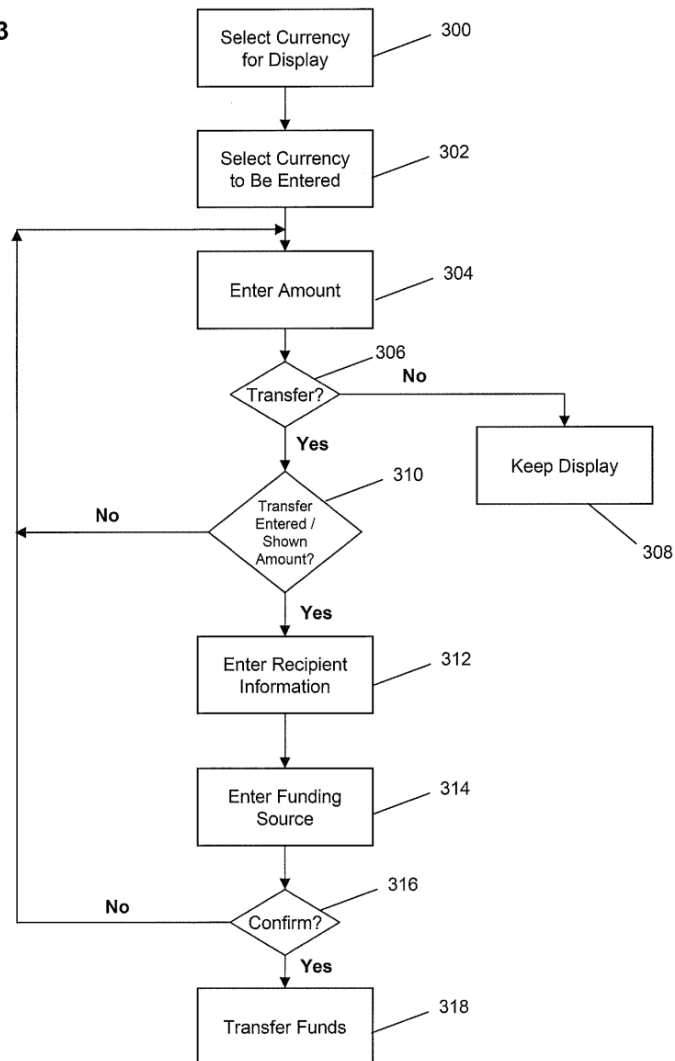


Figure 3 illustrates steps 300 through 318 for transferring funds to a recipient. *See* Ex. 1008 ¶¶ 29–35, Fig. 3.

In step 300, “the user selects the desired currency for display, such as U.S. dollar, Mexican peso, British pound, European Euro, Japanese yen, South Korean won, etc.” Ex. 1008 ¶ 29, Fig. 3. In step 302, the user selects the type of currency that “will be entered.” *Id.* ¶ 30, Fig. 3. For example, “if the user wishes to see how \$126.34 U.S. dollars in South Korean won looks

like, the user would select South Korean won in step 300 and U.S. dollars in step 302.” *Id.* ¶ 30.

In step 304, “the user enters an amount for display.” Ex. 1008 ¶ 31, Fig. 3. The “actual currency in the selected currency for that amount is then displayed.” *Id.* ¶ 31. An application “within the device or connected to the device generates the visual for the currency display.” *Id.*

In step 306, a prompt asks the user if the transaction should proceed. Ex. 1008 ¶ 32, Fig. 3. The “user may want to simply keep the display on screen to show a foreign merchant or other individual.” *Id.* ¶ 32. If so, “the currency stays on the display” in step 308. *Id.*

In step 310, a prompt asks the user to “confirm whether the shown money is what is to be transferred.” Ex. 1008 ¶ 33, Fig. 3. “One reason the user may not want to transfer that money is a realization of how much money it actually is, which may be prompted from seeing the actual currency.” *Id.* ¶ 33.

If the user decides to proceed with the transaction, the user “enters information about the recipient” in step 312, and then the user “selects a funding source” in step 314. Ex. 1008 ¶ 34, Fig. 3. Once the user “selects a funding source,” the display may show “the current balance in the funding source and any other information related to the source, such as past transactions.” *Id.* ¶ 34. After “seeing the funding source balance, the user may decide to cancel the transaction if the source does not have sufficient funds, switch the funding source to a different account, or transfer a lesser amount.” *Id.* ¶ 35.

If the user decides to proceed with the transaction, “the user confirms the transaction” in step 316. Ex. 1008 ¶ 35, Fig. 3. After “the user confirms

the transaction,” the “shown funds are transferred to the desired recipient” in step 318. *Id.* ¶ 35, Fig. 3.

Stone’s Figure 4 (reproduced below) depicts a system for financial transactions using the currency display discussed above:

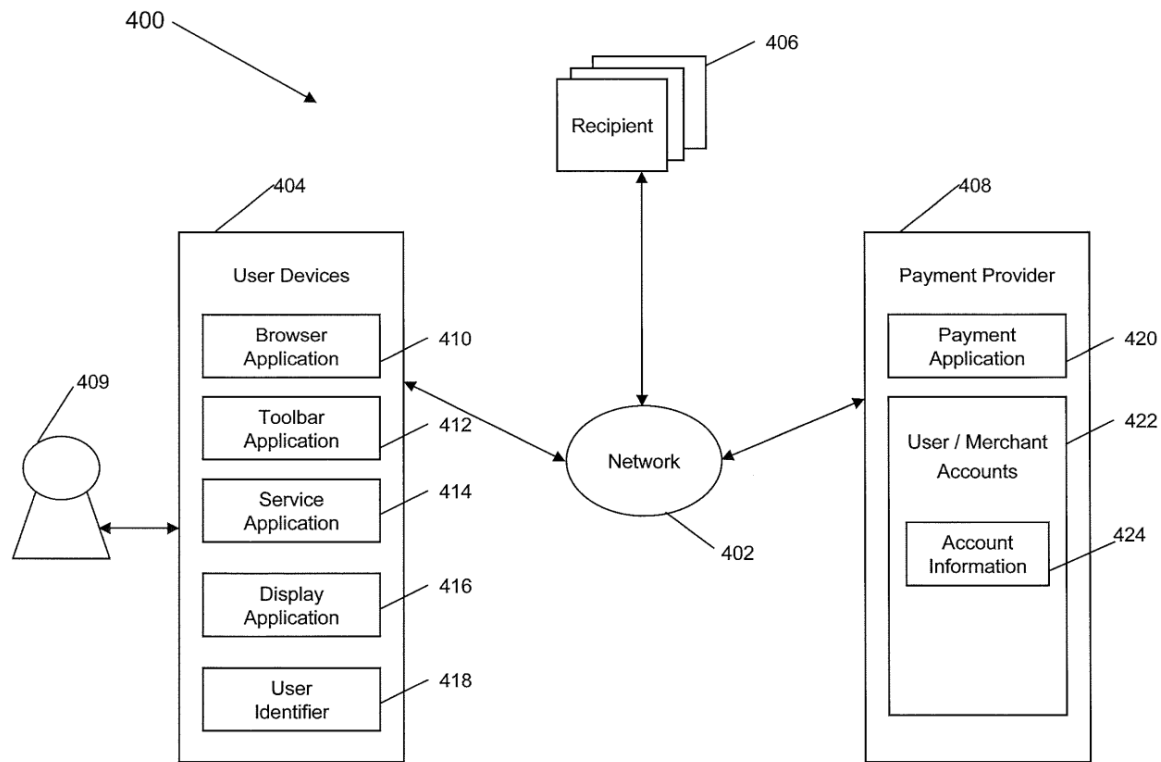


FIG. 4

Figure 4 illustrates system 400 including “at least a user device 404,” one or more recipient devices 406, and “at least one payment provider server 408” communicating “over the network 402.” Ex. 1008 ¶ 40, Fig. 4. User device 404 may comprise “a personal computer of a user 409” or “a wireless telephone (e.g., cell phone), personal digital assistant (PDA), notebook computer, and/or various other generally known types of computing devices.” *Id.* ¶ 42, Fig. 4.

User device 404 may include “any appropriate combination of hardware and/or software configured for wired and/or wireless

communication over network 402.” Ex. 1008 ¶ 42, Fig. 4. For example, a bus or other communication mechanism in user device 404 may interconnect “subsystems and components, such as a processing component,” e.g., “processor, micro-controller, digital signal processor (DSP), etc.” *Id.* ¶ 49.

User device 404 may include “one or more toolbar applications 412” that “provide client-side processing for performing tasks in response to operations selected by user 409.” Ex. 1008 ¶ 43, Fig. 4. User device 404 may also include “service application 414 for facilitating financial transactions on network 402, including money transfer.” *Id.* ¶ 44, Fig. 4. Service application 414 may include “a software program,” such as “a graphical user interface (GUI), executable by a processor that is configured to interface and communicate with the one or more recipient devices 406 and payment provider server 408 via network 402.” *Id.* ¶ 44.

User device 404 may include “one or more user identifiers 418,” such as “operating system registry entries, cookies associated with browser application 410, identifiers associated with hardware of user device 404, or various other appropriate identifiers.” Ex. 1008 ¶ 45, Fig. 4. User identifiers 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.).” *Id.* ¶ 45.

Recipient devices 406 may have “the same basic features as user device 404” and “the same or similar graphics that show when funds are transferred to the recipient’s account by displaying actual currency.” Ex. 1008 ¶¶ 8, 46; *see id.* ¶ 39.

Payment provider server 408 may include “a plurality of user and recipient accounts 422, each of which may include account information 424 associated with individual users, including user 409.” Ex. 1008 ¶ 48, Fig. 4. Account information 424 may include “private financial information of user 409 and recipients, such as one or more account numbers, passwords, credit card information, banking information, or other types of financial information” that may facilitate financial transactions “between user 409 of user device 404 and one or more recipients associated with recipient devices 406.” *Id.* ¶ 48.

Stone’s Figure 5 (reproduced below) depicts a system suitable for implementing “user device 404, one or more recipient devices 406, and payment processing device 408”:

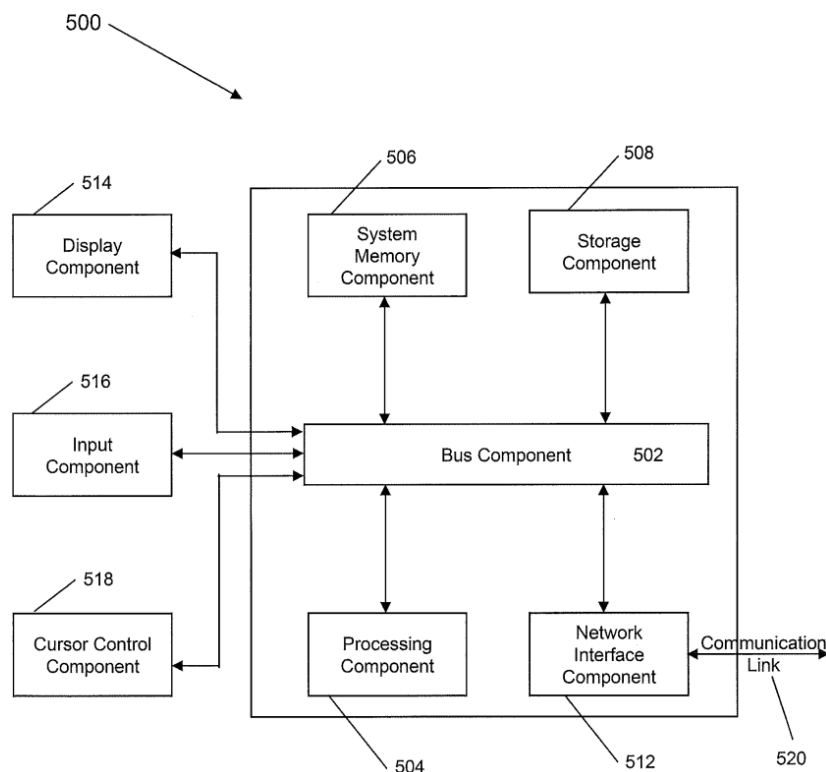


FIG. 5

Figure 5 illustrates system 500 including bus 502 that “interconnects subsystems and components,” such as the following:

- “processing component 504 (e.g., processor, micro-controller, digital signal processor (DSP), etc.)”;
- “system memory component 506 (e.g., RAM)”;
- “static storage component 508 (e.g., ROM)”;
- “network interface component 512”;
- “display component 514”;
- “input component 516 (e.g., keypad or keyboard)”;
- “cursor control component 518 (e.g., a mouse pad).”

Ex. 1008 ¶ 49, Fig. 5. System 500 may comprise “part of a cell phone, personal computer and/or a network server.” *Id.* ¶ 49.

System 500 “performs specific operations by processor 504 executing one or more sequences of one or more instructions contained in system memory component 506.” Ex. 1008 ¶ 50. The “instructions may be read into system memory component 506 from another computer readable medium, such as static storage component 508.” *Id.* The instructions may cause the processor to “create and display the proper currencies, convert currency, display various types of graphics showing transfer of currency, etc.” *Id.*

2. OVERVIEW OF HOYOS (EXHIBIT 1013)

Hoyos is a U.S. patent application publication titled “Fraud Resistant Biometric Financial Transaction System and Method,” filed on October 2, 2007, and published on January 21, 2010. Ex. 1013, codes (12), (22), (43), (54). Hoyos states that the “invention relates to biometric identification and

authentication systems and methods, more particularly to authentication for financial transactions using biometrics.” *Id.* ¶ 2; *see id.* at code (57).

Hoyos describes spoofing as a problem in conventional systems and methods for authenticating financial transactions using biometric data. *See* Ex. 1013 ¶¶ 9, 11–12. For instance, “a life-sized, high-resolution photograph of a person may be presented to” an iris-recognition system. *Id.* ¶ 11. If so, the iris-recognition system may “capture an image of this photograph” and generate a false positive identification. *Id.*

Hoyos describes inadequate analysis of “a measure of liveness” as another problem in conventional systems and methods for authenticating financial transactions using biometric data. Ex. 1013 ¶ 14; *see id.* ¶ 28. Due to this deficiency, “many valid customers are rejected.” *Id.* ¶ 15. The “rejection of a true customer has significant penalty such as a loss of a customer,” and “the substantial business consequences of a false reject [are] often not considered.” *Id.* ¶ 28.

Hoyos identifies “a need in this field of biometric authentication systems and methods for financial transactions for improved deterrent against attempted fraudulent transactions, and decreased rejection of valid customers.” Ex. 1013 ¶ 15; *see id.* ¶ 9. Hoyos endeavors to address that need by disclosing techniques for biometric authentication that:

- (1) acquire biometric data from a person;
- (2) calculate a probability called the “probability of liveness, P_p , of the person”;
- (3) calculate a probability called the “probability of a match, P_m , between the person and known biometric information”; and

- (4) provide an authentication decision, D, based on “a combination of Pp and Pm.”

Id. ¶ 17, claims 1 and 15; *see id.* ¶ 25, code (57).

Preferably, the authentication decision, D, is calculated according to the formula $D=Pp*(K+Pm)$ where “K is a number between 0.1 and 100, and in some embodiments K is a number between 0.5 and 1.5.” Ex. 1013 ¶ 17, claims 2 and 3; *see id.* ¶ 28, code (57). If the value of D exceeds a preset threshold, “the transaction is authorized.” *Id.* ¶ 33, Fig. 1. “A higher transaction may be authorized if the value of D is higher.” *Id.* ¶ 28.

The probability of liveness, Pp, may be calculated by:

- (1) “obtaining a first image of a user positioned in front of a computer screen from a first perspective”;
- (2) “obtaining a second image of the user positioned in front of the computer screen from a second perspective”;
- (3) “identifying a first portion of the first image and a second portion of the second image containing a representation of a human eye”; and
- (4) “detecting a human eye when the first portion of the first image differs from the second portion of the second image.”

Ex. 1013 ¶ 20, claim 7; *see id.* ¶¶ 34–37, Figs. 2–4.

Alternatively, the probability of liveness, Pp, may be calculated by “measuring finger or palm temperature and comparing the resultant measured temperature to [the] expected temperature for a human.” Ex. 1013 ¶ 21, claim 9.

The probability of a match, Pm, may be calculated “in any way which is desired.” Ex. 1013 ¶ 22. The methods for calculating the probability of a match, Pm, include “iris recognition, fingerprint image recognition, finger

vein image recognition, or palm vein image recognition, face recognition, [and] token match.” *Id.* ¶ 22, claim 10; *see id.* ¶ 12.

Hoyos’s Figure 2 (reproduced below) depicts an example system and method for acquiring biometric data from a person:

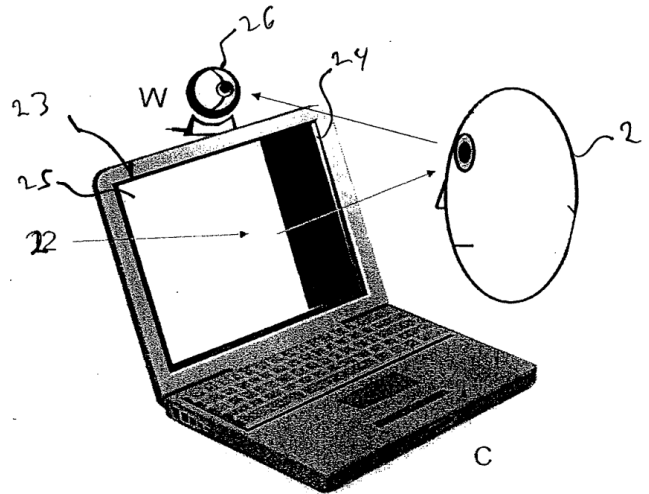


Fig. 2

Figure 2 illustrates a person 21 positioned in front of a personal computer with screen 23 and web-camera 26. Ex. 1013 ¶ 34, Fig. 2.

Initially, screen 23 displays an image with black bar 24 on the right and white area 25 on the left, and web-camera 26 obtains a first image of the person. Ex. 1013 ¶ 34, Fig. 2. Subsequently, screen 23 displays an image with black bar 24 on the left and white area 25 on the right, and web-camera 26 obtains a second image of the person. *Id.* ¶ 34. A comparison of the eye region in each image provides the probability of liveness, P_p . *See id.* ¶¶ 35–37, Figs. 3–4.

By combining the two probabilities P_p and P_m to make a decision in a transaction, “the reject rate of true authentications can be designed to be greatly

reduced.” Ex. 1013 ¶ 26. With the threshold for D set appropriately, “the transaction will be authorized even though the biometric match is not high.” *Id.* ¶ 28; *see id.* ¶ 39.

By combining the two probabilities P_p and P_m to make a decision in a transaction, “an attempted fraudster is never sure whether a transaction was authorized or not authorized because they were matched or not matched, or because they were or were not detected as a real person.” Ex. 1013 ¶ 27; *see id.* ¶ 29. In particular, “if a person fails or passes authentication, the person is not informed as to whether non-authentication or authentication was based on probability of liveness or probability of matching.” *Id.* ¶ 24.

Withholding pass/fail information (1) “eliminates the clear feedback that criminals are provided today that they use to develop new methods to defeat systems” and (2) “makes it much more difficult for an attempted fraudster to refine their fraudulent methods since they are not being provided clear feedback.” Ex. 1013 ¶¶ 24, 27; *see id.* ¶ 29. The “fraudulent user will have to present some live-person data,” and “they will not know how much or how little live-person data is required to incriminate themselves.” *Id.* ¶ 29.

Hence, Hoyos’s techniques provide “an enormous deterrent to criminals since the system is acquiring biometric data that they have no idea can or cannot be used successfully as evidence against them.” Ex. 1013 ¶ 27; *see id.* ¶ 29. Even if “there is a small probability that evidence can be used against them,” that “is sufficient for many criminals to not perform fraud, in consideration of the consequences of the charges and the damning evidence of biometric data (such as a picture of a face tied to a transaction).” *Id.* ¶ 27.

Hoyos's techniques also provide "a means to perform customer redress" by ensuring that "some live-person data is captured." Ex. 1013 ¶ 29. As an example, "if a customer complains then the system can show the customer a picture of them performing a transaction." *Id.* As another example, "a bank agent can manually look at the picture of the user performing the transaction and compare it with a record of the user on file." *Id.*

3. OVERVIEW OF VARGHESE (EXHIBIT 1010)

Varghese is a U.S. patent application publication titled "System and Method for Fraud Monitoring, Detection, and Tiered User Authentication," filed on April 28, 2006, and published on December 14, 2006. Ex. 1010, codes (12), (22), (43), (54). Varghese states that the "invention relates generally to systems and methods for providing protection against identity theft over a computer network." *Id.* ¶ 2; *see id.* at code (57).

Varghese identifies deficiencies in conventional security measures for electronic financial transactions. *See* Ex. 1010 ¶¶ 7–13. For instance, "certain geographic locations are known to contain an inordinate number of identity thieves." *Id.* ¶ 12. "IP addresses are one readily available source of location information," e.g., for identifying suspicious geographic locations. *Id.* But an electronic device's IP address may vary because, for example, a server assigns IP addresses dynamically, e.g., "each time a new message is sent." *Id.* ¶¶ 12–13.

Varghese states that "currently lacking in the art is a security system and method" that:

- (1) "is a device-based fraud monitoring system";

- (2) “provides robust fraud monitoring and detection along with robust fraud analysis and risk assessment so that online service providers have real time information needed to determine how and whether to allow a device to access the provider’s system”;
- (3) “provides selectable levels of secure user authentication as a function of usability and/or security concerns”;
- (4) “is a purely software based solution to identity theft that does not require hardware devices to be issued and maintained”; and
- (5) “is convenient for online users.”

Ex. 1010 ¶¶ 16–19, 22–23.

Varghese endeavors to address those needs by providing security systems and methods with “improved authentication services.” Ex. 1010 ¶ 24; *see id.* ¶¶ 25–30. The security systems and methods employ multiple authentication levels. *See, e.g., id.* ¶¶ 31–32, 39, 78–79, 84, 91, 150, 159, Fig. 14. In some embodiments, the invention:

- (1) initially authenticates “a user and a login request” (called “pre-authentication”) based on (a) “the identity of the device from which the authentication request originates” and (b) “available information concerning the identity of the requesting user”; and
- (2) subsequently authenticates user “workflow sequences” or “transaction sequences” (called “post-authentication”) based on “a user’s transaction history.”

Id. ¶ 65. “Preferred pre-authentication criteria include location information and device information, and preferred post-authentication criteria include user information and workflow information.” *Id.* ¶ 90; *see id.* ¶ 96.

Varghese’s security systems and methods analyze a number of fraud-detection inputs containing information about “the user, the user’s device,

the location of the user's device, the workflow of transaction entered by the user, historical patterns of user accesses,” and “data from 3rd party data sources.” Ex. 1010 ¶ 88; *see id.* ¶¶ 85, 90. The fraud-detection inputs are processed to produce “risk scores, risk alerts, and actions (or action recommendations).” *Id.* ¶ 88. For instance, the fraud-detection inputs are “weighted and analyzed in real time” using customizable analytic processes to produce risk scores indicating “the likely risks that the current request is incorrect, or malicious, or fraudulent.” *Id.*

Additionally, transaction authorization may require “login/password credentials (‘something you know’)” followed by analysis of the “user’s computer and location (‘something you have’) along with behavioral usage patterns on a site to confirm identity (‘something you are’).” Ex. 1010 ¶ 35. These multiple authentication levels provide “strong additional layers of anti-fraud protection.” *Id.*

Varghese’s Figure 14 (reproduced below) depicts an “exemplary functional configuration”:

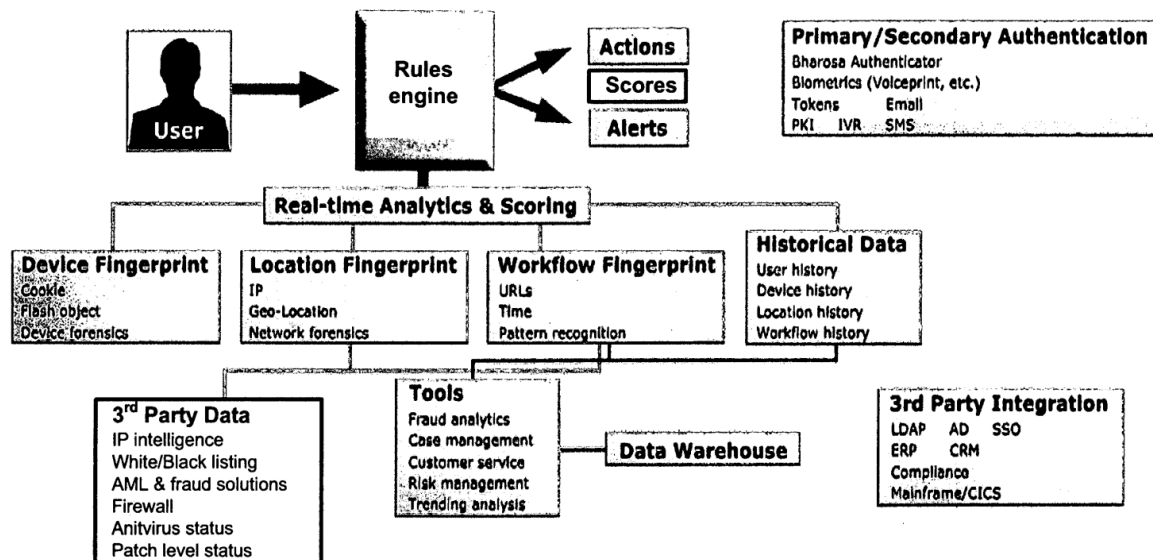


FIG. 14

Figure 14 illustrates “Real-time Analytics & Scoring” for authenticating a user transaction request where the request’s attributes have been “packaged into fingerprints” that are “processed and scored in real-time” by a rules engine to “generate actions, alerts, and scores.” Ex. 1010 ¶¶ 91, 97, Fig. 14. The fingerprints include “a location fingerprint, a device fingerprint, a workflow fingerprint, and an historical data fingerprint.” *Id.* ¶ 91, Fig. 14.

Figure 14 shows the following fingerprints from left to right:

- (1) “Device Fingerprint” including “Cookie, Flash object, Device forensics”;
- (2) “Location Fingerprint” including “IP, Geo-Location, Network forensics”;
- (3) “Workflow Fingerprint” including “URLs, Time, Pattern recognition”; and
- (4) “Historical Data” including “User history, Device history, Location history, Workflow history.”

Ex. 1010, Fig. 14.

The actions resulting from the real-time analytics and scoring include primary authentication and secondary authentication. Ex. 1010 ¶ 91.

Figure 14 shows “Primary/Secondary Authentication” including “Biometrics (Voiceprint, etc.), Tokens, Email, PKI, IVR, SMS.”⁵ *Id.* Fig. 14.

Secondary authentication “can be invoked during a session if authentication confirmation or further authentication is needed.” Ex. 1010 ¶ 91. For instance, “a bank or other financial institution may wish to invoke

⁵ The acronym “PKI” stands for “public key infrastructure.” The acronym “IVR” stands for “interactive voice response.” The acronym “SMS” stands for “short message service.”

a higher security authentication” before permitting “transactions over a certain amount.” *Id.* ¶ 148; *see id.* ¶ 142.

Location “can most easily be estimated from the device’s IP address and the hierarchy of networks linking the device to the Internet.” Ex. 1010 ¶ 93. “Geolocation by IP address is a technique of determining the geographic latitude and longitude corresponding to a user by comparing the user’s IP address with known locations of other nearby servers and routers.” *Id.* ¶ 140.

Varghese explains that “real-time risk scoring” depends on, among other things, location data. Ex. 1010 ¶¶ 77, 88, 109, 140, 142, claim 31 (reciting an “access policy” based on “risks related to the current location of the user device” and “risk related to the current transaction”). Varghese’s analytics-and-scoring system may collect location data from “geolocation data services providing [the] likely geographical source of the current request” during “the course of a valid already-authenticated session.” *Id.* ¶¶ 77, 142, 148, claim 14 (reciting “a device geolocation data provider”). For instance, a user transaction request that involves “an amount of money over a certain threshold” or “large amounts of money” (“a high-value transaction”) may “invoke a higher security authentication.” *Id.* ¶¶ 74–75, 142, 148.

Varghese also explains that transaction rules may “evaluate parameters of individual in-session transactions for the likelihood of fraud or malicious intent.” Ex. 1010 ¶ 109. Varghese discloses model rules including the following:

- (1) “Money transfer request of a certain dollar amount by a user who is logged in from another country”; and

- (2) “Transaction from an un-registered device/location or frequently used fraud device/location.”

Id. ¶ 110.

4. WHETHER STONE IS ANALOGOUS ART

(a) General Principles

“A reference qualifies as prior art for an obviousness determination only when it is analogous to the claimed invention.” *Airbus S.A.S. v. Firepass Corp.*, 941 F.3d 1374, 1379 (Fed. Cir. 2019). According to the Federal Circuit, the Supreme Court’s *KSR* decision “directs us to construe the scope of analogous art broadly, stating that ‘*familiar items may have obvious uses beyond their primary purposes*, and a person of ordinary skill often will be able to fit the teachings of multiple patents together like pieces of a puzzle.’” *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1238 (Fed. Cir. 2010) (emphasis by the court) (quoting *KSR*, 550 U.S. at 402). In an *inter partes* review, the petitioner bears the burden of establishing that a reference is analogous art. See *Sanofi-Aventis Deutschland GmbH v. Mylan Pharms. Inc.*, 66 F.4th 1373, 1377 (Fed. Cir. 2023).

The scope of analogous art includes references “from the same field of endeavor” and references “reasonably pertinent to the particular problem with which the inventor is involved.” *In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004); see *In re Wood*, 599 F.2d 1032, 1036 (CCPA 1979).

When evaluating the field of endeavor, a “factfinder must consider each reference’s disclosure in view of the ‘the reality of the circumstances,’ and ‘weigh those circumstances from the vantage point of the common sense likely to be exerted by one of ordinary skill in the art in assessing the scope of the endeavor.’” *Airbus*, 941 F.3d at 1380 (citations omitted) (quoting

Bigio, 381 F.3d at 1326); *see id.* at 1381. Hence, a field-of-end endeavor analysis should consider a patent’s claims and written description. *See id.* at 1380–81.

A “reasonably pertinent” reference “logically would have commended itself to an inventor’s attention in considering” a problem facing the inventor. *In re Clay*, 966 F.2d 656, 659 (Fed. Cir. 1992). When determining whether a reference is “reasonably pertinent,” a “factfinder should consider record evidence cited by the parties to demonstrate the knowledge and perspective of a person of ordinary skill in the art at the time of the invention.” *Airbus*, 941 F.3d at 1383; *see id.* at 1383–84.

(b) Petitioner’s Contentions

Petitioner contends that Stone is “analogous art to the ’886 patent” because Stone is at least (1) “in the same field of endeavor,” i.e., “electronic financial transactions,” or (2) “reasonably pertinent to a problem with which the inventor of the ’886 patent was involved,” e.g., “fraud detection in electronic financial transactions.” Pet. 13 (citing Ex. 1003 ¶ 58); *see id.* at 6–7; Reply 5.

Regarding “the same field of endeavor,” Petitioner asserts that Stone is “concerned with electronic transactions including fraud prevention for electronic transactions” and therefore in “the same field of endeavor” as the ’886 patent. Reply 5. Petitioner explains that:

- (1) Stone’s Figure 2 illustrates “a user logged in ‘PayPal’ with a balance displayed”; and
- (2) PayPal was “a widely used online payment platform allowing users to send and receive money and transfer funds between bank accounts or credit cards.”

Id. (citing Ex. 1008, Fig. 2; Ex. 1056 ¶ 9).

Additionally, Petitioner contends that Stone “expressly discloses that it is concerned with the processing of electronic transactions including fraud detection, and merely omits details of how funds are transferred that were well-known in the art.” Reply 4 (citing Ex. 1056 ¶ 7).

Further, Petitioner asserts that Stone “discloses secure transactions with multi-factor authentication (e.g., ‘username, password,’ ‘biometric id,’ and/or banking ‘user account numbers, security information’) for fraud prevention.” Prelim. Reply 3 (emphases omitted) (quoting Ex. 1008 ¶ 45) (citing Ex. 1008 ¶ 46, Fig. 2); *see* Reply 2–3 (citing Ex. 1008 ¶ 45).

According to Petitioner, Patent Owner “does not dispute” that “it was well-known” that (1) “ID/password is used for authentication for electronic transactions” and (2) “biometric identifiers are most commonly used as part of a multifactor authentication system” for electronic transactions. Reply 3.

Regarding “reasonably pertinent to the particular problem with which the inventor is involved,” Petitioner asserts that Stone is “reasonably pertinent” to “the particular problem of making an electronic financial transaction seem ‘more concrete’ because ‘physical cash is a concrete, tangible item while a digital payment for a digital good is a more abstract concept.’” Reply 5 (quoting Ex. 1001, 4:28–30, 5:17–18) (citing Ex. 1001, 4:28–30, 4:62–67, 5:16–18; Ex. 1003 ¶ 122; Ex. 1008, Figs. 1–2; Ex. 1056 ¶ 10).

As examples of “reasonably pertinent” references, Petitioner asserts that:

- (1) the Examiner cited “user interface art,” e.g., Gaw and Fujioka,⁶ during the prosecution of an ancestor of the ’886 patent, i.e., U.S. Patent No. 9,972,010 B1; and
- (2) the ’886 patent lists additional “user interface art” in the References Cited section.

Prelim. Reply 4–5 (citing Ex. 1007, 87).

(c) Patent Owner’s Contentions

Patent Owner contends that “Stone is not analogous art.” Resp. 18–19, 40, 43; Sur-reply 4; *see* Resp. 15, 19–22. In particular, regarding the “field of endeavor,” Patent Owner asserts that “the claimed invention relates to improved techniques to prevent and detect fraud, particularly within electronic transactions.” Resp. 20. Patent Owner asserts that the claims are “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.” *Id.* at 20–21.

Additionally, Patent Owner contends that Stone:

- (1) “never discusses fraud”;
- (2) “never discusses any techniques for countering fraud”;
- (3) “is not directed to improved techniques to prevent and detect fraud within electronic transactions”;
- (4) “is not concerned with electronic payment fraud or how to deter it”;

⁶ *See* U.S. Patent No. 7,930,220 B1, to Derek Gaw (“Gaw”), titled “Method, Medium, and System for Associating Graphical Icons with Destination Addresses Using Drag and Drop,” and issued on April 19, 2011; and U.S. Patent Application Publication No. 2009/0288015 A1, to Robb Fujioka (“Fujioka”), titled “Widgetized Avatar and a Method and System of Creating and Using Same,” and published on November 19, 2009.

- (5) “is only concerned with providing an improved currency display”; and
- (6) has a “primary goal” of providing a “more visually rich interface.”

Resp. 7, 21 (quoting Ex. 1008 ¶ 16); Sur-reply 4. According to Patent Owner, Stone’s discussion of financial transactions “is tangential to Stone’s primary purpose—improving a user display.” Resp. 21.

Regarding “reasonably pertinent to the particular problem with which the inventor is involved,” Patent Owner asserts that Stone “is not pertinent to the problem that the ’886 Patent is concerned with solving—electronic payment fraud.” Resp. 21. Patent Owner identifies “the problem facing the inventor” as “fraud detection.” Sur-reply 4. Patent Owner also asserts that Stone “is not concerned with payment processing and does not even recognize payment fraud as a problem needing to be solved.” Resp. 22.

(d) Analysis

For the reasons explained below, we agree with Petitioner that Stone is analogous art. *See* Pet. 13; Prelim. Reply 4–5; Reply 5. In particular, Stone is at least “reasonably pertinent to the particular problem with which the inventor is involved.” *See* Ex. 1001, 4:28–30, 4:62–67, 5:16–18; Ex. 1003 ¶¶ 53, 122; Ex. 1008 ¶¶ 6, 8, 16, 22–25, 31, 33, 39, code (57), Figs. 1–2; Ex. 1056 ¶ 10; Inst. Dec. 41–42; *Bigio*, 381 F.3d at 1325.

The ’886 patent explains that a “\$20 bill, when held in a person’s hand and presented to a merchant, is a tangible item with a concrete value,” but when “the same amount of money is involved in an electronic transaction . . . the amount of money involved may seem less concrete.” Ex. 1001, 5:6–11. Thus, among other things, the inventor faced the problem of making an electronic financial transaction seem “more concrete” because

“physical cash is a concrete, tangible item while a digital payment for a digital good is a more abstract concept.” *Id.* at 4:39–41, 5:4–6, 5:27–29; *see* Ex. 1056 ¶ 10; Inst. Dec. 41.

Stone addresses the problem of making an electronic financial transaction seem “more concrete” by disclosing an electronic device with a display screen that shows the “actual currency” for an electronic financial transaction. Ex. 1008 ¶¶ 6, 8, 10–11, 16, 22–25, 31, 33, 39, code (57), Figs. 1–2; *see* Ex. 1003 ¶ 162; Ex. 1056 ¶ 10; Inst. Dec. 41. Stone explains that “[t]his gives the user a visual representation of the amount, which reinforces the value of the amount and provides the user with a more visually rich interface.” Ex. 1008 ¶ 16; *see* Ex. 1003 ¶ 40.

Also, as Petitioner asserts, the Examiner cited “user interface art” during the ’886 patent’s prosecution and the prosecution of the patent’s ancestors. Ex. 1002, 97, 196, 199; Ex. 1006, 22; Ex. 1007, 87–91, 94, 146–58, 161, 290, 292, 342–50, 353, 454; Ex. 1030, 105, 107–08; *see* Ex. 1001, code (56); Prelim. Reply 4–5. Consistent with this, the patent’s Figure 4 “illustrates an embodiment of an interface,” the patent’s Figure 6 “illustrates an embodiment of an interface,” and the patent’s Figure 7 “illustrates an embodiment of an interface.” Ex. 1001, 1:52, 1:56–57, 6:29–32, 7:60–63, 8:56–58, Figs. 4, 6–7. Stone’s Figures 1 and 2 also illustrate embodiments of an interface, in particular, embodiments that show the “actual currency” for an electronic financial transaction. Ex. 1008 ¶¶ 10–11, 22–25, code (57), Figs. 1–2; *see* Inst. Dec. 41–42.

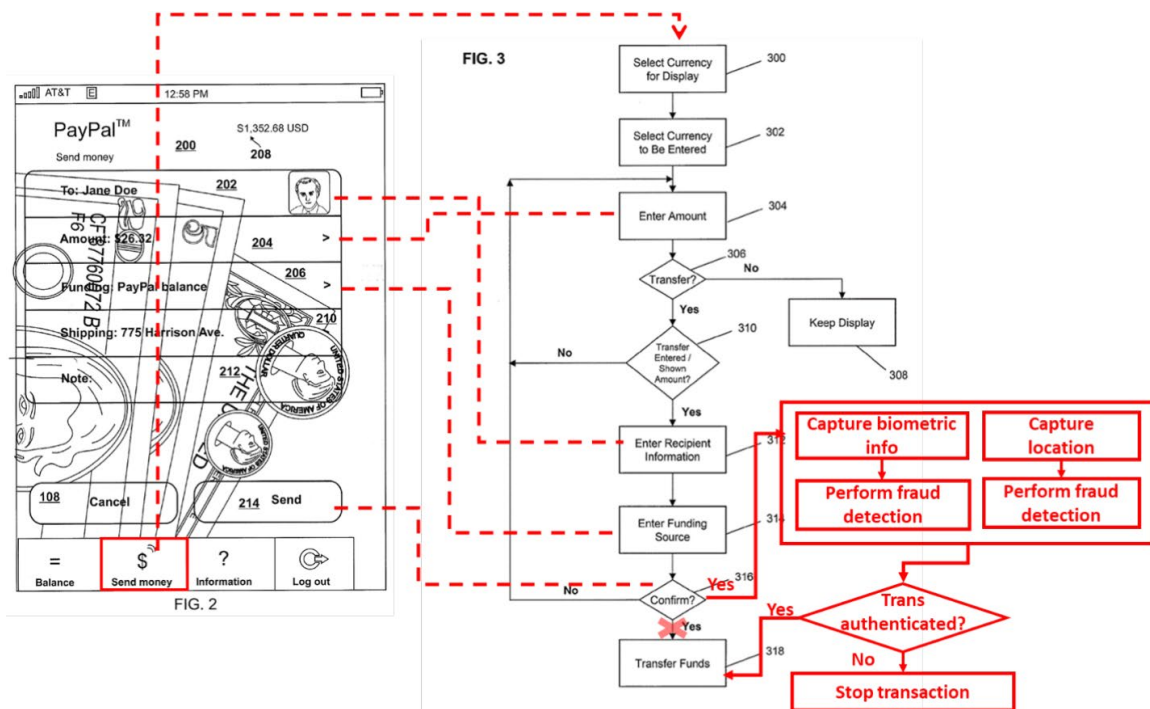
For the reasons discussed above, a preponderance of the evidence establishes that Stone is at least “reasonably pertinent” analogous art, and Patent Owner’s contentions to the contrary lack merit.

5. WHETHER AN ORDINARILY SKILLED ARTISAN WOULD
HAVE BEEN MOTIVATED TO COMBINE THE TEACHINGS OF
THE REFERENCES WITH A REASONABLE EXPECTATION OF SUCCESS

(a) Petitioner's Contentions

(i) Motivation to Combine: The Proposed Combination

To show the proposed combination, Petitioner provides the following annotated version of Stone's Figure 2 combined with Stone's Figure 3 together with additional steps according to Hoyos and Varghese (Pet. 22):



The above illustration includes Stone's Figure 2 showing display 200 on an electronic device, Stone's Figure 3 showing steps 300 through 318 for transferring funds to a recipient, and the following annotations in red:

- (1) a dashed line from the "\$ Send money" button in Figure 2 to step 300 for "Select Currency for Display" in Figure 3;
- (2) a dashed line from name box 202 in Figure 2 to step 312 for "Enter Recipient Information" in Figure 3;

- (3) a dashed line from funds box 204 in Figure 2 to step 304 for “Enter Amount” in Figure 3;
- (4) a dashed line from funding source box 206 in Figure 2 to step 314 for “Enter Funding Source” in Figure 3;
- (5) a dashed line from the “Send” button 214 in Figure 2 to step 316 for “Confirm?” in Figure 3; and
- (6) additional steps after a “Yes” determination in step 316 for “Confirm?” as follows: (i) “Capture biometric info” followed by “Perform fraud detection”; (ii) “Capture location” followed by “Perform fraud detection”; (iii) “Trans authenticated?”; and (iv) “Stop transaction.”

Pet. 22; *see* Ex. 1003 ¶ 68; Ex. 1008 ¶¶ 11–12, 16, 23–24, 29–35, Figs. 2–3.

(ii) Motivation to Combine: Combining the Teachings of Stone and Hoyos

Petitioner contends that an ordinarily skilled artisan “would have been motivated to combine disclosures or embodiments of Stone, e.g., FIG. 2 and 3, to provide a transaction system using user interfaces (e.g., as taught by FIG. 2) for performing an electronic transaction (e.g., as taught by FIG. 3).” Pet. 14. As support, Petitioner quotes the following statement in *Boston Scientific Scimed, Inc. v. Cordis Corp.*, 554 F.3d 982, 991 (Fed. Cir. 2009): “Combining two embodiments disclosed adjacent to each other in a prior art patent does not require a leap of inventiveness.” Pet. 14. Petitioner explains that various “user actions in FIG. 2 correspond to the steps of FIG. 3, e.g., elements 202, 204, 206, and 214 correspond respectively to elements 312, 304, 314, and 316.” *Id.* at 15.

Further, Petitioner asserts that “it was well-known that financial transaction systems of Stone had a need for authentication for fraud detection (e.g., with higher levels of security for higher-risk transactions).” Pet. 16 (citing Ex. 1003 ¶ 66; Ex. 1010 ¶ 148; Ex. 1013 ¶¶ 9, 11; Ex. 1016

¶ 73, Fig. 3; Ex. 1022, 1; Ex. 1037, 1). According to Petitioner, “regulatory mandates” applied “pressure to proactively detect and prevent fraud.” *Id.* (quoting Ex. 1022, 1).

Additionally, Petitioner contends that an ordinarily skilled artisan would have been motivated to combine Hoyos’s biometric authentication with Stone’s system for financial transactions to obtain the benefits of “improved fraud resistancy by addressing spoofing,” “improved deterren[ce] against attempted fraudulent transactions,” and “decreased rejection of valid customers” as taught by Hoyos. Pet. 16–17 (quoting Ex. 1013 ¶ 15) (citing Ex. 1003 ¶¶ 64–73; Ex. 1013 ¶¶ 17–22); *see id.* at 44, 52–53 (quoting Ex. 1013 ¶ 15).

According to Petitioner, using Hoyos’s biometric authentication in Stone’s system for financial transactions would have achieved various advantages including:

- (1) “spoofing prevention”;
- (2) “reducing iterative attacks by eliminating clear feedback,” thus “making it much more difficult for an attempted fraudster to refine fraudulent methods”;
- (3) “greatly reducing ‘the reject rate of true authentications’”;
- (4) “providing ‘an enormous deterrent to criminals’”; and
- (5) “providing ‘a means to perform customer redress’” by ensuring that “some live-person data is captured.”

Pet. 17, 45 (quoting Ex. 1013 ¶¶ 24, 26–27, 29); *see* Reply 4 (citing Ex. 1013 ¶¶ 24, 26–27, 29). Petitioner asserts that “Hoyos itself provides express advantages that would have motivated” an ordinarily skilled artisan to “incorporate Hoyos’ biometric authentication teachings in Stone.” Reply 4 (citing Ex. 1056 ¶ 8).

Petitioner explains that in the proposed combination biometric authentication according to Hoyos would occur after a user confirms a transaction request, i.e., after (1) user interaction with an icon to initiate a transaction, such as a user actuating the “\$ Send money” button in Stone’s display, and (2) user interactions with additional icons in Stone’s display to continue the transaction and confirm the transaction request. Pet. 18–19, 46 (citing Ex. 1003 ¶¶ 69, 129); *see id.* at 40.

Petitioner asserts that an ordinarily skilled artisan would have understood that performing Hoyos’s biometric authentication “after and in response to user transaction request confirmation had various benefits over the alternative design choice of using only previously captured input data before user transaction request confirmation.” Pet. 18–19. According to Petitioner, those “various benefits” include:

- (1) “improved fraud detection and security” from “capturing real-time, more accurate data that leads to more accurate and improved fraud detection and security”;
- (2) “improved fraud detection” due to “risk-based contextual authentication (e.g., specific authentication level requiring specific types of contextual data to capture) based on the specific transaction and assessed risk thereof”;
- (3) “avoiding imposters from communicating based on stolen biometric data,” and
- (4) “reducing spoofing.”

Id. at 19–20, 46 (citing Ex. 1003 ¶¶ 70, 130; Ex. 1010 ¶¶ 97–99, 110 (Table 10), Fig. 14; Ex. 1012 ¶ 28; Ex. 1015, Fig. 4).

As an example of “risk-based contextual authentication,” Petitioner explains that “a large transaction amount would typically be considered

higher risk than a small transaction amount” and would warrant risk assessment after the transaction’s details are “finalized/confirmed by the user’s indication of action taken.” Pet. 19–20.

Petitioner asserts that Stone’s system based on a client-server model and Hoyos’s biometric authentication are complementary. Reply 6. Petitioner also asserts that an ordinarily skilled artisan would have adapted or applied Hoyos’s biometric authentication to “function within Stone’s system (either on the client or on a server), achieving secure authentication without undermining the system’s architecture.” *Id.* at 6–8 (citing Ex. 1003 ¶¶ 71–73; Ex. 1056 ¶¶ 11–16; Pet. 20).

As support, Petitioner quotes the following statements in a 2005 paper titled “Secure Biometric Authentication for Weak Computational Devices” and co-authored by Dr. Goodrich: “There are two broad approaches: The one where the comparison is done at the remote server, and the one where the comparison is done at the client end (the portable device where the biometric measurement is done). Most of the recent work has focused on the second category” Reply 6–7 (emphases omitted) (quoting Ex. 1055, 2); *see* Ex. 1055, 2; Ex. 2031, 16.

(iii) Motivation to Combine: Combining the Teachings of Varghese with the Teachings of Stone and Hoyos

Petitioner contends that an ordinarily skilled artisan would have been motivated to combine Varghese’s “real-time multifactor authentication” including “location authentication combined with biometrics (e.g., voice, fingerprints, retinal scans, etc.)” with the Stone-Hoyos system to provide “improved security for financial transactions.” Pet. 21 (citing Ex. 1003

¶¶ 74–84; Ex. 1010 ¶ 79); *see id.* at 36–39, 49. According to Petitioner, an ordinarily skilled artisan would have understood that:

- (1) real-time authentication “as described in Varghese includes both real-time capture and real-time analysis of input authentication data for transaction authentication”;
- (2) real-time authentication provides “more accurate fraud analysis by using more accurate, real-time input data”; and
- (3) multifactor authentication, e.g., “location authentication combined with biometrics),” provides “additional security for financial transactions, as taught in Varghese.”

Id. at 21, 36–37 (citing Ex. 1003 ¶¶ 77, 114; Ex. 1016 ¶¶ 43–44; Ex. 1035, 4:60–62, 4:66–67); *see id.* at 49.

Petitioner explains that in the proposed combination “real-time multifactor authentication” according to Varghese would occur after a user confirms a transaction request, i.e., after (1) user interaction with an icon to initiate a transaction, such as a user actuating the “\$ Send money” button in Stone’s display, and (2) user interactions with additional icons in Stone’s display to continue the transaction and confirm the transaction request.

Pet. 22, 38–40 (citing Ex. 1003 ¶¶ 79–81, 118; Ex. 1010 ¶¶ 91, 97–99, 110 (Table 10), 148, Fig. 14; Ex. 1013 ¶ 28; Ex. 1015, Fig. 4; Ex. 1016 ¶¶ 36, 43, 73, Fig. 3; Ex. 1035, 4:60–62, 4:66–67); *see id.* at 35–38, 46.

Petitioner asserts that Varghese “explicitly describes capturing real-time contextual information including capturing real-time physical location information” during post-authentication. Reply 9; *see id.* at 17. As support, Petitioner quotes the disclosure in Varghese’s paragraph 109 that business policies (1) “generally include rules (referred to as ‘transaction rules’) that

evaluate parameters of individual in-session transactions for the likelihood of fraud or malicious intent” and (2) are generally applied “during post-authentication.” *Id.* at 9 (emphasis omitted) (quoting Ex. 1010 ¶ 109); *see id.* at 17–18. Petitioner also quotes the disclosure in Varghese’s paragraph 109 about the following “security rule”: “don’t allow (or challenge user for) money transfer request from an international IP address.” *Id.* at 9, 18 (emphasis omitted) (quoting Ex. 1010 ¶ 109) (citing Ex. 1056 ¶ 29).

As additional support, Petitioner provides the following highlighted version of Varghese’s Table 10 in paragraph 110 (Reply 10):

TABLE 10

Restricted business policy model rules
Money transfer request is greater than a certain dollar amount
Money transfer request to and from a specific suspected fraud or an international account
Money transfer request of a certain dollar amount by a user who is logged in from another country
Bill payment to a non-merchant account is greater than certain dollar amount
Transaction from an un-registered device/location or frequently used fraud device/location. This could trigger a customer service request or challenge question or an out of band phone authentication

Table 10 “present[s] exemplary rules that evaluate conditions that can indicate a transaction should be restricted, challenged or rejected.” Ex. 1010 ¶ 110. The above highlighted version of Table 10 includes red highlighting over (1) the title “Restricted business policy model rules” and (2) a model rule for “Transaction from an un-registered device/location or frequently used fraud device/location.” *See* Reply 10; Ex. 1056 ¶ 20.

Further, Petitioner asserts that Varghese “explicitly describes the use of sensor-based biometrics including ‘obtaining biometric identification

information (e.g., fingerprints, retinal scans, or the like)” and “does not exclude sensors for capturing biometrics.” Reply 8 (quoting Ex. 1010 ¶ 79). According to Petitioner, Varghese’s disclosure about providing a “purely software based solution to identity theft that does not require hardware devices to be issued and maintained” concerns “tokens associated with the ‘something the user has’ factor (e.g., password-generating token).” *Id.*

(iv) Reasonable Expectation of Success

Petitioner asserts that an ordinarily skilled artisan “would have reasonably expected to succeed in configuring Stone-Hoyos, since the implementation of Hoyos’ biometric authentication in Stone would have required only routine knowledge well within” the artisan’s skill. Pet. 20 (citing Ex. 1003 ¶¶ 71–73). Petitioner also asserts that an ordinarily skilled artisan “would have reasonably expected to succeed in configuring Stone-Hoyos-Varghese since implementing Varghese’s multifactor real-time authentication functionality would have required only routine knowledge well within” the artisan’s skill. *Id.* at 22–23 (citing Ex. 1003 ¶¶ 82–84).

(b) Patent Owner’s Contentions

(i) Motivation to Combine: Combining the Teachings of Stone and Hoyos

Patent Owner contends that Petitioner provides a “conclusory” explanation for combining Hoyos’s teachings with Stone’s teachings that lacks “a justification for why” an ordinarily skilled artisan would have combined their respective teachings in a way that yields the claimed inventions. Resp. 15 (emphasis omitted) (citing *TQ Delta, LLC v. Cisco Sys., Inc.*, 942 F.3d 1352, 1356 (Fed. Cir. 2019)); *see* Sur-reply 3.

According to Patent Owner, Petitioner’s explanation for combining Hoyos’s teachings with Stone’s teachings “can be summarized” by the following assertions:

- (1) “[I]t was well-known that financial transaction systems of Stone had a need for authentication for fraud detection (e.g., with higher levels of security for higher-risk transactions)”; and
- (2) an ordinarily skilled artisan “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.’”

Resp. 15–16 (alteration by Patent Owner) (quoting Pet. 16–17); *see* Sur-reply 2. Patent Owner argues that the above assertions “do not explain why” an ordinarily skilled artisan would have combined the teachings of the references. Resp. 16 (emphasis omitted).

Regarding Petitioner’s argument about “a need for higher security authentication in high-risk banking and financial institution transactions over certain dollar amounts,” Patent Owner contends that:

- (1) Stone “is assigned to eBay”;
- (2) Stone’s “figures depict PayPal transfers”;
- (3) neither eBay nor PayPal “is a bank or financial institution”; and
- (4) “the example transaction in Stone is for a low-dollar amount,” i.e., \$26.32 as shown in Figure 2.

Sur-reply 3 (citing Pet. 16; Ex. 1008, Fig. 2). According to Patent Owner, the evidence does not support Petitioner’s assertion that it was “well-known”

that the “lower-dollar, non-bank” transactions of Stone “required fraud detection.” *Id.* at 3–4.

Further, Patent Owner asserts that an ordinarily skilled artisan would not have combined Hoyos’s biometric authentication with Stone’s system for financial transactions because:

- (1) “Stone does not identify electronic payment fraud as a problem needing to be solved”;
- (2) “Stone never mentions fraud, nor does it discuss any techniques for preventing fraud, like those described in Hoyos”;
- (3) “Stone discloses an enhanced currency display,” “is not concerned with the actual processing of transactions,” and does not detail “how funds are transferred”;
- (4) “Stone does not state that the user identifier is used for performing some form of authentication or fraud detection, specifically biometric-based fraud detection”;
- (5) “Hoyos has a limited focus—improving known biometric matching techniques by incorporating a method to determine the probability that the subject is alive”; and
- (6) “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).”

Resp. 16–17 (citing Ex. 1008 ¶¶ 2, 16, 23, 45; Ex. 1013 ¶¶ 16–22; Ex. 2032 ¶¶ 57–59); *see* Sur-reply 4. Therefore, according to Patent Owner, “[n]othing in Hoyos would lead [an ordinarily skilled artisan] to combine its biometric authentication methods with an interactive interface, particularly a currency display like the one Stone provides.” Resp. 17–18 (citing Ex. 2032 ¶¶ 57–61).

Patent Owner asserts that an ordinarily skilled artisan would not have combined Hoyos's biometric authentication with Stone's system for financial transactions because "Stone and Hoyos teach away from each other in material ways." Resp. 15, 22; *see id.* at 22–26; Sur-reply 5–7. According to Patent Owner, Stone and Hoyos are "incompatible" because "they are directed to different computing environments." Resp. 23; *see id.* at 26; Sur-reply 5, 21. Patent Owner explains that:

- (1) "Stone discloses only a client-server structure for implementing its currency display" where "the payment server maintains the user accounts, account information, and payment applications";
- (2) "Stone requires a client-server structure" with the payment server storing "all user account information needed to process a money transfer"; and
- (3) Hoyos implements biometric authentication on "a client device and never discusses implementing its techniques on a server."

Resp. 23–24 (citing Ex. 1008 ¶¶ 40–48, Fig. 4; Ex. 1013 ¶¶ 16–22, claim 4; Ex. 2032 ¶ 68); Sur-reply 5, 21.

Patent Owner asserts that the proposed combination of Hoyos's biometric authentication with Stone's system for financial transactions rests on "hindsight bias that the Supreme Court and Federal Circuit have routinely rejected." Resp. 18 (citing *KSR*, 550 U.S. at 421).

Additionally, Patent Owner contends that an ordinarily skilled artisan would not have implemented Hoyos's biometric authentication in "Stone's client-server structure" for several reasons. *See* Resp. 24–26; Sur-reply 6–7. First, Patent Owner asserts that implementing Hoyos's biometric authentication in "Stone's client-server structure" would require a

“redundant” second authentication after an initial authentication needed to view a user’s account balance. *See* Resp. 24–25; Sur-reply 5. According to Patent Owner, using Hoyos’s biometric authentication as “the final step before completing the transaction” would “require on-device authentication after the device has already transferred information in communication with payment server 408.” Resp. 24–25 (emphasis omitted) (citing Ex. 2032 ¶¶ 70–71). Also, “[s]toring the same user account information on the user device would be a waste of device storage.” Sur-reply 5.

Second, Patent Owner asserts that implementing Hoyos’s biometric authentication in “Stone’s client-server structure” would “increase latency within the transaction” by “requiring communication with a server.” Resp. 25; Sur-reply 6; *see* Resp. 26. According to Patent Owner, “increas[ing] latency within the transaction” would undermine Hoyos’s “primary goal” of “transaction speed” to “address a problem that Stone does not even identify as a concern (electronic payment fraud).” Resp. 25 (citing Ex. 1013 ¶¶ 9, 11).

Third, Patent Owner asserts that implementing Hoyos’s biometric authentication in “Stone’s client-server structure” would undermine Hoyos’s “stated goals” of “accuracy” and “security of biometric authentication” due to “the possibility of a data breach of the server where a user’s biometric information would be stored.” Resp. 25–26. Also, “requiring communication with a server” would “decrease privacy and security of user information by requiring transfer of sensitive data over a network.” Sur-reply 6 (citing Ex. 2032 ¶¶ 70–72).

Fourth, Patent Owner asserts that implementing Hoyos’s biometric authentication in “Stone’s client-server structure” would “unnecessarily tie

up resources on the user device that the client-server structure is meant to free up.” Resp. 25 (citing Ex. 2032 ¶ 70). According to Patent Owner, “[r]unning computationally intensive biometric analysis locally could lead to performance bottlenecks, especially on older or lower-end devices.” Sur-reply 5–6 (citing Ex. 1038, 64).

(ii) Motivation to Combine: Combining the Teachings of Varghese with the Teachings of Stone and Hoyos

Patent Owner contends that an ordinarily skilled artisan “would not have been motivated to combine Varghese with Stone and Hoyos.” Resp. 27 (citing Ex. 2032 ¶¶ 73–77); *see id.* at 34 (citing Ex. 2032 ¶¶ 85–87). Specifically, Patent Owner asserts that “Varghese, like Stone, requires a server structure for its location capture” where authentication “involves information transferred from the client to the server.” *Id.* at 27 (citing Ex. 1010 ¶¶ 5–6; Ex. 2032 ¶ 73); Sur-reply 7. Patent Owner asserts that “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 claimed fraud analysis. Resp. 27 (citing Ex. 2032 ¶ 73); *see* Sur-reply 7–8.

Patent Owner also asserts that Varghese:

- (1) provides a “purely software based solution to identity theft that does not require hardware devices to be issued and maintained”;
- (2) concerns “using information from the user’s device itself rather than the user for fraud detection”; and
- (3) does not concern “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).”

Resp. 27–28 (emphasis omitted) (quoting Ex. 1010 ¶ 22) (citing Ex. 1010 ¶¶ 17, 21–22; Ex. 2032 ¶ 74); *see* Sur-reply 8. According to Patent Owner, the “software-only goal of Varghese requires implementation through a client-server structure.” Resp. 27 (citing Ex. 2032 ¶¶ 86–87).

Additionally, Patent Owner contends that 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).” Resp. 28; *see* Sur-reply 8. Therefore, according to Patent Owner, an ordinarily skilled artisan “would not have been motivated to look to Hoyos to improve or alter the system disclosed by Varghese” to yield the claimed inventions. Resp. 28 (citing Ex. 2032 ¶ 76).

Further, Patent Owner asserts that “Varghese specifically teaches against applying a location check as one of the final steps” for “fraud detection analysis” according to the claimed inventions. Resp. 29; *see* Sur-reply 17. Patent Owner explains that “Varghese discloses a multifactor authentication framework divided into pre-authentication and post-authentication stages” where:

- (1) pre-authentication concerns “collection of information related to the user and the user’s device to authenticate a user logging into a web application” and focuses “heavily on information collected from the user’s device,” e.g., “device fingerprint that involves collection of IP address information, among other things”; and
- (2) post-authentication concerns “completing monetary electronic transactions” that “are authenticated using a user’s transaction history and historic workflow” such

that “criteria related to initial authentication [e.g., pre-authentication location data] are usually less important.”

Resp. 29–30 (alteration by Patent Owner) (emphasis omitted) (quoting Ex. 1010 ¶ 89) (citing Ex. 1010 ¶¶ 74, 65, 90; Ex. 2032 ¶ 77); *see id.* at 34–35 (citing Ex. 1010 ¶¶ 65, 74, 90–93, 96, 99; Ex. 2032 ¶¶ 85–87); Sur-reply 16 (citing Ex. 1010 ¶¶ 65, 74, 90–93, 96, 99).

Patent Owner contends that Varghese does not disclose collecting location data “during post-authentication (i.e., in-transaction).” Sur-reply 9 (emphasis omitted); *see id.* at 9–11; Resp. 34–36. Patent Owner also contends that location data used for post-authentication in Varghese was already collected for pre-authentication, i.e., at login, not newly collected for post-authentication. *See* Sur-reply 9–11, 15–20; Tr. 104:3–5, 104:23–105:3.

Regarding the model rules in Varghese’s Table 10, e.g., the model rule for “Money transfer request of a certain dollar amount by a user who is logged in from another country,” Patent Owner asserts that these rules “apply location data that was already collected at login” rather than “location data collected when a transaction was confirmed.” Sur-reply 9, 18. Patent Owner asserts that Varghese’s paragraph 103 and Table 6A, like paragraph 109 and Table 10, (1) “discuss the use of location information within security policies” and (2) “address location associated with user login,” thus “indicating the login is the relevant collection point for location data,” not the “transaction confirmation step as Petitioner’s Stone-Hoyos-Varghese model suggests.” *Id.* at 10, 19 (emphasis omitted) (citing Ex. 1010 ¶¶ 102–114).

As support, Patent Owner provides the following highlighted versions of Varghese’s Tables 6A and 6B in paragraphs 103 and 104 (Sur-reply 10–11, 20):

TABLE 6A		TABLE 6B	
Restricted model		Hacker model	
Location based rules	Logins from restricted countries, (e.g. OFAC countries)	Location based rules	User login from different geographical location (city, state or country) within a given time period
	Logins from restricted IP addresses		Multiple logins from a given IP address within a given time period
	Logins from restricted anonymizers and proxies		User login from different geographical location (city, state or country) within a given time period
User based rules	Logins from restricted users list	User based rules	User login from different device within a given time period
Device based rules	Multiple consecutive failures for the user	Device based rules	Multiple failures from a given device within a given time period
	Logins from restricted devices		Multiple logins from a given device within a given time period
	Multiple consecutive failures from the device		Same device used from different geographical location within a given time period
	Device using stolen cookies		
	User using the device for the first time		

Table 6A titled “Restricted model” above on the left and Table 6B titled “Hacker model” above on the right “present illustrative security models” based on “risk patterns associated with user, device and location information.” Ex. 1010 ¶¶ 103–104. The above highlighted versions of Tables 6A and 6B include orange highlighting over the phrases “Location based rules,” “Logins from,” “Multiple logins from,” and “login from.” See Sur-reply 10–11, 20.

Patent Owner contends that “Varghese’s collection of location data at user login and not at the step where a user confirms a transaction (as Petitioner’s Stone-Hoyos-Varghese transaction model requires) undermines Petitioner’s alleged motivation to combine these references in the manner Petitioner describes.” Sur-reply 11; *see id.* at 15.

Also, Patent Owner asserts that an ordinarily skilled artisan “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.” Resp. 30 (bracketed text added by Patent Owner) (emphasis omitted) (citing Ex. 2032 ¶¶ 73–77); *see* Sur-reply 15.

(c) Analysis

(i) Motivation to Combine: Combining the Teachings of Stone and Hoyos

Petitioner identifies reasons that would have prompted an ordinarily skilled artisan to combine Hoyos’s teachings with Stone’s teachings in the way Petitioner proposes. *See* Pet. 14–20, 44–45, 52–53; Reply 4.

Dr. Jones’s testimony supports Petitioner’s positions. *See* Ex. 1003 ¶¶ 59–70, 126–127, 141; Ex. 1056 ¶ 8.

Regarding reasons to combine Hoyos’s teachings with Stone’s teachings, Stone contemplates security measures for financial transactions, such as using a “password” or “biometric id,” and Petitioner, supported by Dr. Jones’s testimony, identifies several advantages from using Hoyos’s biometric authentication in Stone’s system for financial transactions. *See* Pet. 13–14, 16–20, 44–45, 52–53; Ex. 1003 ¶¶ 58, 64–70, 126–127, 141; Ex. 1008 ¶¶ 45, 48; Ex. 1056 ¶ 8. Those advantages include the following:

- (1) “improved fraud resistance by addressing spoofing”;
- (2) “improved deterren[ce] against attempted fraudulent transactions”;
- (3) “decreased rejection of valid customers”;
- (4) “an enormous deterrent to criminals since the system is acquiring biometric data that they have no idea can or cannot be used successfully as evidence against them”;
and
- (5) providing “a means to perform customer redress” by ensuring that “some live-person data is captured.”

Ex. 1003 ¶¶ 64, 67, 126–127, 141; Ex. 1013 ¶¶ 12, 15, 24, 26–27, 29; Ex. 1056 ¶ 8; *see* Pet. 16–17, 44–45, 52–53. Petitioner and Dr. Jones persuade us that the advantages of using known biometric authentication techniques described by Hoyos to improve financial-transaction security would recommend their use in Stone. *See, e.g.*, Ex. 1003 ¶ 66 (Dr. Jones explaining that “it was well-known that [the] financial transactions of Stone had a need for authentication for fraud detection (e.g., with higher levels of security for some transactions”). The “desire to enhance commercial opportunities by improving a product or process is universal” *DyStar Textilfarben GmbH v. C.H. Patrick Co.*, 464 F.3d 1356, 1368 (Fed. Cir. 2006).

A motivation to combine “can be found explicitly or implicitly in the prior art references themselves, in market forces, in design incentives, or in ‘any need or problem known in the field of endeavor at the time of invention and addressed by the patent.’” *Forest Lab ’ys, LLC v. Sigmapharm Lab ’ys, LLC*, 918 F.3d 928, 934 (Fed. Cir. 2019) (quoting *Arctic Cat Inc. v. Bombardier Recreational Prods. Inc.*, 876 F.3d 1350, 1359 (Fed. Cir. 2017)). Here, Petitioner identifies a motivation to combine “in the prior art references themselves,” i.e., in Hoyos’s disclosures about the advantages of Hoyos’s techniques, such as “improved deterren[ce] against attempted fraudulent transactions” and “decreased rejection of valid customers.” Pet. 16–17, 44–45, 52–53 (quoting Ex. 1013 ¶¶ 15, 24, 26–27, 29); *see* Ex. 1003 ¶¶ 64, 67, 126–127, 141; Ex. 1013 ¶¶ 12, 15, 24, 26–27, 29; Ex. 1056 ¶ 8. Hence, we disagree with Patent Owner that Petitioner provides a “conclusory” explanation for combining Hoyos’s teachings with Stone’s teachings that lacks “a justification for why” an ordinarily skilled

artisan would have combined their respective teachings. *See* Resp. 15 (emphasis omitted).

As for Patent Owner’s contention that “[n]othing in Hoyos would lead [an ordinarily skilled artisan] to combine its biometric authentication methods with an interactive interface,” Stone does not disclose a generic “interactive interface.” *See* Ex. 1008 ¶¶ 6–8, 10–12, 22–39, Figs. 1–3; Resp. 17–18. Instead, Stone discloses an “interactive interface” for completing financial transactions where a sender transfers funds to a recipient. Ex. 1008 ¶¶ 6–8, 10–12, 22–39, Figs. 1–3; *see* Ex. 1003 ¶¶ 39–40. Hoyos similarly discloses financial transactions where a sender transfers funds to a recipient. Ex. 1013 ¶¶ 15–37, codes (54), (57), Fig. 1; *see* Ex. 1003 ¶¶ 41–45.

Moreover, “[t]here is a motivation to combine when a known technique ‘has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way,’ using the ‘prior art elements according to their established functions.’” *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1380–81 (Fed. Cir. 2023) (citations omitted) (quoting *KSR*, 550 U.S. at 417; *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 784, 799–800 (Fed. Cir. 2021)). Here, Petitioner identifies Hoyos’s known techniques used to improve authentication for financial transactions that would improve authentication for financial transactions in Stone’s system in the same way when used according to Hoyos’s teachings. *See* Pet. 16–17, 44–45, 52–53; Ex. 1003 ¶¶ 64–70, 126–127, 141.

We also disagree with Patent Owner that Stone had no need for authentication including “fraud detection” because Stone discloses “lower-dollar, non-bank” transactions. *See* Sur-reply 3–4. As discussed above in

this section, Stone contemplates security measures for financial transactions, such as using a “password” or “biometric id.” Ex. 1008 ¶¶ 45, 48; *see* Ex. 1003 ¶¶ 58, 65. Stone does not limit its disclosure to “lower-dollar, non-bank” transactions. *See* Ex. 1008 ¶¶ 6–8, 16, 18, 23, 27, 29–39, 55–56, code (57), Figs. 1–3. For instance, Stone discloses that funding source box 206 may identify a “bank,” “bank card,” or “bank account” and that the amount transferred may go into a recipient’s “bank account.” *Id.* ¶¶ 8, 19, 34, 38–39, claims 8 and 30; *see id.* ¶ 18 (discussing funds “located in U.S. banks”).

Although Stone discloses illustrative transactions involving \$22.86, \$26.32, \$33.26, \$86.21, \$126.32, \$126.34, and \$765.32, Stone does not place any restrictions on the amount transferred. Ex. 1008 ¶¶ 6, 16, 18, 23, 27, 30–31, 55–56, code (57), Figs. 1–2. Instead, Stone states that the “disclosure is not intended to limit the present invention.” *Id.* ¶ 55. Consistent with that statement, Stone’s claim 1 broadly recites “an input device configured to allow a user to enter a money amount.” *Id.* claim 1.

Further, to paraphrase the expression “one man’s meat is another man’s poison,” one person’s pittance is another person’s fortune. So even “lower-dollar, non-bank” transactions may benefit from “improved fraud resistancy by addressing spoofing,” “improved deterren[ce] against attempted fraudulent transactions,” and “decreased rejection of valid customers” as taught by Hoyos. *See* Ex. 1003 ¶¶ 64, 67, 126–127, 141; Ex. 1013 ¶¶ 12, 15, 24, 26–27, 29.

Additionally, an ordinarily skilled artisan would have understood the desirability of implementing multiple authentications, e.g., “with higher

levels of security for some transactions.” *See* Ex. 1003 ¶¶ 66, 76. As an example, Varghese explains that:

- (1) a “user or service provider may request further authentication during the course of a valid already-authenticated session based on, e.g., the transaction being requested”; and
- (2) a “bank or other financial institution may wish to invoke a higher security authentication interface during a session before transactions over a certain amount are sent to the server.”

Ex. 1010 ¶ 148; *see id.* ¶¶ 79, 84, 91, 109–110; Ex. 1003 ¶ 66 (quoting Ex. 1010 ¶ 148); Inst. Dec. 55 (quoting Ex. 1010 ¶ 148).

As another example, Carter explains that “different authentication levels may be necessary for different transactions” and that “the necessary authentication level is determined based on the transaction criteria” or “the context of the transaction.” Ex. 1016 ¶¶ 36, 73; *see* Ex. 1003 ¶ 66 (quoting Ex. 1016 ¶ 73); Inst. Dec. 55 (quoting Ex. 1016 ¶¶ 36, 73). Carter also explains that “the risk of fraud is greatly decreased” by requiring “greater authentication” for “higher value (and higher risk) purchases.” Ex. 1016 ¶ 36.

Carter discloses the following illustrative authentication levels:

- (1) a “first level of authentication is a fingerprint identification,” which “can be required for all transactions, due to its ease and simplicity”;
- (2) a “second level of authentication is a personal identification number (PIN) that is memorized by the person and entered”;
- (3) a “third level of authentication is a voice biometric identification, which can be performed locally or by transmission of voice data to a remote source”;

- (4) a “fourth level of identification is facial recognition, which can also be performed locally or by transmission of facial data to a remote source”; and
- (5) a “fifth level of authentication is GPS location authentication,” which “can be reserved for significant transactions having high value.”

Ex. 1016 ¶¶ 36, 38–40, 42–43; *see* Ex. 1003 ¶¶ 72–73, 76–77 (citing Ex. 1016 ¶¶ 36, 40, 42–43, 76); Ex. 1056 ¶¶ 14, 16 (quoting Ex. 1016 ¶¶ 40, 42). For instance, when using “value-based authentication,” “transactions of higher value may require PIN authentication, as well as fingerprint,” and “transactions of still higher value may require PIN, fingerprint, and voice biometric authentication.” Ex. 1016 ¶¶ 39–40.

Because an ordinarily skilled artisan would have understood the desirability of implementing multiple authentications to reduce the risk of fraud, we disagree with Patent Owner that implementing Hoyos’s biometric authentication in “Stone’s client-server structure” would require a “redundant” second authentication after an initial authentication needed to view a user’s account balance. *See* Ex. 1003 ¶¶ 66, 76; Ex. 1010 ¶¶ 79, 84, 91, 109–110, 148; Ex. 1016 ¶¶ 36, 38–40, 42–43, 73; Resp. 24–25. An ordinarily skilled artisan would have recognized Hoyos’s biometric authentication as “complementary” rather than “redundant” in Stone’s system for financial transactions. Ex. 1056 ¶ 14.

As for Patent Owner’s contentions that Stone and Hoyos are “incompatible” because “Stone requires a client-server structure” with the payment server storing “all user account information needed to process a money transfer” and Hoyos implements biometric authentication on “a client device,” we disagree. *See* Resp. 23–24; Sur-reply 5. As Dr. Jones testifies,

an ordinarily skilled artisan could have implemented (1) “biometric information capturing” and (2) “fraud detection analysis” either “locally” at a client device or “remotely,” e.g., “by sending the biometric information to a payment provider device, or another remote device.” Ex. 1003 ¶ 72. An ordinarily skilled artisan would have adapted or applied Hoyos’s biometric authentication to “function within Stone’s system (either on the client or on a server), achieving secure authentication without undermining the system’s architecture.” Ex. 1056 ¶¶ 14, 16.

Consistent with Dr. Jones’s testimony, a 2005 paper titled “Secure Biometric Authentication for Weak Computational Devices” and co-authored by Dr. Goodrich explains that “[t]here are two broad approaches” for biometric authentication. Ex. 1055, 2; *see* Ex. 1056 ¶ 14; Ex. 2031, 16. Specifically, “the comparison is done at” either “the client end (the portable device where the biometric measurement is done)” or “the remote server.” Ex. 1055, 2; *see* Ex. 1056 ¶ 14. Similarly, a 2006 paper titled “Privacy Preserving Multi-Factor Authentication with Biometrics” states that biometric authentication “can be implemented through systems performing the matching either on the server or on the client side.” Ex. 1038, 64 (emphases omitted); *see* Ex. 1003 ¶ 73 (quoting Ex. 1038, 64); Ex. 1056 ¶ 15 (quoting Ex. 1038, 64); Inst. Dec. 54 (quoting Ex. 1038, 64).

Also consistent with Dr. Jones’s testimony, Carter discloses performing “voice biometric identification” and “facial recognition” either “locally” or “by transmission” of data to a remote computer. Ex. 1016 ¶¶ 40, 42; *see* Ex. 1056 ¶¶ 14, 16 (quoting Ex. 1016 ¶¶ 40, 42).

Dr. Jones explains, however, that an ordinarily skilled artisan “would have been motivated to implement the fraud detection analysis based on the

biometric information locally on the user device of Stone” to obtain the following benefits:

- (1) “reduced latency (e.g., by minimizing communication delays between the user device and network server)”;
- (2) “offline analysis capabilities (allowing for analysis even when the user device is offline or has limited connectivity)”;
- (3) “enhanced privacy (by reducing the amount of data that needs to be transmitted to the server and minimizing potential privacy concerns)”;
- (4) “efficient resource utilization (helping distributing the processing load to the user device)”;
- (5) “customization for device characteristics (enhancing fraud detection by considering user device specific characteristics and capabilities)”;
- (6) “improved security (where a malicious actor intends to compromise the user device system)”;
- (7) “reduced server load for cost savings and improved scalability (especially where the system has a large user base).”

Ex. 1003 ¶ 73 (emphasis omitted).

For the reasons Dr. Jones explains, implementing “the fraud detection analysis based on the biometric information locally on the user device of Stone” would avoid problems that Patent Owner identifies, such as “increase[d] latency within the transaction,” “decrease[d] privacy and security of user information,” and “the possibility of a data breach of the server where a user’s biometric information would be stored.” *See* Ex. 1003 ¶ 73; Resp. 25–26; Sur-reply 6.

Regarding Patent Owner’s assertion that “[s]toring the same user account information on the user device would be a waste of device storage,”

implementing “the fraud detection analysis based on the biometric information locally on the user device of Stone” would not require transferring user account information from payment provider server 408 to the user device. *See* Ex. 1003 ¶ 73; Sur-reply 5. Hence, the user device would not need to store “the same user account information” as the payment provider server 408.

Regarding Patent Owner’s assertion that “[r]unning computationally intensive biometric analysis locally could lead to performance bottlenecks,” Hoyos does not identify any performance issues when accomplishing biometric authentication locally on a client device according to its teachings. *See* Ex. 1013 ¶¶ 16–40; Sur-reply 5–6. Nothing in Hoyos indicates that implementing “the fraud detection analysis based on the biometric information locally on the user device of Stone” according to Hoyos’s teachings would cause any performance bottlenecks. *See* Ex. 1013 ¶¶ 16–40.

Moreover, Stone contemplates the user device accomplishing tasks not expressly described in Stone that could reasonably include biometric authentication. *See* Ex. 1008 ¶ 43, Fig. 4. Specifically, Stone explains that user device 404 may include “one or more toolbar applications 412” that “provide client-side processing for performing tasks in response to operations selected by user 409.” *Id.* ¶ 43.

We disagree with Patent Owner that an ordinarily skilled artisan would not have combined Hoyos’s biometric authentication with Stone’s system for financial transactions because “Stone and Hoyos teach away from each other in material ways.” *See* Resp. 15, 22–26; Sur-reply 5–7. “A reference does not teach away” if “it merely expresses a general

preference for an alternative invention but does not ‘criticize, discredit, or otherwise discourage’ investigation into the invention claimed.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1327 (Fed. Cir. 2009) (quoting *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004)). Patent Owner does not identify any statement in Stone or Hoyos that “criticize[s], discredit[s], or otherwise discourage[s]” the proposed combination that yields the claimed inventions. *See, e.g.*, Resp. 15, 22–26; Sur-reply 5–7; *see also* Ex. 1056 ¶¶ 11–15.

As for Patent Owner’s assertion that the proposed combination of Hoyos’s biometric authentication with Stone’s system for financial transactions rests on “hindsight bias,” we disagree. *See* Resp. 18. An explicit analysis “whether there was an apparent reason to combine” the teachings of the references reduces “the risk of . . . falling prey to hindsight bias.” *See KSR*, 550 U.S. at 418, 421. As discussed above in this section, Petitioner provides an explicit analysis why an ordinarily skilled artisan would have been motivated to combine Hoyos’s teachings with Stone’s teachings, e.g., to obtain the benefits of “improved fraud resistancy by addressing spoofing,” “improved deterren[ce] against attempted fraudulent transactions,” and “decreased rejection of valid customers” as taught by Hoyos. *See* Pet. 16–17, 44–45, 52–53; Ex. 1003 ¶¶ 64, 67, 126–127, 141; Ex. 1056 ¶ 8.

(ii) Motivation to Combine: Combining the Teachings of Varghese with the Teachings of Stone and Hoyos

Petitioner identifies reasons that would have prompted an ordinarily skilled artisan to combine Varghese’s “real-time multifactor authentication” including “location authentication combined with biometrics (e.g., voice,

fingerprints, retinal scans, etc.)” with the Stone-Hoyos system in the way Petitioner proposes. *See* Pet. 21–22, 36–39, 49. Dr. Jones’s testimony supports Petitioner’s positions. *See* Ex. 1003 ¶¶ 74, 76–81, 114–118, 135; Ex. 1056 ¶¶ 16–20.

In particular, combining Varghese’s “real-time multifactor authentication” including “location authentication combined with biometrics (e.g., voice, fingerprints, retinal scans, etc.)” with the Stone-Hoyos system would have “improved security for financial transactions,” for example by:

- (1) providing “more accurate fraud analysis by using more accurate, real-time data”;
- (2) “evaluating fraud risk based on physical location determined from location data”;
- (3) providing “contextual authentication adaptive for the specific transaction based on transaction information (e.g., type, amount)”;
- (4) performing “fraud detection based on whether the two locations (captured before and after confirmation at block 316 [in Stone’s Figure 3]) match, for improved security.”

Ex. 1003 ¶¶ 81, 114, 118, 135; *see* Pet. 36–39, 49. Hence, we disagree with Patent Owner that an ordinarily skilled artisan “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].” *See* Resp. 30 (emphasis omitted).

Additionally, we disagree with Patent Owner that location data used for post-authentication in Varghese was already collected for pre-authentication, i.e., at login, not newly collected for post-authentication. *See* Sur-reply 9–11, 15–20; Tr. 104:3–5, 104:23–105:3. Varghese discloses

“real-time risk scoring” for “each online login and transaction,” i.e., “at login and in session,” to “increase authentication security in real time.” Ex. 1010 ¶¶ 38–39; *see* Ex. 1003 ¶ 113; Ex. 1056 ¶¶ 28–29. Evaluating “in-session characteristics” (post-authentication) of each transaction “ensure[s] fraud detection and transactional integrity.” Ex. 1010 ¶ 38. For example, post-authentication may apply to “an existing user making a request that needs particular authentication,” e.g., a request involving “high risk or potential fraud.” *Id.* ¶¶ 38, 79.

Varghese explains that “real-time risk scoring” depends on, among other things, location data. Ex. 1010 ¶¶ 77, 88, 109, 140, 142, claim 31 (reciting an “access policy” based on “risks related to the current location of the user device” and “risk related to the current transaction”); *see* Ex. 1003 ¶¶ 48, 113; Ex. 1056 ¶¶ 28–29. Varghese’s analytics-and-scoring system may collect location data from “geolocation data services providing [the] likely geographical source of the current request” during “the course of a valid already-authenticated session.” Ex. 1010 ¶¶ 77, 142, 148, claim 14 (reciting “a device geolocation data provider”); *see* Inst. Dec. 56 (citing Ex. 1010 ¶¶ 74–75, 77, 142, 148). For instance, a user transaction request that involves “an amount of money over a certain threshold” or “large amounts of money” (“a high-value transaction”) may “invoke a higher security authentication.” Ex. 1010 ¶¶ 74–75, 142, 148. Moreover, one of Varghese’s model rules focuses on the location when a transaction actually occurs by specifying “Transaction from an un-registered device/location or frequently used fraud device/location.” *Id.* ¶ 110; *see* Ex. 1003 ¶ 113; Ex. 1056 ¶¶ 19–20.

Further, Varghese’s Figure 14 depicts an “exemplary functional configuration” with “Real-time Analytics & Scoring” for authenticating a user transaction request based on fingerprints that are “processed and scored in real-time” by a rules engine. Ex. 1010 ¶¶ 91, 97, Fig. 14; *see* Ex. 1003 ¶ 48. The fingerprints include “a location fingerprint, a device fingerprint, a workflow fingerprint, and an historical data fingerprint.” Ex. 1010 ¶ 91, Fig. 14; *see* Ex. 1003 ¶ 113. Figure 14 illustrates a “Location Fingerprint” including “IP, Geo-Location, Network forensics.” Ex. 1010, Fig. 14; *see* Ex. 1003 ¶ 113; Ex. 1056 ¶ 28.

An ordinarily skilled artisan would have understood that real-time authentication according to Varghese includes “both real-time capture and real-time analysis of authentication data,” including location data. Ex. 1003 ¶ 114; *see* Ex. 1010 ¶¶ 38–39, 74–75, 77, 79, 88, 91, 97, 109, 140, 142, 148, claim 14, Fig. 14; Ex. 1056 ¶ 28.

Patent Owner’s assertion that “Varghese specifically teaches against applying a location check as one of the final steps” for “fraud detection analysis” according to the claimed inventions lacks merit. *See* Resp. 29. A “reference does not teach away” if “it merely expresses a general preference for an alternative invention but does not ‘criticize, discredit, or otherwise discourage’ investigation into the invention claimed.” *DePuy Spine*, 567 F.3d at 1327. Patent Owner does not identify any statement in Varghese that “criticize[s], discredit[s], or otherwise discourage[s]” the proposed combination that yields the claimed inventions. *See, e.g.*, Resp. 27–30; Sur-reply 7–11.

As for Varghese’s disclosure about providing a “purely software based solution to identity theft that does not require hardware devices to be

issued and maintained,” we agree with Petitioner that the disclosure concerns “tokens associated with the ‘something the user has’ factor (e.g., password-generating token).” *See* Reply 8; Ex. 1056 ¶ 17. Varghese also discloses using hardware-based biometric sensors, e.g., for “obtaining biometric identification information (e.g., fingerprints, retinal scans, or the like), or obtaining voice prints, or the like.” Ex. 1010 ¶ 79; *see* Ex. 1056 ¶ 17. Additionally, Varghese’s Figure 14 depicts “Primary/Secondary Authentication” including “Biometrics (Voiceprint, etc.).” Ex. 1010, Fig. 14; *see* Ex. 1003 ¶ 113. Varghese’s disclosure about using hardware-based biometric sensors demonstrates that Varghese’s analytics-and-scoring system accommodates biometric sensors as disclosed in Hoyos. *See* Ex. 1010 ¶ 79; Ex. 1056 ¶¶ 16–17.

Patent Owner’s assertion that an ordinarily skilled artisan “would not have been motivated to look to Hoyos to improve or alter the system disclosed by Varghese” to yield the claimed inventions mischaracterizes the proposed combination. *See* Pet. 16–22; Resp. 28. Petitioner does not propose modifying Varghese’s analytics-and-scoring system based on Hoyos’s teachings. *See* Pet. 16–22. Rather, Petitioner proposes modifying Stone’s system for financial transactions based on Hoyos’s teachings and Varghese’s teachings. *See id.*

Patent Owner’s assertion about problems “using a client-server structure (Varghese) with techniques performed only on a client device (Hoyos) to achieve” the claimed fraud analysis lacks merit for the reasons discussed above. *See* Resp. 27; *supra* § III.D.5(c)(i).

(iii) Reasonable Expectation of Success

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that an ordinarily skilled artisan:

- (1) “would have reasonably expected to succeed in configuring Stone-Hoyos, since the implementation of Hoyos’ biometric authentication in Stone would have required only routine knowledge well within” the artisan’s skill; and
- (2) “would have reasonably expected to succeed in configuring Stone-Hoyos-Varghese since implementing Varghese’s multifactor real-time authentication functionality would have required only routine knowledge well within” the artisan’s skill.

See Pet. 20, 22–23; Ex. 1003 ¶¶ 71–73, 82–84.

6. INDEPENDENT CLAIM 1

(a) Preamble 1.0

Claim 1 recites “[a] system.” Ex. 1001, 14:2.

Petitioner contends that Stone teaches claim 1’s preamble because Stone discloses system 400 “configured to utilize the currency display over a network 402.” Pet. 23 (emphasis omitted) (quoting Ex. 1008 ¶ 40); *see id.* at 70. According to Petitioner, system 400 includes “at least a user device 404,” one or more recipient devices 406, and “at least one payment provider server 408” communicating “over the network 402.” *Id.* (quoting Ex. 1008 ¶ 40).

Patent Owner makes no arguments specific to claim 1’s preamble. *See, e.g.,* Resp. 14–36; Sur-reply 2–22. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Generally, a preamble does not limit a claim. *Allen Eng'g Corp. v. Bartell Indus., Inc.*, 299 F.3d 1336, 1346 (Fed. Cir. 2002). We need not decide whether claim 1's preamble limits the claim because, for the reasons stated by Petitioner and supported by Dr. Jones's testimony, we agree with Petitioner that Stone teaches claim 1's preamble. *See* Pet. 23–24; Ex. 1003 ¶¶ 85–88.

(b) Limitation 1.1

Claim 1 recites “one or more processors configured to.” Ex. 1001, 14:3 (limitation 1.1).

Petitioner contends that Stone teaches limitation 1.1 and alternatively that the combined disclosures in Stone, Hoyos, and Varghese teach limitation 1.1. *See* Pet. 24–26. Specifically, Petitioner asserts that Stone's system 400 includes “one or more processors (e.g., processor 504 in user device 404 alone, or in combination with processors 504 of [other] devices in the system) configured to perform processes for a transaction.” *Id.* at 25–26 (citing Ex. 1008 ¶ 49, Figs. 4–5); *see id.* at 54. According to Petitioner, Stone discloses the following examples for processor 504: “processor, micro-controller, digital signal processor (DSP), etc.” *Id.* at 25 (emphasis omitted) (quoting Ex. 1008 ¶ 49).

Additionally, Petitioner asserts that Stone alone or the combined disclosures in Stone, Hoyos, and Varghese teach “one or more processors configured to” perform the processes recited in limitations 1.2.1–1.4.2, including “initiating, authenticating, and completing the electronic transaction.” Pet. 26 (citing Ex. 1003 ¶ 93).

Patent Owner makes no arguments specific to limitation 1.1. *See, e.g.,* Resp. 14–36; Sur-reply 2–22.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that Stone alone and the combined disclosures in Stone, Hoyos, and Varghese teach limitation 1.1. *See* Pet. 24–26; Ex. 1003 ¶¶ 89–94; *infra* §§ III.D.6(c)–(h).

(c) Limitation 1.2.1

Claim 1 requires a processor configured to “render, in one or more interfaces, a virtual likeness of a face associated with an account holder.” Ex. 1001, 14:4–5 (limitation 1.2.1).

Petitioner contends that Stone teaches limitation 1.2.1 for two independent reasons. *See* Pet. 26–29, 70. First, for a sender account holder, Petitioner asserts that Stone’s Figure 2 shows “a photograph of a user’s face on the personalized currency on interface 200” corresponding to “a virtual likeness of a face associated with an account holder (user/sender)” as claimed. *Id.* at 27 (emphasis omitted). As support, Petitioner quotes Stone’s disclosure about personalizing the currency for display as follows: “the user may select or create his own currency for display, such as . . . personalized currency with the user’s photo, etc.” *Id.* (alteration by Petitioner) (emphasis omitted) (quoting Ex. 1008 ¶ 7).

Second, for a recipient account holder, Petitioner asserts that Stone’s Figure 2 shows a “picture of the recipient” in name box 202. Pet. 28 (citing Ex. 1008 ¶¶ 20, 24, 36, Fig. 2).

Patent Owner makes no arguments specific to limitation 1.2.1. *See, e.g.,* Resp. 14–36; Sur-reply 2–22.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that Stone teaches limitation 1.2.1. *See* Pet. 26–29; Ex. 1003 ¶¶ 95–99.

(d) Limitation 1.2.2

Claim 1 recites “wherein the virtual likeness of the face was selected by the account holder as part of an enrollment.” Ex. 1001, 14:5–7 (limitation 1.2.2).

(i) Petitioner’s Contentions

Petitioner contends that “Stone combined with Hoyos and Varghese” teaches limitation 1.2.2. *See* Pet. 29–32, 70; Reply 11–16. Specifically, Petitioner asserts that Stone discloses:

- (1) “payment provider server 408 may be configured to maintain [a] plurality of user and recipient accounts 422”;
- (2) “the account holder (user 409) registers using user device 404” with payment provider server 408 during an enrollment/registration procedure;
- (3) user account 422 is “established as part of the enrollment/registration procedure”; and
- (4) user identifiers 418 including a “photograph image” selected by the user for display on virtual currency, profile icon, etc.) are generated and stored on user device 404.

Pet. 29–30 (quoting Ex. 1008 ¶ 45); Reply 13–14 (quoting Ex. 1008 ¶ 48) (citing Ex. 1008 ¶¶ 45–46; Ex. 1056 ¶¶ 22–24).

Regarding the “photograph image” in user identifiers 418 and the “personalized currency with the user’s photo,” Petitioner asserts that an ordinarily skilled artisan “would have been motivated to use the sender image selected by the sender during enrollment (stored either in the user device or in the payment provider, whichever design option is chosen), because that image would already be stored in the system.” Reply 14–15. Petitioner explains that using the “already stored image would be understood

to be efficient and reliable and avoid redundancy and unnecessary user effort, compared to a new separate user photo to be provided by the user.” *Id.* at 15 (citing Ex. 1056 ¶ 25). Petitioner also explains using the same user-selected image on the user’s own device and as “an online identity for display for other users” provides “various benefits,” including “providing the sender confirmation that its chosen image is being displayed correctly, consistency between the image shown to the sender and the other users, and increasing the user’s trust in the platform where the sender is ensured that its selected profile image is presented as intended.” *Id.* (citing Ex. 1056 ¶ 25).

Further, Petitioner asserts that “[s]imilar features apply to [a] recipient account holder using recipient device 406.” Pet. 30 (citing Ex. 1003 ¶¶ 101–102; Ex. 1008 ¶¶ 45–46, 48). As support, Petitioner quotes Stone’s disclosure that a recipient may “establish an account with payment provider server 408 so that payment server provider 408 is able to process money transfers from user 409 with payment provider server.” Reply 11 (emphasis omitted) (quoting Ex. 1008 ¶ 46). Petitioner asserts that an ordinarily skilled artisan would have understood that “a selected recipient image, which is associated with the recipient account so established, can be stored on the recipient device 406 and/or the payment provider server 408, and would be provided through network 402” so that “user device 404 may be able to access recipient attributes, such as icon information, for display or use by user device 404.” *Id.* (quoting Ex. 1008 ¶ 46) (citing Ex. 1056 ¶ 22).

Petitioner asserts that Stone’s “user registration/enrollment includes biometric enrollment” and teaches the claimed “enrollment.” Pet. 30. Petitioner asserts that it was well known that the “biometric id” in Stone’s user identifiers 418 “was captured and stored during biometric enrollment.”

Id. Petitioner asserts that “Hoyos and Varghese each disclose biometric authentication.” Reply 15. Petitioner further asserts that “biometric authentication” performs “a comparison based at least in part on the stored biometric information (obtained and stored during [an] enrollment stage) and the captured biometric information” obtained during an authentication stage. *Id.* at 15–16; *see* Pet. 30–31.

Petitioner also asserts that an ordinarily skilled artisan would have understood that:

- (1) “Stone’s electronic transaction system provides a well-known social networking aspect for connecting people”;
- (2) a “user image” was “routinely selected by the account holder as part of user registration/enrollment with a service provider”; and
- (3) “the selected user image is then used for display representing the user online.”

Pet. 31 (citing Ex. 1003 ¶ 105; Ex. 1008 ¶¶ 20, 36, Fig. 2); Reply 13 (citing Ex. 1008 ¶¶ 20, 36, Fig. 2).

Additionally, Petitioner asserts that an ordinarily skilled artisan “would have been motivated to provide a user the selection option to choose images to use as the profile image for display both on its own display and on other users’ display” because doing so allows “the user to select an online identity to connect with others.” Pet. 31–32 (citing Ex. 1003 ¶ 105; Ex. 1009, 1:20–28, 15:15–27); *see* Reply 13 (citing Ex. 1009, 1:20–28, 15:15–27; Ex. 1056 ¶ 23).

(ii) Patent Owner’s Contentions

Patent Owner disputes that Stone teaches limitation 1.2.2. *See* Resp. 30–33; Sur-reply 12–15. In particular, Patent Owner contends that “Stone

does not disclose any enrollment or registration procedure or process, much less an enrollment in which a user selects a photo of themselves.” Resp. 31 (citing Ex. 2032 ¶ 79); *see* Sur-reply 14. According to Patent Owner, Petitioner’s assertion that a “user image” was “routinely selected by the account holder as part of user registration/enrollment with a service provider” constitutes a “hindsight justification to add an enrollment process into Stone’s disclosure.” Resp. 31–32 (citing Ex. 2032 ¶ 79); *see id.* at 33.

Patent Owner contends that the rendered “virtual likeness” required by limitation 1.2.1 and the selected “virtual likeness” required by limitation 1.2.2 must be the same “virtual likeness.” Sur-reply 12. Patent Owner also contends that Petitioner does not identify the same “virtual likeness” for limitations 1.2.1 and 1.2.2. *See id.* at 12–15.

Regarding Stone’s user identifiers 418 including a “photograph image,” Patent Owner asserts that neither the “photograph of a user’s face on the personalized currency” for a sender account holder nor the “picture of the recipient” in name box 202 “is associated with user identifier 418.” Resp. 32; *see* Sur-reply 12–15. Patent Owner asserts that Stone:

- (1) does not disclose “an enrollment process for selecting user identifier 418”;
- (2) does not disclose that “user identifier 418 is displayed in Stone’s interface”;
- (3) does not suggest that “the currency image or recipient photo is the user identifier”; and
- (4) “provides no link between user identifier 418” and “any user likeness displayed in the interface.”

Resp. 32–33 (citing Ex. 2032 ¶ 82); Sur-reply 14–15 (citing Ex. 1008 ¶¶ 40–48).

Patent Owner also asserts that a “user photograph for display in an interface could be selected in a manner of ways,” including after a user creates an account. Resp. 33.

Patent Owner further asserts that Stone “suggests that the user identifier is associated with the device, not a payment account.” Resp. 32. As support, Patent Owner quotes Stone’s disclosure that user device 404 “may include one or more user identifiers 418, which may be implemented, for example, as operating system registry entries, cookies associated with browser application 410, identifiers associated with hardware of user device 404, or various other appropriate identifiers.” *Id.* (quoting Ex. 1008 ¶ 45).

(iii) Analysis

For the reasons explained below, we agree with Petitioner that “Stone combined with Hoyos and Varghese” teaches limitation 1.2.2. *See* Pet. 29–32, 70; Reply 11–16; Ex. 1003 ¶¶ 65, 100–107; Ex. 1056 ¶¶ 22–26.

First, Stone discloses that “payment provider server 408 may be configured to maintain a plurality of user and recipient accounts 422, each of which may include account information 424 associated with individual users, including user 409.” Ex. 1008 ¶ 48; *see* Ex. 1003 ¶ 103. Establishing “an account with payment provider server 408” allows the server to “process money transfers from user 409.” Ex. 1008 ¶ 46; *see* Ex. 1056 ¶ 22. Moreover, account information 424 may include “private financial information of user 409 and recipients, such as one or more account numbers, passwords, credit card information, banking information, or other types of financial information,” that may “facilitate online transactions

between user 409 of user device 404 and one or more recipients.” Ex. 1008 ¶ 48; *see* Inst. Dec. 30 (quoting Ex. 1008 ¶ 48).

Second, Stone discloses that user device 404 “may include one or more user identifiers 418,” such as the following:

- (a) “personal information (e.g., a user name, password, photograph image, biometric id, address, phone number, etc.)”; and
- (b) “banking information (e.g., banking institution, credit card issuer, user account numbers, security information, etc.).”

Ex. 1008 ¶ 45; *see* Ex. 1003 ¶¶ 65, 102. Payment provider server 408 may receive user identifiers 418 from user device 404 and utilize user identifiers 418 to “associate user 409 with a particular user account maintained by payment provider server 408.” Ex. 1008 ¶ 45; *see* Ex. 1003 ¶ 103.

Third, an ordinarily skilled artisan would have understood that user account 422 was “established as part of the enrollment/registration procedure.” Ex. 1056 ¶ 24. Among other things, the skilled artisan would have known that:

- (a) the “biometric id” in Stone’s user identifiers 418 was “captured during an enrollment process” and “used as ‘enrollment data’ for comparison with the later captured data for authentication”; and
- (b) “biometric authentication” performs “a comparison based at least in part on the stored biometric information (obtained and stored during [an] enrollment stage) and the captured biometric information” obtained during an authentication stage.

Ex. 1003 ¶ 104; Ex. 1056 ¶ 26; *see* Ex. 1003 ¶ 101; Ex. 1008 ¶¶ 45–46, 48.

Hence, we disagree with Patent Owner that “Stone does not disclose any

enrollment or registration procedure or process.” *See* Resp. 31; Sur-reply 14.

Fourth, Stone’s user identifiers 418 include not only a “biometric id” but also a “photograph image” selected by the user, e.g., as part of the enrollment/registration procedure. Ex. 1003 ¶ 101; *see* Ex. 1008 ¶ 45.

Fifth, an ordinarily skilled artisan would have been motivated to use the already stored “photograph image” in user identifiers 418 for the “personalized currency with the user’s photo” in the display on user device 404. *See* Ex. 1056 ¶¶ 24–25. Doing so would have been “efficient and reliable” and would have “avoid[ed] redundancy and unnecessary user effort.” *Id.* ¶ 25.

Sixth, if a sender account holder used the already stored “photograph image” in user identifiers 418 for the “personalized currency with the user’s photo” in the display on user device 404, then the rendered “virtual likeness” required by limitation 1.2.1 and the selected “virtual likeness” required by limitation 1.2.2 would be the same “virtual likeness.” *See* Ex. 1056 ¶ 24.

Seventh, Stone discloses that recipient devices 406 “may be the same or have the same basic features as user device 404” and “may include attributes related to the recipient, such as personal and banking information, as well as icon information.” Ex. 1008 ¶ 45; *see* Ex. 1003 ¶ 103. The personal information may include “a user name, password, photograph image, biometric id, address, phone number, etc.” Ex. 1008 ¶ 45; *see* Ex. 1003 ¶¶ 65, 102. The banking information may include “banking institution, credit card issuer, user account numbers, security information, etc.” Ex. 1008 ¶ 45; *see* Ex. 1003 ¶ 65.

Eighth, Stone discloses that “user device 404 may be able to access recipient attributes, such as icon information, for display or use by user device 404.” Ex. 1008 ¶ 46; *see* Ex. 1056 ¶ 22. User device 404 “may visually show other users” when “the user is connected to a network with other users.” Ex. 1008 ¶ 20; *see* Ex. 1003 ¶ 105; Ex. 1056 ¶ 23. Further, “when the recipient is selected, an appropriate icon may appear on the screen, such as a picture of the person.” Ex. 1008 ¶ 36; *see* Ex. 1003 ¶ 105; Ex. 1056 ¶ 23. For instance, Stone’s Figure 2 shows a “picture of the recipient” in name box 202. Ex. 1008 ¶ 24, Fig. 2; Ex. 1003 ¶¶ 98, 148.

Ninth, an ordinarily skilled artisan would have been motivated to use the already stored “photograph image” in user identifiers 418 on the user’s own device and as “an online identity for display for other users.” Ex. 1056 ¶ 25. Doing so provides “various benefits,” including “providing the sender confirmation that its chosen image is being displayed correctly, consistency between the image shown to the sender and the other users, and increasing the user’s trust in the platform where the sender is ensured that its selected profile image is presented as intended.” *Id.*

Tenth, if a recipient account holder used the already stored “photograph image” in user identifiers 418 as “an online identity for display for other users,” e.g., for display in name box 202 on sender user device 404, then the rendered “virtual likeness” required by limitation 1.2.1 and the selected “virtual likeness” required by limitation 1.2.2 would be the same “virtual likeness.” *See* Ex. 1056 ¶ 22.

Eleventh, the “expansive and flexible” obviousness analysis “need not seek out” the “precise” disclosure of a specific feature in a challenged claim because the analysis “can take account of the inferences and creative steps

that a person of ordinary skill in the art would employ.” *KSR*, 550 U.S. at 415, 418. For a particular user, Stone does not disclose multiple different user images stored in multiple different locations. *See* Ex. 1008 ¶¶ 7, 19, 24, 28, 36, 44–46, 48; Tr. 27:12–19. Thus, based on Stone’s disclosures, a person of ordinary skill would have reasonably inferred that:

- (1) a sender would use the “photograph image” in user identifiers 418 on the sender’s user device for the “personalized currency with the user’s photo” on the sender’s user device; and
- (2) a recipient would use the “photograph image” in user identifiers 418 on the recipient’s user device for the recipient’s “icon information” displayed on another’s user device.

See Ex. 1008 ¶¶ 7, 19, 24, 28, 36, 44–46, 48; Ex. 1056 ¶¶ 22–25.

Further, Patent Owner’s assertion that Stone “suggests that the user identifier is associated with the device, not a payment account,” lacks merit. *See* Resp. 32. Stone discloses that payment provider server 408 may receive user identifiers 418 from user device 404 and utilize user identifiers 418 to “associate user 409 with a particular user account maintained by payment provider server 408.” Ex. 1008 ¶ 45; *see* Ex. 1003 ¶ 103.

(e) Limitation 1.3.1

Claim 1 requires a processor configured to “capture contextual information comprising location data usable to determine a physical location associated with the user” subsequent to “an interaction by a user with an icon rendered in the one or more interfaces.” Ex. 1001, 14:8–12 (limitation 1.3.1).

(i) Petitioner's Contentions

Petitioner contends that “Stone in view of Hoyos and Varghese” teaches limitation 1.3.1 for several related reasons. *See* Pet. 32–40; Reply 16–18. Specifically, Petitioner asserts that Stone teaches “an interaction by a user with an icon rendered in the one or more interfaces” because Stone’s Figure 2 illustrates display 200 on an electronic device including the following “control elements” or icons:

- (1) name box 202 “indicating the recipient of funds”;
- (2) funding source box 206 “indicating the source or account where the user’s funds will be transferred from”;
- (3) send button 214 to transfer the funds;
- (4) “\$ Send money” button at the bottom of the display; and
- (5) personalized currency representing the amount to be transferred in the background of the display.

Pet. 32–34. Petitioner asserts that “user interaction with the icon (e.g., clicking, tapping on, dragging/sliding, dragging/sliding to/from) provides an indication that the user initiates, continues, or confirms a transaction request associated with the electronic transaction.” *Id.* at 33 (citing Ex. 1003 ¶ 109); *see id.* at 35 (citing Ex. 1003 ¶ 112).

Further, Petitioner asserts that Stone’s Figure 3 illustrates steps or blocks that an ordinarily skilled artisan would have implemented with icons serving as visual indicators to the user for “various user interactions to continue/confirm the transaction.” Pet. 34 (citing Ex. 1003 ¶ 111; Ex. 1008 ¶¶ 24–25).

Petitioner also asserts that to the extent Stone does not explicitly describe Figure 2’s control elements and Figure 3’s blocks as an “icon,” an ordinarily skilled artisan “would have been motivated to implement the

control items/blocks using an icon, because icon and button are alternative design choices for control elements/blocks, and using icons provides ‘a more visually rich interface.’” Pet. 34–35 (quoting Ex. 1008 ¶ 16) (citing Ex. 1008 ¶¶ 4, 35, 38).

Additionally, Petitioner contends that Varghese discloses that after a user confirms a transaction request (during post-authentication), the system captures “real-time contextual information including capturing real-time location data usable to determine a user physical location for fraud analysis, where the ‘Real-time Analytics & Scoring’ for authentication uses ‘Location Fingerprint’ including ‘IP, Geo-Location, Network Forensics.’” Pet. 35 (emphases omitted) (citing Ex. 1010 ¶¶ 74, 89, 97–99); *see* Reply 17–18. According to Petitioner, Varghese’s real-time location data is “contextual information of the transaction, e.g., a user location from which the transaction request originates.” Pet. 37 (citing Ex. 1003 ¶ 115; Ex. 1010 ¶¶ 81, 140, 142, claim 31).

Also, as discussed above, Petitioner explains that in the proposed combination “real-time multifactor authentication” according to Varghese would occur after a user confirms a transaction request by interacting with an icon rendered in an interface. Pet. 22, 38–40; *see supra* § III.D.5(a)(iii).

(ii) Patent Owner’s Contentions

Patent Owner disputes that “Stone in view of Hoyos and Varghese” teaches limitation 1.3.1. *See* Resp. 33–36; Sur-reply 9–11, 15–20. In particular, Patent Owner contends that Varghese does not disclose collecting location data during post-authentication. Sur-reply 9; *see id.* at 9–11; Resp. 34–36. Patent Owner also contends that location data used for post-authentication in Varghese was already collected for pre-authentication, i.e.,

at login, not newly collected for post-authentication. *See* Sur-reply 9–11, 15–20; Tr. 104:3–5, 104:23–105:3. Therefore, according to Patent Owner, Varghese does not disclose “captur[ing] contextual information comprising location data usable to determine a physical location associated with the user” subsequent to “an interaction by a user with an icon rendered in the one or more interfaces” as required by limitation 1.3.1. Resp. 36 (citing Ex. 2032 ¶¶ 85–87).

Further, Patent Owner asserts that an ordinarily skilled artisan “would not have been motivated to implement Varghese’s location capture at the final step of Petitioner’s Stone-Hoyos-Varghese transaction model because Varghese teaches that the user device’s geolocation would have already been collected at login.” Sur-reply 15.

(iii) Analysis

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that “Stone in view of Hoyos and Varghese” teaches limitation 1.3.1. *See* Pet. 32–40; Reply 16–18; Ex. 1003 ¶¶ 108–120; Ex. 1056 ¶¶ 27–29. Further, for the reasons discussed above about the motivation to combine Varghese’s teachings with the teachings of Stone and Hoyos, we disagree with Patent Owner that location data used for post-authentication in Varghese was already collected for pre-authentication, i.e., at login, not newly collected for post-authentication. *See* Sur-reply 9–11, 15–20; Tr. 104:3–5, 104:23–105:3; *supra* § III.D.5(c)(ii).

(f) Limitation 1.3.2

Claim 1 requires a processor configured to “capture a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images” subsequent to “an interaction by

a user with an icon rendered in the one or more interfaces.” Ex. 1001, 14:8–9, 14:13–15 (limitation 1.3.2).

Petitioner contends that “Stone in view of Hoyos and Varghese” teaches limitation 1.3.2 for several related reasons. *See* Pet. 41–47. Specifically, Petitioner asserts that Stone teaches “an interaction by a user with an icon rendered in the one or more interfaces” for the reasons discussed for limitation 1.3.1. *Id.* at 41.

Petitioner asserts that Hoyos discloses “capturing a set of biometric information for performing biometric authentication including fraud detection (including blocks 11 and 13 of FIG. 1).” Pet. 41 (citing Ex. 1003 ¶ 123; Ex. 1013 ¶ 17). According to Petitioner, the biometric information used for Hoyos’s biometric authentication includes “a set of user facial images (e.g., portion thereof containing a representation of a human eye) captured using a camera (e.g., web-camera 26).” *Id.* at 42 (citing Ex. 1003 ¶ 124; Ex. 1011, code (57); Ex. 1012, code (57); Ex. 1013 ¶¶ 3, 12, 18–22, 40). As support, Petitioner quotes the following limitations in Hoyos’s claim 7: (1) “obtaining [a] first image of a user positioned in front of a computer screen from a first perspective”; and (2) “obtaining a second image of the user positioned in front of the computer screen from a second perspective.” *Id.* at 42–43 (quoting Ex. 1013, claim 7).

Also, as discussed above, Petitioner explains that in the proposed combination biometric authentication according to Hoyos would occur after a user confirms a transaction request by interacting with an icon rendered in an interface. Pet. 18–19, 46; *see supra* § III.D.5(a)(ii).

Patent Owner makes no arguments specific to limitation 1.3.2. *See, e.g.,* Resp. 14–36; Sur-reply 2–22.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that “Stone in view of Hoyos and Varghese” teaches limitation 1.3.2. *See* Pet. 41–47; Ex. 1003 ¶¶ 121–131.

(g) Limitation 1.4.1

Claim 1 requires a processor configured to “facilitate a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed based at least in part” on “the physical location associated with the user determined using the captured location data.” Ex. 1001, 14:16–21 (limitation 1.4.1).

Petitioner contends that “Stone in view of Hoyos and Varghese” teaches limitation 1.4.1. *See* Pet. 47–49. Specifically, Petitioner explains that in the proposed combination Stone’s user device 404 would “capture information including location information and biometric information, and these captured information (e.g., location data usable to determine a physical location associated with the user, the set of biometric information including a set of images) are provided to facilitate a fraud detection analysis.” *Id.* at 47. According to Petitioner, “the fraud detection analysis provides a decision regarding whether the transaction is authenticated/authorized.” *Id.*

Further, Petitioner asserts that Varghese discloses “facilitating and performing fraud detection analysis based at least in part on the physical location associated with the user determined using the captured location data.” Pet. 48 (citing Ex. 1010 ¶¶ 12, 88).

Patent Owner makes no arguments specific to limitation 1.4.1. *See, e.g.,* Resp. 14–36; Sur-reply 2–22.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that “Stone in view of Hoyos and Varghese” teaches limitation 1.4.1. *See* Pet. 47–49; Ex. 1003 ¶¶ 132–135.

(h) Limitation 1.4.2

Claim 1 requires a processor configured to “facilitate a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed based at least in part” on “an analysis of the set of captured biometric information comprising a determination of whether the user is alive based at least in part on an analysis of the set of images captured using the camera.” Ex. 1001, 14:16–19, 14:22–25 (limitation 1.4.2).

Petitioner contends that “Stone in view of Hoyos and Varghese” teaches limitation 1.4.2. *See* Pet. 50–53. Specifically, Petitioner asserts that the combined disclosures in Stone, Hoyos, and Varghese teach (1) “capturing contextual information and a set of captured biometric information” and (2) “facilitating a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed” for the reasons discussed for limitations 1.3.1, 1.3.2, and 1.4.1. *Id.* at 50.

Further, Petitioner asserts that Hoyos discloses “facilitating and performing fraud detection by performing an analysis of the set of captured biometric information.” Pet. 50 (citing Ex. 1003 ¶ 138; Ex. 1013 ¶¶ 17–22, 40, claims 1 and 5–8). Petitioner also asserts that Hoyos’s biometric authentication includes determining whether the user is alive “based at least in part on an analysis of the set of images, including computing the probability, Pp of a live person being presented (e.g., block 11 of FIG. 1)

based on analysis of the set of captured images (e.g., as described with reference to FIGS. 2–4).” *Id.* at 51 (citing Ex. 1003 ¶ 139; Ex. 1013, Fig. 1); *see id.* at 51–52.

Patent Owner makes no arguments specific to limitation 1.4.2. *See, e.g.,* Resp. 14–36; Sur-reply 2–22.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that “Stone in view of Hoyos and Varghese” teaches limitation 1.4.2. *See* Pet. 50–53; Ex. 1003 ¶¶ 136–142.

(i) Limitation 1.5

Claim 1 recites “a memory coupled to the one or more processors and configured to provide the processor with instructions.” Ex. 1001, 14:26–27 (limitation 1.5).

(i) Petitioner’s Contentions

Petitioner contends that Stone teaches limitation 1.5 because Stone discloses “a memory (memory component 506 of FIG. 5) coupled to a processor 504 in each device of the system including e.g., user devices 404.” Pet. 54; *see id.* at 81. Petitioner also contends that “the memory is configured to provide the processor with instructions,” such as “instructions to create and display the proper currencies, convert currency, display various types of graphics showing transfer of currency, etc.” *Id.* at 54. As support, Petitioner quotes Stone’s disclosure that “system 500 performs specific operations by processor 504 executing one or more sequences of one or more instructions contained in system memory component 506.” *Id.* (emphasis omitted) (quoting Ex. 1008 ¶ 50).

(ii) Patent Owner's Contentions

Patent Owner disputes that Stone teaches limitation 1.5. *See* Resp. 14 (citing Ex. 2032 ¶¶ 84–87); Sur-reply 21–22. In particular, Patent Owner contends that Stone does not disclose “one or more processors configured to” accomplish limitations 1.2.2 and 1.3.1 and, therefore, cannot disclose “a memory coupled to the one or more processors and configured to provide the processor with instructions” to accomplish limitations 1.2.2 and 1.3.1. Sur-reply 21.

Patent Owner contends that the claimed “a memory” (a single memory) must provide “instructions” to the “one or more processors” for causing the “one or more processors” to perform each of limitations 1.2.1–1.4.2. Sur-reply 22 (citing Ex. 1050, 59:3–8). Patent Owner also contends that the memory in Stone’s user device 404 does not provide:

- (1) “any instructions to the payment provider server 408 where the association” required by limitation 1.2.1 “occurs in Petitioner’s server-side model”; or
- (2) “the necessary instructions to perform” each of limitations 1.2.1–1.4.2 in Petitioner’s client-side model because the processor in Stone’s user device 404 “does not perform these limitations.”

Id.

(iii) Analysis

For the reasons explained below, we agree with Petitioner that Stone teaches limitation 1.5. *See* Pet. 53–54; Ex. 1003 ¶¶ 143–146.

First, we disagree with Patent Owner that a single memory must provide “instructions” to the “one or more processors” for causing the “one or more processors” to perform each of limitations 1.2.1–1.4.2. *See* Sur-reply 22. Limitation 1.5 recites “a memory coupled to the one or more

processors and configured to provide the processor with instructions.”
Ex. 1001, 14:26–27. The “indefinite article ‘a’ or ‘an’ in patent parlance carries the meaning of ‘one or more’ in open-ended claims containing the transitional phrase ‘comprising.’” *KCJ Corp. v. Kinetic Concepts, Inc.*, 223 F.3d 1351, 1356 (Fed. Cir. 2000). “That ‘a’ or ‘an’ can mean ‘one or more’ is best described as a rule, rather than merely as a presumption or even a convention.” *Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1342 (Fed. Cir. 2008). “The subsequent use of definite articles ‘the’ or ‘said’ in a claim to refer back to the same claim term does not change the general plural rule, but simply reinvokes that non-singular meaning.” *Id.* “The exceptions to this rule are extremely limited: a patentee must evince a clear intent to limit ‘a’ or ‘an’ to ‘one.’” *01 Communique Lab’y, Inc. v. LogMeIn, Inc.*, 687 F.3d 1292, 1297 (Fed. Cir. 2012).

Patent Owner identifies nothing in the intrinsic evidence demonstrating a “clear intent” to limit “a” memory in claim 1 to “one” memory. *See* Resp. 14; Sur-reply 21–22. For example, limitations 1.2.1–1.4.2 do not reference “the” or “said” memory in limitation 1.5. *See* Ex. 1001, 14:4–25. So the claim language does not indicate that “a” memory means “one” memory. Nor does the patent’s specification indicate that “a” memory means “one” memory. *See, e.g., id.* at 2:6–20. Absent “an express intent to impart a novel meaning” to claim language, “the words are presumed to take on the ordinary and customary meanings attributed to them by those of ordinary skill in the art.” *Brookhill-Wilk 1, LLC v. Intuitive Surgical, Inc.*, 334 F.3d 1294, 1298 (Fed. Cir. 2003); *see Sigray, Inc. v. Carl Zeiss X-Ray Microscopy, Inc.*, 137 F.4th 1372, 1379 (Fed. Cir. 2025).

Second, Stone discloses system 500 suitable for implementing “user device 404, one or more recipient devices 406, and payment processing device 408.” Ex. 1008 ¶ 49, Fig. 5; *see* Ex. 1003 ¶ 91. System 500 “performs specific operations by processor 504 executing one or more sequences of one or more instructions contained in system memory component 506.” Ex. 1008 ¶ 50; *see* Ex. 1003 ¶ 145. The “instructions may be read into system memory component 506 from another computer readable medium, such as static storage component 508.” Ex. 1008 ¶ 50; *see* Ex. 1003 ¶ 145. The instructions may cause the processor to “create and display the proper currencies, convert currency, display various types of graphics showing transfer of currency, etc.” Ex. 1008 ¶ 50; *see* Ex. 1003 ¶ 145.

Third, for the reasons discussed above, the combined disclosures in Stone, Hoyos, and Varghese teach limitations 1.2.1–1.4.2 performed by “one or more processors” according to limitation 1.1. *See supra* §§ III.D.6(b)–(h). To permit the “one or more processors” to perform limitations 1.2.1–1.4.2, one or more memories in the proposed Stone-Hoyos-Varghese combination provide the “one or more processors” with instructions. *See* Ex. 1003 ¶¶ 144–146. For instance, in each of sender user device 404, recipient device 406, and payment provider server 408, “processor 504 execut[es] one or more sequences of one or more instructions contained in system memory component 506.” Ex. 1008 ¶¶ 49–50; *see* Ex. 1003 ¶¶ 91, 145. Hence, in the proposed Stone-Hoyos-Varghese combination implementing either client-side authentication or server-side authentication, one or more memories provide the “one or more processors” with instructions to perform limitations 1.2–1.8. *See* Ex. 1003 ¶¶ 144–146.

Fourth, even if claim 1 required that one processor perform each of limitations 1.2.1–1.4.2 according to instructions provided by one memory, the combined disclosures in Stone, Hoyos, and Varghese teach that arrangement. Specifically, if authentication according to Hoyos and Varghese occurs on Stone’s user device 404, then processor 504 in user device 404 performs each of limitations 1.2.1–1.4.2 according to instructions provided by memory component 506 in user device 404. *See supra* §§ III.D.6(b)–(h).

Regarding the “association” required by limitation 1.2.1, Stone discloses that user device 404 may include “one or more user identifiers 418,” such as (1) “personal information (e.g., a user name, password, photograph image, biometric id, address, phone number, etc.)” and (2) “banking information (e.g., banking institution, credit card issuer, user account numbers, security information, etc.).” Ex. 1008 ¶ 45; *see* Ex. 1003 ¶¶ 65, 102. Hence, user identifiers 418 in sender user device 404 contain an “association” for a sender between a “photograph image” corresponding to the claimed “virtual likeness” and a “user name” with “user account numbers” corresponding to the claimed “account holder.”

Additionally, user identifiers 418 in recipient device 406 contain the same “association” for a recipient because Stone discloses that recipient device 406 “may be the same or have the same basic features as user device 404” and “may include attributes related to the recipient, such as personal and banking information, as well as icon information.” Ex. 1008 ¶ 46; *see* Ex. 1003 ¶¶ 87, 103.

(j) Conclusion Concerning Obviousness/Nonobviousness for Claim 1

For the reasons discussed above, the combined disclosures in Stone, Hoyos, and Varghese teach claim 1's subject matter. *See supra* §§ III.D.6(a)–(i). Moreover, an ordinarily skilled artisan would have been motivated to combine the teachings of Stone, Hoyos, and Varghese in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.D.5(c). Hence, Petitioner has shown by a preponderance of the evidence that claim 1 is unpatentable under § 103(a) because the claim would have been obvious over Stone, Hoyos, and Varghese.

7. INDEPENDENT CLAIMS 6 AND 11

Claim 6 recites a “method” in its preamble and includes limitations similar to claim 1. *Compare* Ex. 1001, 14:2–27 (claim 1), *with id.* at 14:39–61 (claim 6). Claim 11 recites a “computer program product embodied in a non-transitory computer readable storage medium” in its preamble and includes limitations similar to claim 1. *Compare id.* at 14:2–27 (claim 1), *with id.* at 15:6–31 (claim 11).

Petitioner identifies disclosures in Stone corresponding to claim 6's preamble and claim 11's preamble. Pet. 60–62. For a “method” according to claim 6's preamble, Petitioner asserts that Stone's Figure 3 illustrates steps in a “method for fund transfer.” *Id.* at 60–61 (citing Ex. 1008 ¶¶ 29–36, Fig. 3). For a “computer program product embodied in a non-transitory computer readable storage medium” according to claim 11's preamble, Petitioner asserts that Stone discloses software including computer program code in a computer program product embodied in a

memory configured to provide one or more processors with instructions. *Id.* at 62 (citing Ex. 1003 ¶ 178; Ex. 1008 ¶ 54).

Patent Owner makes no arguments specific to claim 6's preamble or claim 11's preamble. *See, e.g.*, Resp. 14–37, 30 n.1; Sur-reply 2–23, 12 n.1, 15 n.2.

Generally, a preamble does not limit a claim. *Allen Eng'g*, 299 F.3d at 1346. We need not decide whether the preambles in claims 6 and 11 limit the claims because, for the reasons stated by Petitioner and supported by Dr. Jones's testimony, we agree with Petitioner that Stone teaches the preambles in claims 6 and 11. *See* Pet. 60–62; Ex. 1003 ¶¶ 164–166, 177–179.

Additionally, Petitioner contends that the combined disclosures in Stone, Hoyos, and Varghese teach the subject matter in claims 6 and 11 for the reasons that the combined disclosures teach claim 1's subject matter. *See* Pet. 61–63. Dr. Jones's testimony supports Petitioner's contentions. *See* Ex. 1003 ¶¶ 167–172, 180–185.

Patent Owner disputes that the combined disclosures in Stone, Hoyos, and Varghese teach the subject matter in claims 6 and 11 for the same reasons Patent Owner disputes that the combined disclosures teach claim 1's subject matter. *See* Resp. 14–37, 30 n.1; Sur-reply 2–23, 12 n.1, 15 n.2.

For the reasons discussed above, we consider Patent Owner's patentability arguments about claim 1 unavailing. *See supra* §§ III.D.5(c), III.D.6(d)(iii), III.D.6(e)(iii), III.D.6(i)(iii). For (1) the reasons stated by Petitioner and supported by Dr. Jones's testimony and (2) the reasons discussed above for claim 1, we agree with Petitioner that the combined disclosures in Stone, Hoyos, and Varghese teach the subject matter in

claims 6 and 11. *See* Pet. 60–63; Ex. 1003 ¶¶ 164–172, 177–185; *supra* §§ III.D.6(a)–(i). Moreover, an ordinarily skilled artisan would have been motivated to combine the teachings of Stone, Hoyos, and Varghese in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.D.5(c). Hence, Petitioner has shown by a preponderance of the evidence that claims 6 and 11 are unpatentable under § 103(a) because the claims would have been obvious over Stone, Hoyos, and Varghese.

8. DEPENDENT CLAIMS 2–5, 7–10, 12, 14–18, AND 20–23

(a) Claims 2 and 7

Claim 2 depends directly from claim 1 and specifies that (1) “the account holder comprises a recipient of the electronic transaction” and (2) “the electronic transaction comprises a payment from the user to the account holder.” Ex. 1001, 14:28–31. Claim 7 depends directly from claim 6 and includes limitations similar to claim 2. *Id.* at 14:62–65.

Petitioner contends that Stone teaches the limitations in claims 2 and 7 because Stone’s Figure 2 illustrates display 200 on an electronic device including:

- (1) name box 202 “indicating the recipient of funds”;
- (2) a “picture of the recipient” in name box 202;
- (3) funds box 204 “indicating the amount of funds to be transferred”; and
- (4) “send button 214 to transfer the funds [as] noted in [funds] box 204.”

Pet. 54–55, 62.

As support, Petitioner provides the following annotated version of Stone's Figure 2 (Pet. 55):

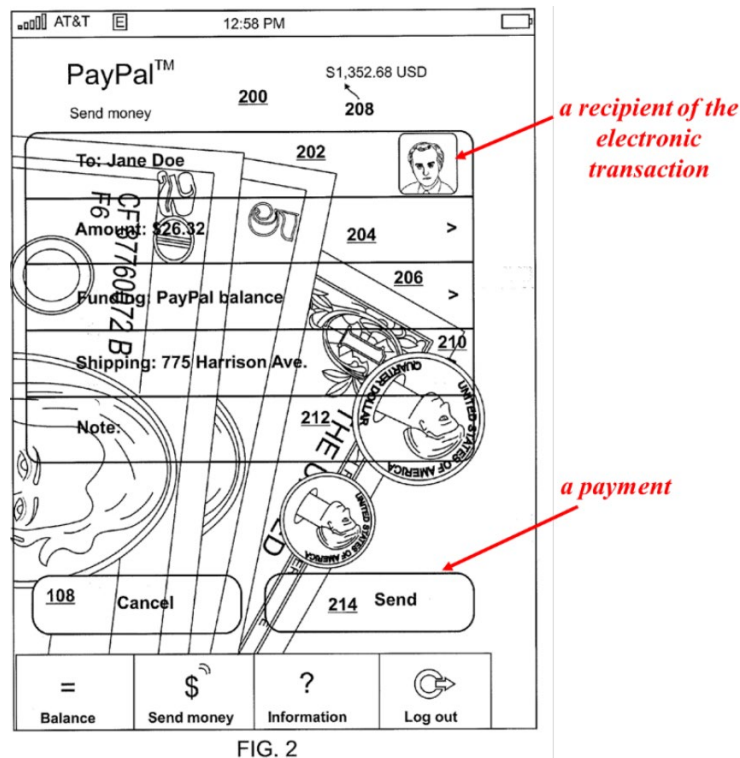


Figure 2 illustrates display 200 on an electronic device including various display elements. Ex. 1008 ¶¶ 11, 24, Fig. 2. The above annotated version of Figure 2 includes the red annotation “a recipient of the electronic transaction” identifying the “picture of the recipient” in name box 202 and the red annotation “a payment” identifying send button 214. Pet. 55; *see* Ex. 1003 ¶ 148; Ex. 1008 ¶¶ 24–25.

Patent Owner makes no arguments specific to claims 2 and 7. *See, e.g.,* Resp. 36–37; Sur-reply 23.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that Stone teaches the limitations in claims 2 and 7. *See* Pet. 54–55, 62; Ex. 1003 ¶¶ 147–149, 173.

(b) Claims 3 and 8

Claim 3 depends directly from claim 1 and specifies that “the icon represents a form of payment.” Ex. 1001, 14:32–33. Claim 8 depends directly from claim 6 and includes a limitation similar to claim 3. *Id.* at 14:66–67.

(i) Petitioner’s Contentions

Petitioner contends that Stone teaches the limitations in claims 3 and 8 because Stone discloses:

- (1) funding source box 206 in Figure 2 corresponding to the claimed “icon”;
- (2) step 314 for “Enter Funding Source” in Figure 3 related to funding source box 206 in Figure 2;
- (3) “interaction by a user” with funding source box 206 when the user “clicks on” funding source box 206 to “make a transfer from a selected funding source”; and
- (4) the user “confirm[ing] the transaction” by “tapping an appropriate button” so that “the shown funds are transferred to the desired recipient” in step 318 for “Transfer Funds” in Figure 3.

Pet. 55–57, 62 (emphasis omitted) (quoting Ex. 1008 ¶ 35) (citing Ex. 1008 ¶¶ 4, 24, 34, Fig. 2); *see* Reply 19 (citing Ex. 1056 ¶ 32). Further, Petitioner asserts that funding source box 206 may represent “a form of payment,” such as “PayPal, a bank, a credit card, a debit card, etc.” Pet. 56 (quoting Ex. 1008 ¶ 34).

Additionally, Petitioner contends that Stone teaches “using a visual image to present the selected funding source in the display” because Stone discloses that a user device may display “the specific card, such as a PayPal card, Visa, MC, AMEX, etc., as contrasted to a generic representation of a

card or no visual at all.” Pet. 57 (emphasis omitted) (quoting Ex. 1008 ¶ 38); Reply 19 (quoting Ex. 1008 ¶ 38) (citing Ex. 1056 ¶ 33).

Petitioner asserts that it “would have been obvious to” an ordinarily skilled artisan to “implement the funding source selection using an icon with the visual representation of the payment for improved visual presentation.” Pet. 57 (citing Ex. 1003 ¶ 152; Ex. 1008 ¶ 4); *see* Reply 20 (citing Ex. 1056 ¶ 34).

Further, referencing Stone’s Figure 3 with step 300 for “Select Currency for Display” and step 302 for “Select Currency to Be Entered,” Petitioner asserts that an ordinarily skilled artisan “would have been motivated to use an icon of a form of payment (e.g., type of currency) to provide a visual indication to assist the user to select a currency” at step 300 and/or step 302. Pet. 58; *see* Reply 20 (citing Ex. 1056 ¶ 35).

(ii) Patent Owner’s Contentions

Patent Owner disputes that Stone teaches the limitations in claims 3 and 8. *See* Resp. 36–37; Sur-reply 23. In particular, Patent Owner contends that “Stone and Hoyos do not disclose that a transaction icon can be that of a payment form.” Resp. 36 (citing Ex. 2032 ¶ 89).

Patent Owner also contends that Petitioner provides “no explanation or justification why” it would have been obvious to an ordinarily skilled artisan to “implement the funding source selection [of Stone Fig. 2] using an icon” representing “a form of payment” without working “backward” from the claims using hindsight. Resp. 37 (alteration by Patent Owner) (quoting Pet. 57) (citing Ex. 2032 ¶ 89); *see* Sur-reply 23.

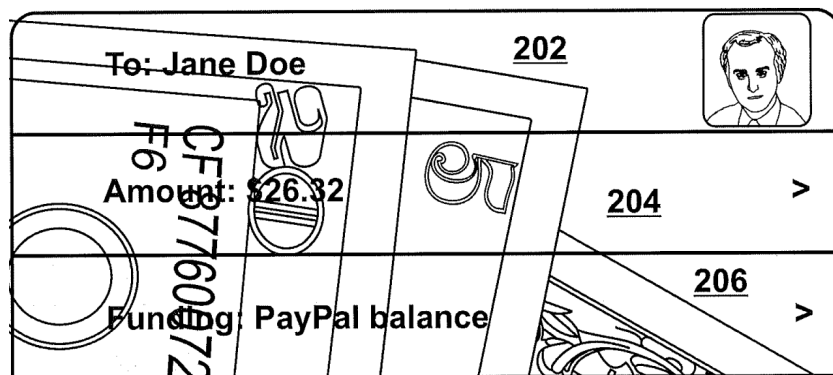
Further, regarding Stone’s Figure 3 with step 300 for “Select Currency for Display” and step 302 for “Select Currency to Be Entered,”

Patent Owner asserts that Petitioner’s justification for using “an icon of a form of payment” is “conclusory and rooted in hindsight bias.” Resp. 37 (citing Ex. 2032 ¶ 90).

(iii) Analysis

We agree with Petitioner that Stone teaches the limitations in claims 3 and 8. *See* Pet. 55–58; Reply 18–20; Ex. 1003 ¶¶ 150–154, 174; Ex. 1056 ¶¶ 31–35. Specifically, Stone’s Figure 2 illustrates display 200 on an electronic device including, among other things, funding source box 206 corresponding to the claimed “icon.” Ex. 1008 ¶ 24, Fig. 2; *see* Ex. 1003 ¶ 152; Ex. 1056 ¶ 32. As representative funding sources, Stone identifies “PayPal, a bank, a credit card, a debit card, etc.” Ex. 1008 ¶ 34; *see* Ex. 1003 ¶ 152. Additionally, Stone discloses that a user device may display “the specific card, such as a PayPal card, Visa, MC, AMEX, etc., as contrasted to a generic representation of a card or no visual at all.” Ex. 1008 ¶ 38; *see* Ex. 1003 ¶ 152; Ex. 1056 ¶ 33. When funding source box 206 displays “the specific card, such as a PayPal card, Visa, MC, AMEX, etc.,” “the icon represents a form of payment” according to claims 3 and 8. *See* Ex. 1003 ¶ 152; Ex. 1056 ¶¶ 32–33.

For example, the following excerpt from Stone’s Figure 2 shows that funding source box 206 contains “a form of payment”:



The above excerpt from Stone’s Figure 2 illustrates (1) name box 202 “indicating the recipient of funds” with a “picture of the recipient” in name box 202, (2) funds box 204 “indicating the amount of funds to be transferred,” and (3) funding source box 206 “indicating the source or account where the user’s funds will be transferred from” with the words “Funding” and “PayPal balance” in funding source box 206. Ex. 1008 ¶ 24, Fig. 2. The words “PayPal balance” constitute “a form of payment” according to claims 3 and 8.

We disagree with Patent Owner that Petitioner worked “backward” from the claims using hindsight. *See* Resp. 37; Sur-reply 23. Petitioner provides an explicit analysis about how Stone teaches the limitations in claims 3 and 8 by disclosing (1) funding source box 206 and (2) specific payment forms for funding source box 206, “such as a PayPal card, Visa, MC, AMEX, etc.” *See* Pet. 56–58; Reply 19; Ex. 1003 ¶ 152; Ex. 1056 ¶¶ 32–33.

(c) Claims 4 and 9

Claim 4 depends directly from claim 1 and specifies that “the image comprises at least one of a photograph or an avatar.” Ex. 1001, 14:34–35. Claim 9 depends directly from claim 6 and includes a limitation similar to claim 4. *Id.* at 15:1–2.

Petitioner contends that the combined disclosures in Stone, Hoyos, and Varghese teach the limitations in claims 4 and 9. *See* Pet. 58–59, 62. To “the extent that ‘the image’ is ‘a virtual likeness of a face’” according to limitation 1.2.1, Petitioner contends that Stone discloses “personalized currency with the user’s photo” and a “picture of the recipient” in name box 202 displayed on a user device. *Id.* at 59 (citing Ex. 1003 ¶ 158;

Ex. 1008 ¶¶ 7, 20, 24, 36). To “the extent that ‘the image’ is of ‘a set of images’” according to limitation 1.3.2, Petitioner contends that Hoyos discloses web-camera 26 capturing a set of photographs of a user. *Id.* (citing Ex. 1003 ¶ 157; Ex. 1013 ¶ 34, Fig. 2).

Further, Petitioner asserts that an ordinarily skilled artisan “would have been motivated to implement the virtual likeness in Stone-Hoyos-Varghese using an avatar, because an avatar and a photo were well-known alternative choices for the profile image.” Pet. 59 (citing Ex. 1003 ¶ 159; Ex. 1009, 9:30–35).

Patent Owner makes no arguments specific to claims 4 and 9. *See, e.g.*, Resp. 36–37; Sur-reply 23.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that the combined disclosures in Stone, Hoyos, and Varghese teach the limitations in claims 4 and 9. *See* Pet. 58–59, 62; Ex. 1003 ¶¶ 155–160, 175.

(d) Claims 5 and 10

Claim 5 depends directly from claim 1 and specifies that “the one or more interfaces are associated with at least one of a phone, a tablet device, or a laptop.” Ex. 1001, 14:36–38. Claim 10 depends directly from claim 6 and includes a limitation similar to claim 5. *Id.* at 15:3–5.

Petitioner contends that Stone teaches the limitations in claims 5 and 10 because Stone’s system includes “user devices of different types (‘mobile phone, laptop computer, PDA, or personal computer,’ or ‘other suitable device’) for displaying the interfaces.” Pet. 59–60, 62 (quoting Ex. 1008 ¶¶ 4, 22) (citing Ex. 1008 ¶¶ 24, 41, 44, 46).

Patent Owner makes no arguments specific to claims 5 and 10. *See, e.g.,* Resp. 36–37; Sur-reply 23.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that Stone teaches the limitations in claims 5 and 10. *See* Pet. 59–60, 62; Ex. 1003 ¶¶ 161–163, 176.

(e) Claims 12 and 18

Claim 12 depends directly from claim 1 and specifies that “the analysis of the set of images captured using the camera further comprises determining whether a face is detected in the captured set of images.” Ex. 1001, 15:32–35. Claim 18 depends directly from claim 6 and includes a limitation similar to claim 12. *Id.* at 16:16–19.

Petitioner contends that the combined disclosures in Stone, Hoyos, and Varghese teach the limitations in claims 12 and 18. *See* Pet. 63. Specifically, Petitioner asserts that Hoyos “discloses that the analysis of the set of images includes determining whether a face is detected therein, because its authentication uses a face recognition match score.” *Id.* (citing Ex. 1003 ¶¶ 187–188; Ex. 1013 ¶¶ 22, 38, claim 7; Ex. 1017). Additionally, Petitioner asserts that it “would have been obvious to” an ordinarily skilled artisan to “implement face recognition as an additional authentication technique in Stone-Hoyos-Varghese for imp[r]oved security, where ‘the face biometric is easy to acquire (a web camera for example).’” *Id.* (quoting Ex. 1013 ¶ 7) (citing Ex. 1003 ¶ 189; Ex. 1010 ¶ 145; Ex. 1013 ¶ 3; Ex. 1016 ¶ 42, Fig. 4; Ex. 1037, 11).

Patent Owner makes no arguments specific to claims 12 and 18. *See, e.g.,* Resp. 36–37; Sur-reply 23.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that the combined disclosures in Stone, Hoyos, and Varghese teach the limitations in claims 12 and 18. *See* Pet. 63; Ex. 1003 ¶¶ 186–190.

(f) Claims 14 and 20

Claim 14 depends directly from claim 1 and specifies that “the set of images comprises a plurality of images successively captured using the camera.” Ex. 1001, 16:1–3. Claim 20 depends directly from claim 6 and includes a limitation similar to claim 14. *Id.* at 16:24–26.

Petitioner contends that the combined disclosures in Stone, Hoyos, and Varghese teach the limitations in claims 14 and 20. *See* Pet. 64. Specifically, Petitioner asserts that Hoyos “describes that the set of images are successively captured using the camera at successive times T1 and T2.” *Id.* As support, Petitioner cites Hoyos’s Figures 3 and 4 (reproduced below):

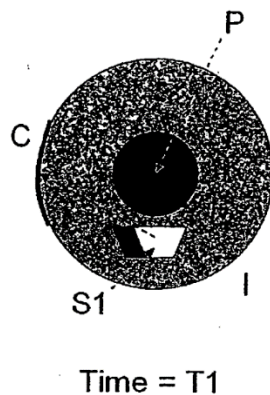


Fig. 3

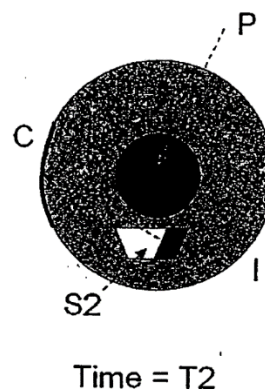


Fig. 4

Figures 3 and 4 “represent cornea C with pupil P and section S1 at time T1 and S2 at time T2, with I representing an iris.” Ex. 1013 ¶ 36, Figs. 3–4; *see* Pet. 64; Ex. 1003 ¶ 192.

Additionally, Petitioner asserts that an ordinarily skilled artisan “would have implemented the image captures to continue one after the other for improved spoofing, accuracy, and reduced delay in user experience.” Pet. 64 (citing Ex. 1003 ¶ 192; Ex. 1013 ¶¶ 18–20, 36, claims 5–8).

Patent Owner makes no arguments specific to claims 14 and 20. *See, e.g.,* Resp. 36–37; Sur-reply 23.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that the combined disclosures in Stone, Hoyos, and Varghese teach the limitations in claims 14 and 20. *See* Pet. 64; Ex. 1003 ¶¶ 191–193.

(g) Claims 15 and 21

Claim 15 depends directly from claim 1 and specifies that “the set of captured biometric information further comprises an audio sample.” Ex. 1001, 16:4–6. Claim 21 depends directly from claim 6 and includes a limitation similar to claim 15. *Id.* at 16:27–28.

Petitioner contends that the combined disclosures in Stone, Hoyos, and Varghese teach the limitations in claims 15 and 21. *See* Pet. 65–66. In particular, Petitioner asserts that Varghese “describes multifactor authentication including voice authentication, which includes capturing an audio sample.” *Id.* at 65 (citing Ex. 1010 ¶¶ 78–79, 84, Fig. 14; Ex. 1033, Fig. 3). Petitioner also asserts that an ordinarily skilled artisan “would have been motivated to implement the multifactor authentications with an additional voice authentication for improved security based on assessed risk of a transaction.” *Id.* at 65–66 (citing Ex. 1003 ¶ 196; Ex. 1010 ¶ 145; Ex. 1016 ¶¶ 36, 40–41, Fig. 4; Ex. 1018, 51:12–15, 52:20–24).

Patent Owner makes no arguments specific to claims 15 and 21. *See, e.g.,* Resp. 36–37; Sur-reply 23.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that the combined disclosures in Stone, Hoyos, and Varghese teach the limitations in claims 15 and 21. *See* Pet. 65–66; Ex. 1003 ¶¶ 194–197.

(h) Claims 16 and 22

Claim 16 depends directly from claim 15 and specifies that “facilitating the fraud detection analysis to determine whether the electronic transaction associated with the account holder is allowed to proceed is further based at least in part on a determination of whether the audio sample matches a previously recorded voice sample.” Ex. 1001, 16:7–12. Claim 22 depends directly from claim 21 and includes a limitation similar to claim 16. *Id.* at 16:29–34.

Petitioner contends that the combined disclosures in Stone, Hoyos, and Varghese teach the limitations in claims 16 and 22 because an ordinarily skilled artisan would have known that “biometric authentication (including voice authentication) makes an accept/reject decision based on a determination of whether there is a match between a captured sample (e.g., a voice sample) and a previously captured reference (e.g., a previously recorded voice sample).” Pet. 66 (citing Ex. 1003 ¶¶ 199–200; Ex. 1010 ¶ 145; Ex. 1016 ¶¶ 36, 40–41; Ex. 1018, 51:12–15; Ex. 1033, Fig. 3).

Patent Owner makes no arguments specific to claims 16 and 22. *See, e.g.,* Resp. 36–37; Sur-reply 23.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that the combined disclosures in Stone,

Hoyos, and Varghese teach the limitations in claims 16 and 22. *See* Pet. 66; Ex. 1003 ¶¶ 198–201.

(i) Claims 17 and 23

Claim 17 depends directly from claim 16 and specifies that “the determination of whether the audio sample matches the previously recorded voice sample is based at least in part on performing a Fast Fourier Transform.” Ex. 1001, 16:12–15. Claim 23 depends directly from claim 22 and includes a limitation similar to claim 17. *Id.* at 16:35–38.

Petitioner contends that the combined disclosures in Stone, Hoyos, and Varghese teach the limitations in claims 17 and 23 because:

- (1) a Fast Fourier Transform (FFT) was a fundamental, highly efficient, and well-known technique for “matching audio samples” for “voice authentication” by “converting the time-domain audio signal into the frequency domain for comparing frequency domain features of the audio samples”; and
- (2) “it would have been obvious to” an ordinarily skilled artisan to “determine whether the audio samples match based on performing an FFT.”

Pet. 66–67 (citing Ex. 1003 ¶ 203; Ex. 1031, 12:15–19; Ex. 1032, Fig. 2; Ex. 1033, 1445).⁷

Patent Owner makes no arguments specific to claims 17 and 23. *See, e.g.,* Resp. 36–37; Sur-reply 23.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that the combined disclosures in Stone,

⁷ For Exhibit 1033 (Campbell), we follow Petitioner’s practice and cite to the page numbers that appear in the publication instead of the page numbers that Petitioner applied to the exhibit.

Hoyos, and Varghese teach the limitations in claims 17 and 23. *See* Pet. 66–67; Ex. 1003 ¶¶ 202–204.

(j) Summary for Dependent Claims 2–5, 7–10, 12, 14–18, and 20–23

For the reasons discussed above, the combined disclosures in Stone, Hoyos, and Varghese teach the limitations in claims 2–5, 7–10, 12, 14–18, and 20–23. *See supra* §§ III.D.8(a)–(i). Moreover, an ordinarily skilled artisan would have been motivated to combine the teachings of Stone, Hoyos, and Varghese in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.D.5(c). Hence, Petitioner has shown by a preponderance of the evidence that claims 2–5, 7–10, 12, 14–18, and 20–23 are unpatentable under § 103(a) because the claims would have been obvious over Stone, Hoyos, and Varghese.

*E. Petitioner’s Other Patentability Challenges:
Claims 1–12, 14–18, and 20–23*

As noted above, Petitioner presents other challenges to the patentability of claims 1–12, 14–18, and 20–23, e.g., based on Stone and the Guidance. *See supra* § II.G.

For the reasons discussed above, the challenge based on Stone, Hoyos, and Varghese resolves the patentability questions for claims 1–12, 14–18, and 20–23 favorable to Petitioner. *See supra* §§ III.D.5–III.D.8. Hence, we need not reach Petitioner’s other patentability challenges. *See SAS Inst. Inc. v. Iancu*, 584 U.S. 357, 371 (2018) (holding that a petitioner “is entitled to a final written decision addressing all of the claims it has challenged”); *Bos. Sci. Scimed, Inc. v. Cook Grp. Inc.*, 809 F. App’x 984, 990 (Fed. Cir. 2020) (agreeing that the Board “need not address issues that are not necessary to the resolution of the proceeding”).

IV. CONCLUSION

Based on the evidence presented with the Petition, the evidence introduced during the trial, and the parties' respective arguments, Petitioner has shown by a preponderance of the evidence that claims 1–12, 14–18, and 20–23 are unpatentable under § 103(a) because the claims would have been obvious over Stone, Hoyos, and Varghese.

In summary:⁸

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1–12, 14–18, 20–23	103(a)	Stone, Hoyos, Varghese	1–12, 14–18, 20–23	
1–12, 14–18, 20–23	103(a)	Stone, Guidance ⁹		

⁸ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding after the issuance of this Final Written Decision, we draw Patent Owner's attention to the April 2019 Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. §§ 42.8(a)(3), (b)(2).

⁹ In view of our determination that claims 1–12, 14–18, and 20–23 are unpatentable based on the Stone-Hoyos-Varghese challenge, we do not reach this challenge to those claims. *See supra* § III.E.

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
15–17, 21–23	103(a)	Stone, Hoyos, Varghese, Campbell ¹⁰		
15–17, 21–23	103(a)	Stone, Guidance, Campbell ¹¹		
Overall Outcome			1–12, 14–18, 20–23	

V. ORDER

Accordingly, it is

ORDERED that claims 1–12, 14–18, and 20–23 in the '886 patent are determined to be unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, the parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

¹⁰ In view of our determination that claims 15–17 and 21–23 are unpatentable based on the Stone-Hoyos-Varghese challenge, we do not reach this challenge to those claims. *See supra* § III.E.

¹¹ In view of our determination that claims 15–17 and 21–23 are unpatentable based on the Stone-Hoyos-Varghese challenge, we do not reach this challenge to those claims. *See supra* § III.E.

IPR2024-00331
Patent 11,526,886 B1

For PETITIONER:

David W. O'Brien
Hong Shi
Kelly Lyle
HAYNES AND BOONE, LLP
david.obrien.ipr@haynesboone.com
hong.shi.ipr@haynesboone.com
kelly.lyle.ipr@haynesboone.com

For PATENT OWNER:

Richard A. Kamprath
George Fishback
Bradley Jarrett
McKOOL SMITH, P.C.
rkamprath@mckoolsmith.com
gfishback@mckoolsmith.com
bjarrett@mckoolsmith.com
Carbyne_Apple@mckoolsmith.com