

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner

Case No. IPR2024-00329
Patent No. 9,972,010

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 29,), and from all underlying findings, determinations, rulings, opinions, orders, issues, and decisions regarding the *inter partes* review of United States Patent No. 9,972,010 B1 (“the ’010 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, 2, 4-7, 9, 10, 12-15, 17, and 20 - 23 of the '010 patent were shown to be anticipated and 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.

IPR2024-00329
Patent 9,972,010 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, 2, 4–7, 9, 10, 12–15, 17, and 20–23 in U.S. Patent No. 9,972,010 B1 (“the ’010 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, 2, 4–7, 9, 10, 12–15, 17, and 20–23 in the ’010 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 '010 Patent (Exhibit 1001)

The '010 patent, titled “Method, Medium, and System for Reducing Fraud,” issued on May 15, 2018, from an application filed on May 1, 2013. Ex. 1001, codes (22), (45), (54). The patent identifies that application as a continuation of an application filed on May 3, 2011. *Id.* at 1:7–11, code (63).

The '010 patent describes fraudulent electronic transactions as “an ongoing problem.” Ex. 1001, 1:19. 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 1:24–27.

The '010 patent's Figure 1 (reproduced below) depicts an example of an electronic environment where fraudulent transactions may occur:

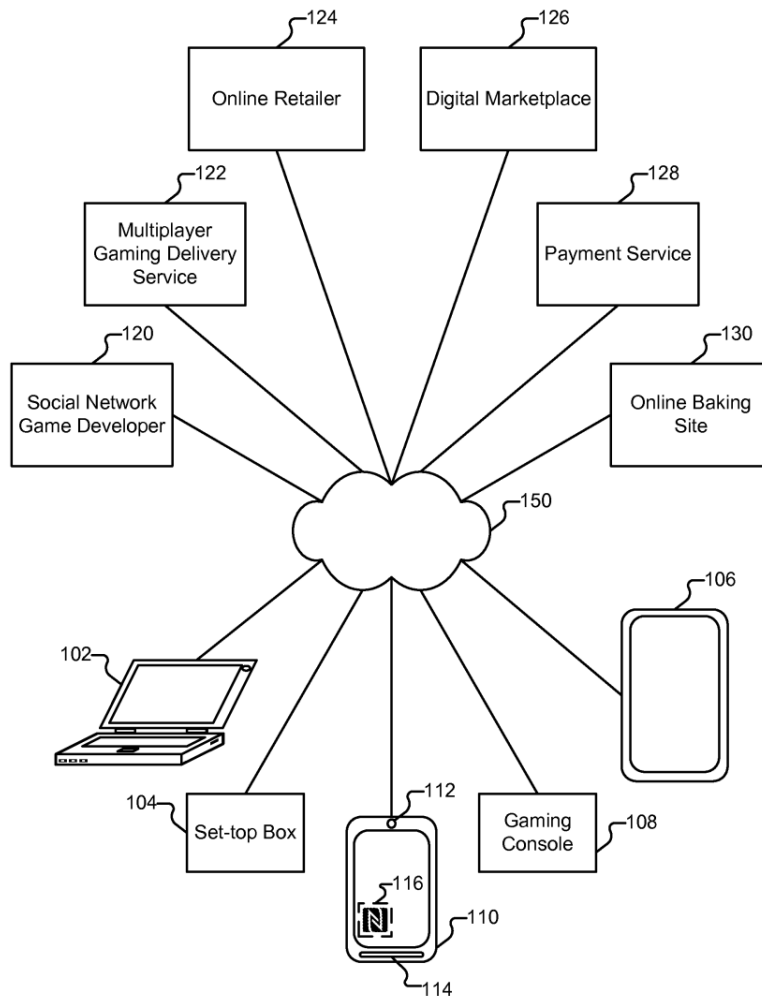


FIG. 1

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, 1:36–37, 2:28–29, 2:39–42, 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 2:54–4:3, 13:19–20, Fig. 1. Mobile telephone 110 includes front-facing camera 112,

microphone 114, and near-field-communication (NFC) chip 116. *Id.* at 3:53–56, 13:19–20, 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, 2:59–62. 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 3:1–4. 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 3:45–49.

“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, 4:4–7. The fraudsters “are probably not hardened criminals, but regular people who fall for the temptation.” *Id.* at 4:8–9. Yet the “otherwise honest fraudsters” still commit fraudulent transactions. *Id.* at 4:14–16.

To reduce fraudulent transactions, the ’010 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, 4:41–48; *see id.* at 7:44–48. The techniques “can be used with devices and services that are not protected by passwords, or where passwords are commonly shared.” *Id.* at 2:29–32.

The ’010 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, 4:62–67. Specifically, “physical cash is a concrete, tangible item while a digital payment for a digital good is a more abstract concept.” *Id.* at 4:28–30. The “more concrete the value of a transaction is,” however, “the more guilty a fraudster might feel when perpetrating the fraud.” *Id.* at 4:60–62. “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 5:16–18.

The '010 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:

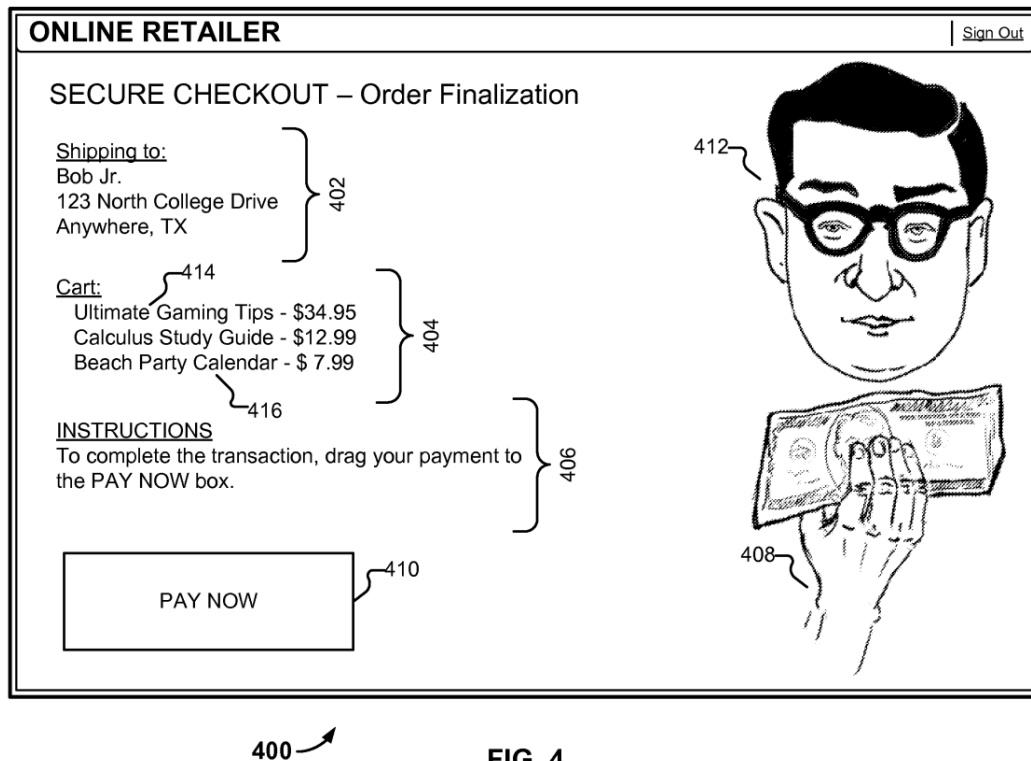


Figure 4 “illustrates an embodiment of an interface” as “rendered in a browser application of a personal computer.” Ex. 1001, 1:42, 6:18–20, Fig. 4. In particular, “Bob has specifically told Bob Jr. that it is ok for Bob Jr. to purchase schoolbooks using Bob’s account with online retailer 124” in Figure 1, and the Figure 4 interface is “shown to Bob Jr. during a checkout process.” *Id.* at 5:25–27, 6:18–21, 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, 6:26–30, 6:46–47, 10:56–57, Fig. 4.

The “amount of money held by the hand” may correspond to the “amount of money implicated by the transaction.” Ex. 1001, 10:21–23. Other transaction icons “can also be used, such as those depicting only the money” without a hand. *Id.* at 10:31–32.

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, 6:6–8, 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, 6:29–30, 6:47–49, 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 6:55–58.

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, 6:39–43; *see id.* at 9:13–17. “Such biometric information may be partial (e.g., the size or shape of a fingerprint) or more complete (e.g., a fingerprint).” *Id.* at 6:43–45.

The '010 patent's Figure 6 (reproduced below) depicts an interface for an electronic device:

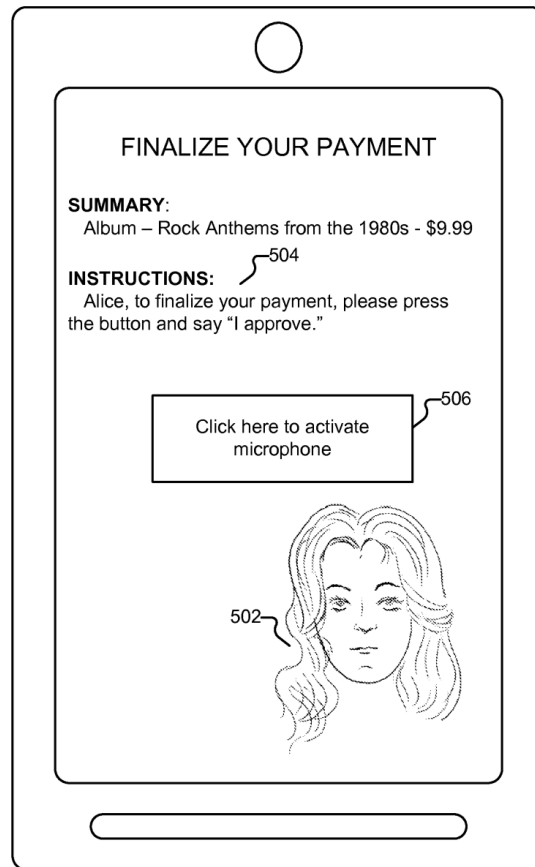


FIG. 6

Figure 6 “illustrates an embodiment of an interface” as rendered on mobile telephone 110 during a checkout process for Alice. Ex. 1001, 1:46, 7:49–52, Fig. 6. Previously, as part of an enrollment process, “Alice was asked to photograph herself, and to provide a short voice sample.” *Id.* at 7:53–55.

“As part of the checkout process, Alice is shown the image she provided at registration (502).” Ex. 1001, 7:55–57. The checkout process provides “instructions (504) for Alice (by name) on how to complete the transaction.” *Id.* at 7:57–59. 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 7:59–64. “Alice’s voice is recorded after she activates the microphone of device 110 by selecting box 506.” *Id.* at 10:1–3.

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, 7:66–8:2. 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 8:2–7. 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 8:8–12.

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, 8:38–44.

The '010 patent's Figure 7 (reproduced below) depicts an interface for an electronic device:

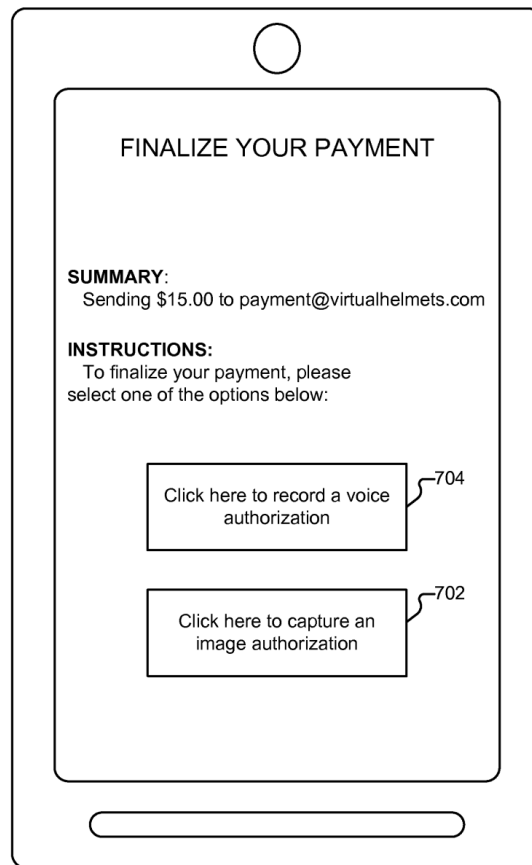


FIG. 7

Figure 7 “illustrates an embodiment of an interface” as rendered on mobile telephone 110 during a checkout process. Ex. 1001, 1:47, 8:45–47, 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, 8:47–51, 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 8:51–53.

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, 8:55–60.

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, 9:1–3. 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 9:3–6. “Other contextual information can also be captured (or threatened to be captured) and analyzed, if applicable.” *Id.* at 9:6–8.

E. The Challenged Claims

The ’010 patent includes 23 claims. Ex. 1001, 13:56–16:53. Petitioner challenges the following claims:

- independent claim 1 for a “system”;
- claims 2, 4–7, and 20–23 that depend directly from claim 1;
- independent claim 9 for a “method”;
- claims 10 and 12–15 that depend directly from claim 9; and
- independent claim 17 for a “computer program product embodied in a non-transitory computer readable storage medium.”

Pet. 6, 14–85.

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] receive a virtual likeness of a face of an account holder; associate, in a data store, the virtual likeness of the face of the account holder with an account of the account holder;
 - [1.3] render, in an interface, the virtual likeness of the face of the account holder;
 - [1.4] render a transaction icon associated with an electronic transaction, wherein the transaction icon is rendered in the interface with the virtual likeness of the face of the account holder;
 - [1.5] receive an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the account holder;
 - [1.6] capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information associated with a user;
 - [1.7] perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises determining, based at least in part on the captured biometric information, that the user is alive; and
 - [1.8] based at least in part on both the user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the

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

account holder and performing the fraud detection analysis comprising determining that the user is alive based at least in part on the captured biometric information, complete the electronic transaction; and

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

Ex. 1001, 13:56–14:25.

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
Guidance	Federal Financial Institutions Examination Council (FFIEC) Guidance, <i>Authentication in an Internet Banking Environment</i> , 1–14 (October 2005)	1037

Pet. 6, 14–85.

Petitioner asserts that:

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

Pet. 6; *see* 35 U.S.C. § 102(a), (b), (e) (2006).²

² 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

Patent Owner disputes that Stone and the Guidance qualify as prior art. *See* Resp. 22, 26–29, 42, 44–45; Sur-reply 24; Tr. 110:24–113:11. In particular, Patent Owner contends that “Stone is not analogous art.” Resp. 26, 42, 45; Sur-reply 24; *see* Resp. 22, 26–29; *infra* § III.D.3(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. 44. Patent Owner does not dispute that Varghese and Hoyos qualify as prior art. *See, e.g.*, Resp. 14–40; Sur-reply 2–28.

For the reasons explained in the patentability analysis below, we determine that Stone is analogous art. *See infra* § III.D.3(d). Because we do not reach the challenge based on Stone and the Guidance, we do not address whether the Guidance is analogous art. *See infra* § III.F.

G. The Asserted Challenges to Patentability

Petitioner asserts the following challenges to patentability:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1, 2, 4–6, 9, 10, 12–14, 17, 20, 21, 23	103(a)	Stone, Hoyos
7, 15, 22	103(a)	Stone, Hoyos, Varghese
1, 2, 4–7, 9, 10, 12–15, 17, 20–23	103(a)	Stone, Guidance

Pet. 6, 14–85.

predates the AIA’s amendments to § 102 and § 103, this decision refers to the pre-AIA versions of § 102 and § 103.

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.³ *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.

³ The parties do not address objective indicia of nonobviousness. *See, e.g.*, Pet. 14–85; Resp. 1–6, 14–45.

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.* at 4–5. 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 ’010 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 ¶ 1).

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. 5.

Patent Owner “accepts Petitioner’s position that none of the claim terms” of the ’010 patent “require construction.” Resp. 13 (citing Pet. 5). 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, 2, 4–7, 9, 10, 12–15, 17, and 20–23 are unpatentable under § 103(a).

In the patentability analysis below, however, we address claim-construction issues raised with respect to limitations 1.1 and 1.9. See *infra* §§ III.D.5(b)(iii), III.D.5(i)(iii). We do so to provide better context to explain those issues and our resolution of those issues.

*D. Alleged Obviousness over Stone and Hoyos:
Claims 1, 2, 4–6, 9, 10, 12–14, 17, 20, 21, and 23*

Petitioner contends that claims 1, 2, 4–6, 9, 10, 12–14, 17, 20, 21, and 23 are unpatentable under § 103(a) because the claims would have been obvious over Stone and Hoyos. *See* Pet. 6, 14–60; Reply 2–25. Patent Owner disputes Petitioner’s contentions. *See* Resp. 14–36; Sur-reply 2–27.

Below, we provide overviews of Stone and Hoyos. Then, we consider the obviousness issues. For the reasons explained below, we agree with Petitioner that claims 1, 2, 4–6, 9, 10, 12–14, 17, 20, 21, and 23 are unpatentable under § 103(a) because the claims would have been obvious over Stone and Hoyos.

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:

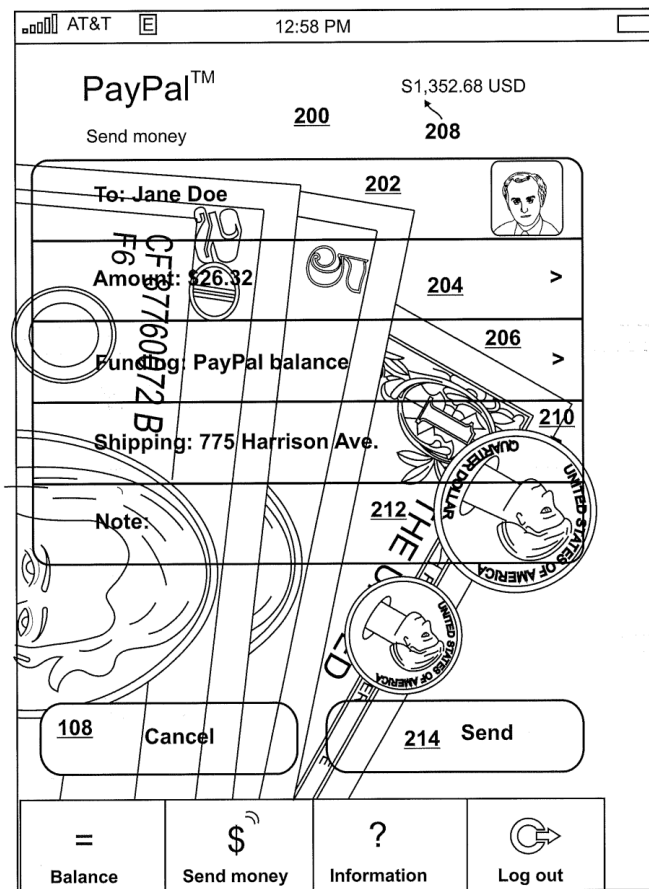


FIG. 2

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:

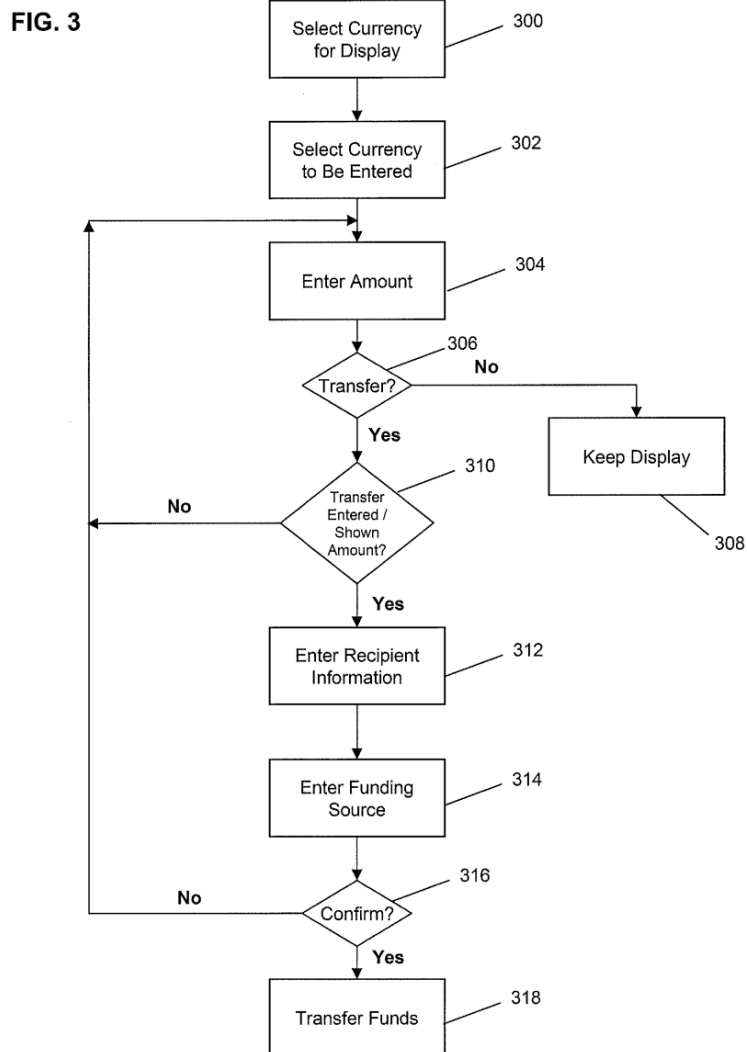


Figure 3 illustrates steps 300 through 318 for transferring funds to a recipient. *See* Ex. 1008 ¶¶ 29–35, Fig. 3.

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:

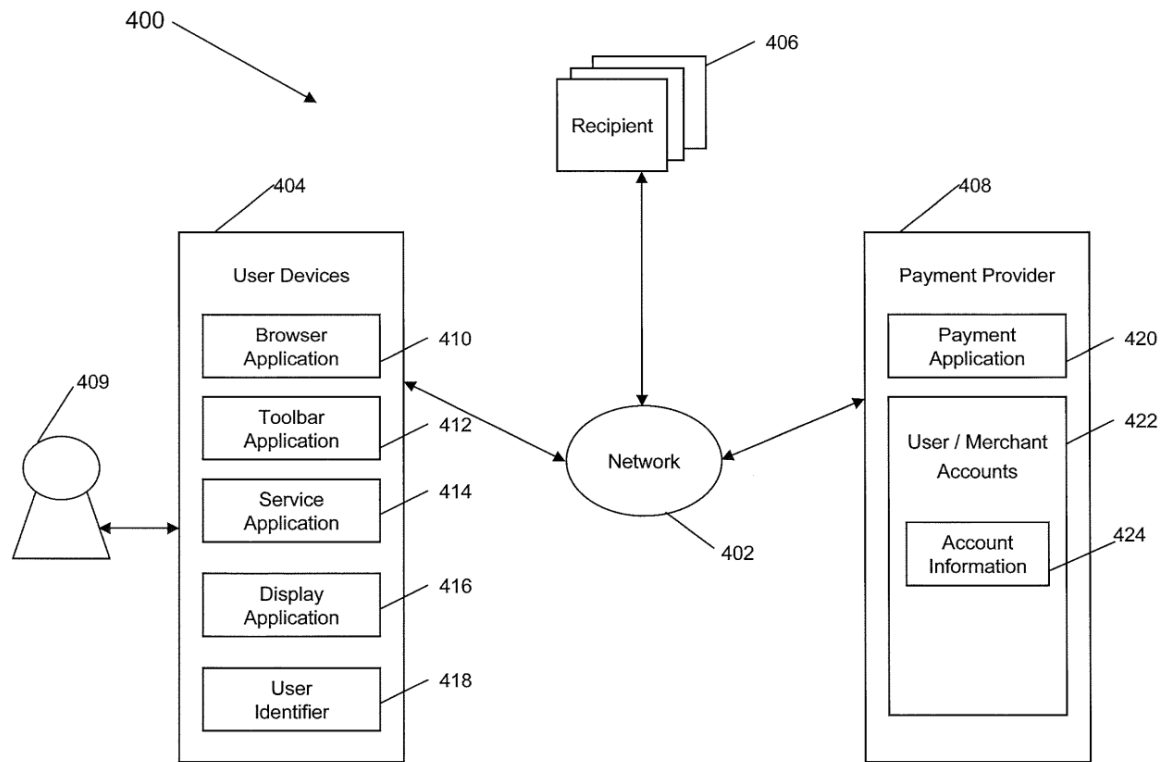


FIG. 4

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”:

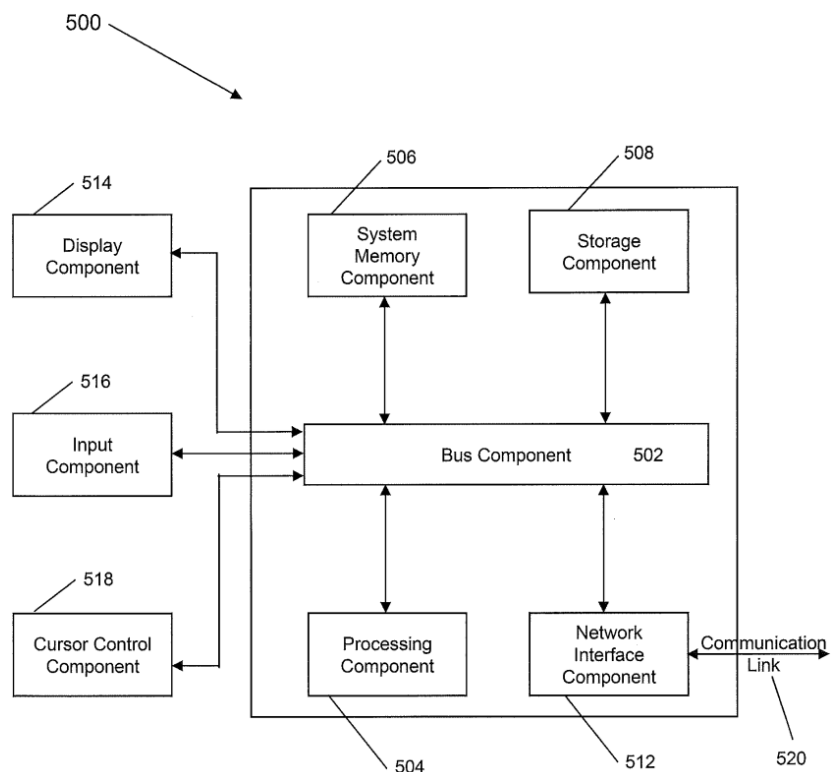


FIG. 5

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:

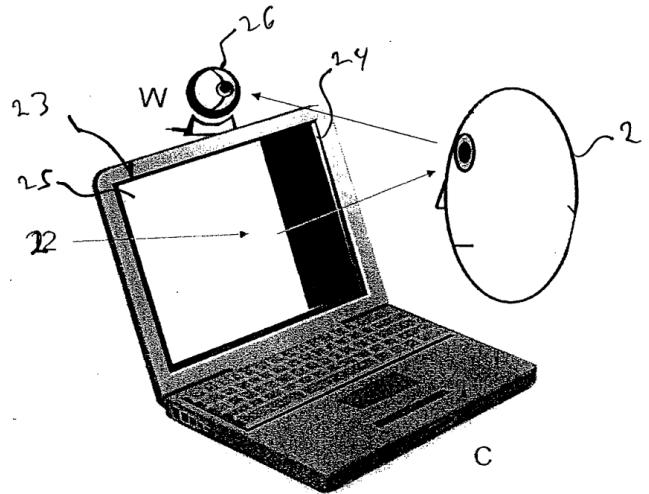


Fig. 2

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. 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-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 ’010 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 ’010 patent was involved,” e.g., “fraud detection in electronic financial transactions.” Pet. 13 (citing Ex. 1003 ¶ 53); *see id.* at 7; Reply 20.

Regarding “the same field of endeavor,” Petitioner asserts that:

- (1) Stone “explicitly describes its implementation in the context of PayPal”;
- (2) an ordinarily skilled artisan “would have understood PayPal to be a widely used online payment platform

allowing users to send and receive money and transfer funds between bank accounts or credit cards”; and

- (3) PayPal is in “the same field of endeavor” as the ’010 patent.

Reply 20 (citing Ex. 1056 ¶ 29).

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).

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 20 (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 ¶ 29).

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

- (1) the Examiner cited “user interface art,” e.g., Gaw and Fujioka,⁴ during the ’010 patent’s prosecution; and

⁴ 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.

- (2) the '010 patent lists additional “user interface art,” e.g., “Haynes,^[5] Lindquist,^[6] Synstelien,^[7] Mengerink,^[8] etc.,” in the References Cited section.

Prelim. Reply 4–5 (citing Ex. 1002, 87).

(c) Patent Owner’s Contentions

Patent Owner contends that “Stone is not analogous art.” Resp. 26, 42, 45; Sur-reply 24; *see* Resp. 22, 26–29. 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. 28. 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.*

Additionally, Patent Owner contends that Stone:

- (1) “never discusses fraud”;
- (2) “never discusses any techniques for countering fraud”;

⁵ *See* U.S. Patent No. 5,428,734, to Thom R. Haynes et al. (“Haynes”), titled “Method and Apparatus for Enhancing Drag and Drop Manipulation of Objects in a Graphical User Interface,” and issued on June 27, 1995.

⁶ *See* U.S. Patent Application Publication No. 2002/0152137, Wesley D. Lindquist et al. (“Lindquist”), titled “Drag-and-Drop Web Site Navigation System,” and published on October 17, 2002.

⁷ *See* U.S. Patent Application Publication No. 2008/0040426, to Don Synstelien et al. (“Synstelien”), titled “System and Method for Placing a Widget onto a Desktop,” and published on February 14, 2008.

⁸ *See* U.S. Patent Application Publication No. 2009/0171810, to Matthew Mengerink et al. (“Mengerink”), titled “Systems and Methods for Facilitating Financial Transactions over a Network,” and published on July 2, 2009.

- (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”;
- (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, 28 (quoting Ex. 1008 ¶ 16); Sur-reply 24. According to Patent Owner, Stone’s discussion of financial transactions “is tangential to Stone’s primary purpose—improving a user display.” Resp. 29.

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 ’010 Patent is concerned with solving—electronic payment fraud.” Resp. 29. Patent Owner identifies “the problem facing the inventor” as “fraud detection.” Sur-reply 24. 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. 29.

(d) Analysis

For the reasons explained below, we agree with Petitioner that Stone is analogous art. *See* Pet. 13; Prelim. Reply 4–5; Reply 20. 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 ¶ 29; Inst. Dec. 38–39; *Bigio*, 381 F.3d at 1325.

The ’010 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, 4:62–67. 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 4:28–30, 4:62–67, 5:16–18; *see* Ex. 1056 ¶ 29; Inst. Dec. 38.

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 ¶ 122; Ex. 1056 ¶ 29; Inst. Dec. 38. 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 ¶ 39.

Also, as Petitioner asserts, the Examiner cited “user interface art” during the ’010 patent’s prosecution. Ex. 1002, 87–91, 94, 146–58, 161, 290, 292, 342–50, 353, 454; *see* Ex. 1001, code (56); Prelim. Reply 4–5; Inst. Dec. 38. 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, 1:42, 1:46–47, 6:18–21, 7:49–52, 8:45–47, Figs. 4, 6–7; *see* Inst. Dec. 38. 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. 38–39.

Further, the Examiner characterized application claims 1–6, 8, and 10 corresponding to patent claims 1–8 as “drawn to [a] system configured to drag an icon associated with a payment and drop it on a destination region.” Ex. 1002, 82, 457; *see* Inst. Dec. 39. Stone discloses dragging an icon associated with a payment and dropping it on a recipient’s icon. Ex. 1008 ¶¶ 20, 36, claim 12; *see* Ex. 1003 ¶ 91.

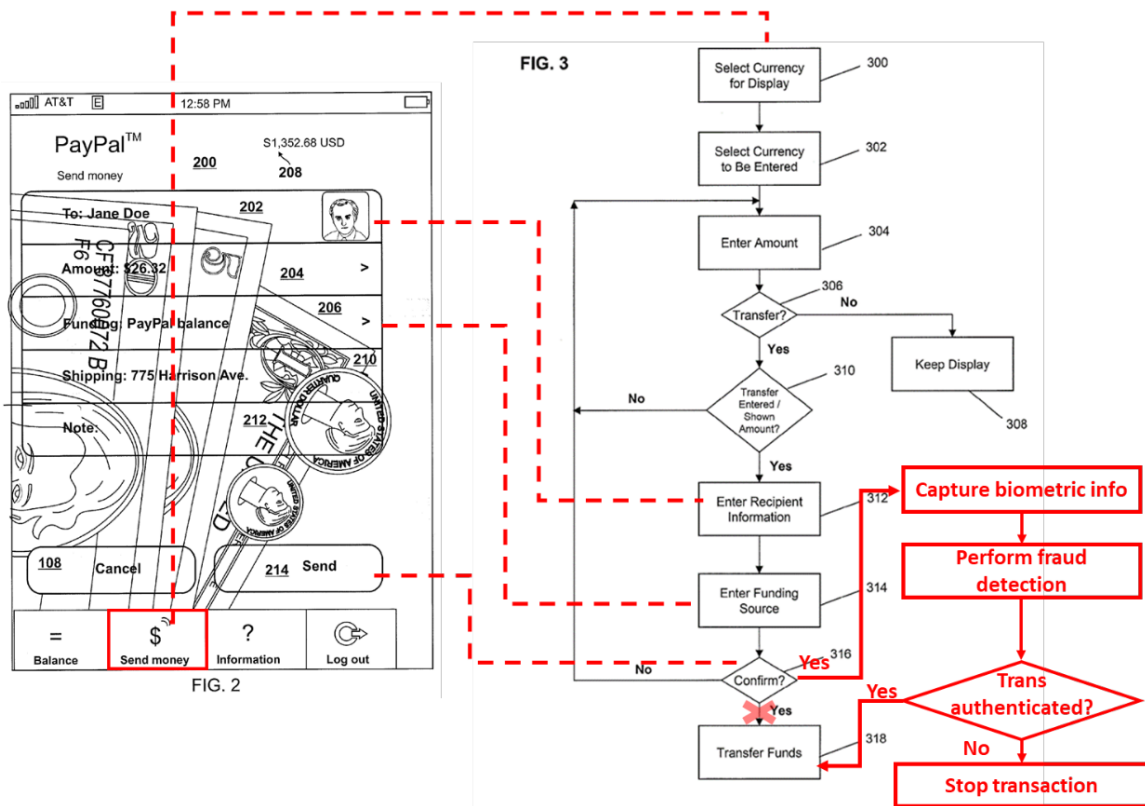
For the reasons discussed above, a preponderance of the evidence establishes that Stone is at least “reasonably pertinent” analogous art, and Patent Owner’s contentions to the contrary lack merit.

4. 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 (Pet. 20):



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

Pet. 20; *see* Ex. 1003 ¶ 62; 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; *see* Reply 19–22. 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., block 202 corresponds to block 312, block 206 corresponds to block 314, and block 214 corresponds to block 316.” *Id.* at 16.

Further, Petitioner asserts that “it was well-known that financial transactions of Stone had a need for authentication including fraud detection (e.g., with higher levels of security for some transactions).” Pet. 17 (citing

Ex. 1003 ¶ 61; Ex. 1010 ¶ 148; Ex. 1013 ¶¶ 9, 11; Ex. 1016 ¶ 73, Fig. 3). As support, Petitioner quotes the following statement in Varghese: “For example, 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.” *Id.* at 17–18 (emphasis omitted) (quoting Ex. 1010 ¶ 148). As further support, Petitioner quotes the following statements in Carter:⁹ “[T]he transaction must then be authenticated before proceeding,” and “the necessary authentication level is determined based on the transaction criteria,” such as “value and type of transaction.” *Id.* at 18 (emphases omitted) (quoting Ex. 1016 ¶ 73).

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. 17 (quoting Ex. 1013 ¶ 15) (citing Ex. 1003 ¶¶ 59–68; Ex. 1013 ¶¶ 17–22); *see id.* at 40 (quoting Ex. 1013 ¶ 15) (citing Ex. 1003 ¶ 103); Reply 20–21 (citing Ex. 1003 ¶¶ 59–68; Ex. 1013 ¶¶ 15, 17–22; Ex. 1056 ¶ 30).

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

- (1) “addressing spoofing”;

⁹ U.S. Patent Application Publication No. 2009/0157560 A1, to Samuel J. Carter et al. (“Carter”), titled “Information Banking and Monetization of Personal Information,” and published on June 18, 2000.

- (2) “‘making it much more difficult for an attempted fraudster to refine fraudulent methods’ and thereby reducing iterative attacks by eliminating clear feedback”;
- (3) “‘greatly reducing ‘the reject rate of true authenticics’ by using the liveness probability that is less sensitive to conditions like illumination changes”;
- (4) “‘providing ‘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.’”

Pet. 18 (quoting Ex. 1013 ¶¶ 24, 26–27, 29).

Petitioner explains that in the proposed combination biometric authentication according to Hoyos would occur 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, e.g., to continue and confirm the transaction.

Pet. 20 (citing Ex. 1003 ¶ 64).

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 previously captured authentication information for transaction authentication.” Pet. 21. According to Petitioner, those “various benefits” include (1) performing “risk-based contextual authentication adaptive to a particular transaction request and its assessed risk,” (2) “capturing more accurate data by avoiding imposters from communicating based on stolen biometric data,” and (3) “reducing spoofing.” *Id.* (citing Ex. 1003 ¶ 65).

Petitioner asserts that Stone’s system based on a client-server model and Hoyos’s biometric authentication are complementary. Reply 21. 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 21, 25 (citing Ex. 1003 ¶¶ 67–68; Ex. 1056 ¶ 33; Pet. 22).

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 21 (emphases omitted) (quoting Ex. 1055, 2); *see* Ex. 1055, 2; Ex. 2031, 16.

(iii) Reasonable Expectation of Success

Petitioner asserts that an ordinarily skilled artisan “would have reasonably expected to succeed in configuring Stone-Hoyos to leverage Hoyos’ biometric authentication functionality since its implementation would have required only routine knowledge well within” the artisan’s skill. Pet. 21 (citing Ex. 1003 ¶ 66).

Petitioner explains that Stone and Hoyos each concern systems for financial transactions including electronic devices known to have cameras or readily connectable to cameras that would obtain biometric information, e.g., facial photographs. Pet. 21–22 (citing Ex. 1008 ¶ 4; Ex. 1009, 15:22–23; Ex. 1013 ¶ 7, code (54), claims 13–14). Petitioner also explains that

implementing (1) “biometric information capturing” and (2) “fraud detection analysis” either “locally” at a client device or “remotely” at a server would have been within the skills of an ordinarily skilled artisan. *Id.* at 22 (citing Ex. 1003 ¶¶ 67–68; Ex. 1015, Fig. 3; Ex. 1016 ¶¶ 40, 42; Ex. 1038, 64);¹⁰ *see* Reply 16 (citing Ex. 1003 ¶¶ 67–68; Ex. 1056 ¶ 18).

(b) Patent Owner’s Contentions

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. 22–23 (emphasis omitted) (citing *TQ Delta, LLC v. Cisco Sys., Inc.*, 942 F.3d 1352, 1356 (Fed. Cir. 2019)); *see* Sur-reply 22.

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 transactions of Stone had a need for authentication including fraud detection (e.g., with higher levels of security for some transactions)”; and
- (2) “In view of Stone’s need to implement authentication with fraud detection,” an ordinarily skilled artisan “would have implemented biometric authentication and fraud detection as taught by Hoyos in the system of Stone.”

Resp. 23 (alteration by Patent Owner) (quoting Pet. 17–18); *see* Sur-reply 22. Patent Owner argues that the above assertions “do not explain

¹⁰ For Exhibit 1038, we cite to the page numbers that appear in the publication instead of the page numbers that Petitioner applied to the exhibit.

why” an ordinarily skilled artisan would have combined the teachings of the references. Resp. 23 (emphasis omitted) (citing Ex. 2032 ¶¶ 67–72).

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) Stone’s example transactions “are for low-dollar amounts,” e.g., \$26.32 as shown in Figure 2.

Sur-reply 23 (citing Pet. 17–18; 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.*

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. 23–25 (citing Ex. 1008 ¶¶ 2, 16, 23, 45; Ex. 1013 ¶¶ 16–22; Ex. 2032 ¶¶ 68–72); *see* Sur-reply 23–24. 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. 25 (citing Ex. 1013 ¶¶ 16–22; Ex. 2032 ¶ 71).

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. 22, 29–30; *see id.* at 30–34; Sur-reply 24–26. According to Patent Owner, Stone and Hoyos are “incompatible” because “they are directed to different computing environments.” Resp. 30–31; *see id.* at 34; Sur-reply 24. 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. 31 (citing Ex. 1008 ¶¶ 40–48, Fig. 4; Ex. 1013 ¶¶ 16–22, claim 4; Ex. 2032 ¶ 78); Sur-reply 24–25.

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. 26 (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. 31–33; Sur-reply 25–26, 28. 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. 31–32; Sur-reply 25. According to Patent Owner, using Hoyos’s biometric authentication as “the final step to complete the transaction” would “require on-device authentication after the device has already transferred information in communication with payment server 408.” Resp. 32 (emphasis omitted) (citing Ex. 2032 ¶¶ 80–81). Also, “[s]toring the same user account information on the user device would be a waste of device storage.” Sur-reply 25.

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. 32; Sur-reply 26; *see* Resp. 33. 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. 32 (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. 32–33. 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 26 (citing Ex. 2032 ¶¶ 81–83).

Fourth, Patent Owner asserts that implementing Hoyos’s biometric authentication in “Stone’s client-server structure” would “tie up processing resources on the user device that ‘the client-server structure is meant to free up.’” Resp. 32 (quoting Ex. 2032 ¶ 81). 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 26 (citing Ex. 1038, 64).

(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. 14–21, 40; Reply 19–22. Dr. Jones’s testimony supports Petitioner’s positions. *See* Ex. 1003 ¶¶ 54–65, 103; Ex. 1056 ¶¶ 27–34.

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, 17–21, 40; Ex. 1003 ¶¶ 53, 59–60, 62–65, 103; Ex. 1008 ¶¶ 45, 48. Those advantages include the following:

- (1) “improved fraud resistancy 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 ¶¶ 59, 62, 103; Ex. 1013 ¶¶ 12, 15, 24, 26–27, 29; *see* Pet. 17–18, 40. 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 ¶ 61 (Dr. Jones explaining that “it was well-known that [the] financial transactions of Stone had a need for authentication including 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. 17–18, 40 (quoting Ex. 1013 ¶¶ 15, 24, 26–27, 29); *see* Ex. 1003 ¶¶ 59, 62, 103; Ex. 1013 ¶¶ 12, 15, 24, 26–27, 29. 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. 22–23.

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. 25. 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 ¶¶ 38–39. 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 ¶¶ 40–44.

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. 17–21, 40; Ex. 1003 ¶¶ 59–65, 103.

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 23. 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 ¶¶ 53, 60. 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 ¶¶ 59, 65, 103; 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 ¶¶ 61, 177. 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 ¶ 61 (quoting Ex. 1010 ¶ 148); Inst. Dec. 51 (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 ¶ 61 (quoting Ex. 1016 ¶ 73); Inst. Dec. 51 (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 ¶¶ 67–68, 177 (citing Ex. 1016 ¶¶ 36, 40, 42–43, 76); Ex. 1056 ¶¶ 18, 33 (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 ¶¶ 61, 177; Ex. 1010 ¶¶ 79, 84, 91, 109–110, 148; Ex. 1016 ¶¶ 36, 38–40, 42–43, 73; Resp. 31–32. 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 ¶ 33.

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. 30–31; Sur-reply 24–25. 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 ¶ 67; *see* Ex. 1056 ¶ 18. 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 ¶¶ 33, 44.

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 ¶¶ 33, 44; 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 ¶¶ 33, 44.

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 ¶ 68 (quoting Ex. 1038, 64); Inst. Dec. 50 (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 ¶¶ 18, 33 (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 ¶ 68 (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 ¶ 68; Resp. 32–33; Sur-reply 26.

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 ¶ 68; Sur-reply 25. 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 26. 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. 22, 29–33; Sur-reply 24–26. “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. 22, 29–34; Sur-reply 24–26; *see also* Ex. 1056 ¶¶ 30–34.

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. 26. 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. 17–18, 40; Ex. 1003 ¶¶ 59, 62, 103.

(ii) Reasonable Expectation of Success

We agree with Petitioner that an ordinarily skilled artisan would have had a reasonable expectation of success in combining the teachings of the references. *See* Pet. 21–22; Ex. 1003 ¶¶ 66–68; Ex. 1056 ¶ 18.

As Petitioner explains, Stone and Hoyos each concern systems for financial transactions including electronic devices known to have cameras or readily connectable to cameras that would obtain biometric information, e.g., facial photographs. *See* Ex. 1003 ¶ 66; Ex. 1008 ¶¶ 4, 49, Fig. 5; Ex. 1013 ¶¶ 7, 18–19, code (54), Fig. 2, claims 13–14); Pet. 21–22. For instance, Stone notes that system 500 may comprise “part of a cell phone,” and cell phones were known to include cameras. *See* Ex. 1003 ¶¶ 66, 75; Ex. 1008 ¶ 49.

As Petitioner also explains, implementing (1) “biometric information capturing” and (2) “fraud detection analysis” either “locally” at a client device or “remotely” at a server would have been within the skills of an ordinarily skilled artisan. *See* Ex. 1003 ¶¶ 67–68; Ex. 1056 ¶ 18; Pet. 22.

For instance, 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 ¶¶ 18, 33 (quoting Ex. 1016 ¶¶ 40, 42). Further, 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 ¶ 68 (quoting Ex. 1038, 64).

5. INDEPENDENT CLAIM 1

(a) Preamble 1.0

Claim 1 recites “[a] system.” Ex. 1001, 13:56.

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. 22 (emphasis omitted) (quoting Ex. 1008 ¶ 40). According to Petitioner, “Stone further describes that its system includes software ‘such as program code and/or data . . . stored on one or more computer readable mediums.’” *Id.* at 23 (alteration by Petitioner) (quoting Ex. 1008 ¶ 54).

Patent Owner makes no arguments specific to claim 1’s preamble. *See, e.g.*, Resp. 14–34; Sur-reply 2–26. 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. 22–24; Ex. 1003 ¶¶ 69–72.

(b) Limitation 1.1

Claim 1 recites “one or more processors configured to.” Ex. 1001, 13:57 (limitation 1.1).

(i) Petitioner's Contentions

Petitioner contends that Stone teaches limitation 1.1 and alternatively that the combined disclosures in Stone and Hoyos 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 other processors including the processor 504 of payment provider device 408).” *Id.* at 24. According to Petitioner, the “one or more processors” are configured to “perform processes for a transaction.” *Id.*

Further, Petitioner asserts that Stone discloses system 500, “such as part of a cell phone, personal computer and/or a network server.” Pet. 24 (quoting Ex. 1008 ¶ 49). Petitioner asserts that Stone's system 500 includes “bus 502 or other communication mechanism for communicating information” that “interconnects subsystems and components,” such as “processing component 504 (e.g., processor, micro-controller, digital signal processor (DSP), etc.).” *Id.* (emphasis omitted) (quoting Ex. 1008 ¶ 49).

Additionally, Petitioner asserts that Stone alone or the combined disclosures in Stone and Hoyos teach a processor configured to perform the processes recited in limitations 1.2–1.8, including “initiating, authenticating, and completing the electronic transaction.” Pet. 26 (citing Ex. 1003 ¶ 77).

(ii) Patent Owner's Contentions

Patent Owner contends that the language “one or more processors configured to” in limitation 1.1 requires “at least one processor capable of performing each of” the subsequent limitations 1.2–1.8. Sur-reply 13 (emphases omitted) (citing *Salazar v. AT&T Mobility LLC*, 64 F.4th 1311, 1317 (Fed. Cir. 2023)). According to Patent Owner, Petitioner identifies different processors that perform limitations 1.2 and 1.3 and, therefore, fails to show how Stone “disclose[s] or render[s] obvious ‘one or more processors configured to perform’ the functionality of” the challenged claims. *Id.* (citing Ex. 2032 ¶¶ 54–58).

(iii) Analysis

We agree with Petitioner that Stone teaches limitation 1.1. *See* Pet. 24–26; Ex. 1003 ¶¶ 73–76. Specifically, Stone discloses 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; *see* Ex. 1003 ¶ 70. User device 404 includes a processor, e.g., processing component 504 in system 500. Ex. 1008 ¶ 49, Fig. 5; *see* Ex. 1003 ¶¶ 74–76. Each recipient device 406 includes a processor, e.g., processing component 504 in system 500. Ex. 1008 ¶ 49, Fig. 5; *see* Ex. 1003 ¶¶ 74–76. Payment provider server 408 also includes a processor, e.g., processing component 504 in system 500. Ex. 1008 ¶ 49, Fig. 5; *see* Ex. 1003 ¶¶ 74–76. Stone describes processing component 504 as a “processor, micro-controller, digital signal processor (DSP), etc.” Ex. 1008 ¶ 49; *see* Ex. 1003 ¶ 75.

We disagree with Patent Owner that the language “one or more processors configured to” in limitation 1.1 requires “at least one processor

capable of performing each of” the subsequent limitations 1.2–1.8. *See* Sur-reply 13. By requiring “at least one processor capable of performing each of” the subsequent limitations 1.2–1.8, Patent Owner’s proposed construction precludes different processors from performing different limitations. *See id.* For example, Patent Owner’s proposed construction precludes a first processor from “receiv[ing] a virtual likeness of a face of an account holder” according to limitation 1.2 and a second processor from “render[ing], in an interface, the virtual likeness of the face of the account holder” according to limitation 1.3. *See* Ex. 1001, 13:58–63; Sur-reply 13.

By precluding different processors from performing different limitations, Patent Owner’s proposed construction renders the language “or more” in the phrase “one or more processors” in limitation 1.1 “void, meaningless, or superfluous.” Preferably, a claim construction should not render claim language “void, meaningless, or superfluous.” *Wasica Fin. GmbH v. Cont’l Auto. Sys., Inc.*, 853 F.3d 1272, 1288 n.10 (Fed. Cir. 2017); *see Ortho-McNeil Pharm., Inc. v. Mylan Lab’ys, Inc.*, 520 F.3d 1358, 1362 (Fed. Cir. 2008). Patent Owner does not explain why the intrinsic evidence supports its proposed construction. *See* Sur-reply 13.

Although Patent Owner cites *Salazar* as supporting its proposed construction, the circumstances in *Salazar* differ materially from the circumstances here. The claim at issue in *Salazar* included the transition term “comprising” and the following limitations:

- (1) “a microprocessor for generating . . .”;
- (2) “said microprocessor creating . . .”;
- (3) “retriev[ing] by said microprocessor”; and
- (4) “said microprocessor generating”

Salazar, 64 F.4th at 1313.

The Federal Circuit explained that the term “a microprocessor” does not require “only one microprocessor.” *Salazar*, 64 F.4th at 1317. But the Federal Circuit also explained that “the subsequent limitations referring back to ‘said microprocessor’ require that at least one microprocessor be capable of performing each of the claimed functions.” *Id.* Further, the Federal Circuit distinguished the claim at issue in *Salazar* from a claim at issue in *Convolve* that “had no subsequent reference to ‘the’ or ‘said’ processor, and thus did not require a single processor.” *Id.* at 1318 (citing *Convolve, Inc. v. Compaq Computer Corp.*, 812 F.3d 1313, 1321 (Fed. Cir. 2016)).

Here, limitations 1.2–1.8 do not reference “the” or “said” processor recited in limitation 1.1. Ex. 1001, 13:58–14:22. Hence, contrary to Patent Owner’s proposed construction, claim 1’s language does not require “at least one processor capable of performing each of” the subsequent limitations 1.2–1.8. *See* Ex. 1001, 13:56–14:25; Sur-reply 13.

Additionally, the ’010 patent’s written description does not support Patent Owner’s proposed construction. In particular, the written description defines the singular term “processor” as including multiple components by stating as follows: “As used herein, the term ‘processor’ refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.” Ex. 1001, 2:11–13; *see* Tr. 51:3–52:5.

In any event, as explained below, Petitioner identifies in the proposed Stone-Hoyos combination “at least one processor capable of performing each of” the subsequent limitations 1.2–1.8. *See infra* §§ III.D.5(c)–(h).

(c) Limitations 1.2 and 1.3

Claim 1 requires a processor configured to “receive a virtual likeness of a face of an account holder; [and] associate, in a data store, the virtual likeness of the face of the account holder with an account of the account holder.” Ex. 1001, 13:58–61 (limitation 1.2). Claim 1 also requires a processor configured to “render, in an interface, the virtual likeness of the face of the account holder.” *Id.* at 13:62–63 (limitation 1.3).

(i) Petitioner’s Contentions in the Petition

Petitioner contends that Stone teaches limitation 1.2 for two related reasons. *See* Pet. 26–29, 71. First, 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 other processors)” that are configured to “receive a virtual likeness of a face (‘photograph image’) of an account holder (user 409 (as either sender or recipient) with a user account 422), and store the received photograph image in user identifier 418” on user device 404. *Id.* at 26–27 (citing Ex. 1001, 16:31–53 (claim 23); Ex. 1003 ¶ 81; Ex. 1008 ¶¶ 46, 48).

Second, Petitioner asserts that Stone discloses “associating, using user identifier 418, in a data store (storage component 508 of user devices [sic] 404 alone, or in combination with storage component 508 of other devices including payment provider server 408), the virtual likeness of the face (photo) of the account holder (user 409) with an account (user account 422) of the account holder (user 409).” Pet. 28–29 (citing Ex. 1003 ¶ 82; Ex. 1008 ¶¶ 45, 48).

Petitioner contends that Stone teaches limitation 1.3 for each of a sender account holder and a recipient account holder, i.e., “either a sender or

a recipient of a transaction.” *See* Pet. 29–31, 71. 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 other processors including the processor 504 of payment provider device 408)” that are configured to “render, in an interface (e.g., interface 100 of FIG. 1, interface 200 of FIG. 2), the virtual likeness of the face (e.g., either a photo of the account holder on a visual representation of the currency, or a photo of a recipient of the electronic transaction, each disclosed by Stone) of the account holder (user 409).” *Id.* at 29 (emphases omitted).

Regarding a sender account holder, Petitioner asserts that the interface in Stone’s Figure 2 includes “the virtual likeness of the face” of a sender account holder in “personalized currency with the user’s photo.” Pet. 29–30 (emphasis omitted) (quoting Ex. 1008 ¶ 7). As support, Petitioner quotes Stone’s disclosure that “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.* at 30 (emphasis omitted) (quoting Ex. 1008 ¶ 7).

Regarding a recipient account holder, Petitioner asserts that the interface in Stone’s Figure 2 includes “the virtual likeness of the face” of a recipient account holder in name box 202 containing a “picture of the recipient.” Pet. 30–31 (emphasis omitted) (quoting Ex. 1008 ¶ 24). As support, Petitioner quotes Stone’s disclosure that “display 200 has a name box 202 indicating the recipient of funds as well as a picture of the recipient . . . and a send button 214 to transfer the funds in noted in box 204.” *Id.* at 31 (alteration by Petitioner) (emphasis omitted) (quoting Ex. 1008 ¶ 24).

As further support for its assertions, Petitioner provides the following annotated version of Stone’s Figure 2 (Pet. 30):

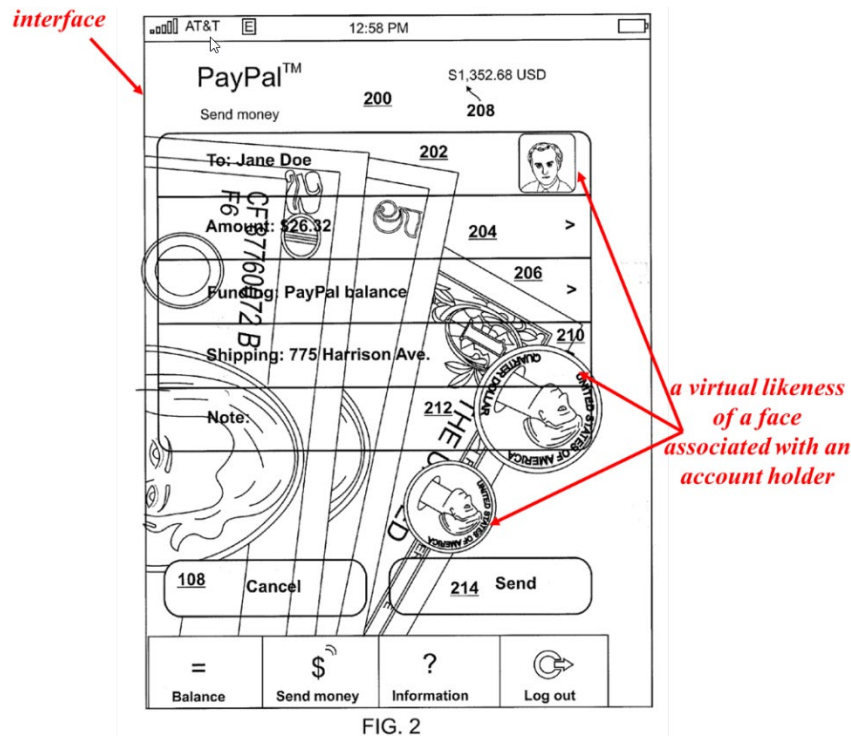


Figure 2 illustrates display 200 on an electronic device including various display elements. Ex. 1008 ¶¶ 11, 24, Fig. 2. The above annotated version of Figure 2 includes the following annotations:

- (1) the red annotation “*interface*” identifying display 200; and
- (2) the red annotation “*a virtual likeness of a face associated with an account holder*” identifying (i) a “picture of the recipient” in name box 202 and (ii) “personalized currency with the user’s photo” indicating “the amount entered by the user” in the background of the display.

Pet. 30; *see* Ex. 1003 ¶ 86; Ex. 1008 ¶¶ 7, 16, 24.

(ii) Patent Owner’s Contentions in the Response

Patent Owner disputes that Stone teaches limitations 1.2 and 1.3. *See* Resp. 15–19. Specifically, Patent Owner asserts that “one virtual likeness of the account holder’s face must satisfy the claim element ‘the virtual likeness of the face of the account holder’” recited in limitations 1.2 and 1.3. *Id.*

at 16–17. Further, Patent Owner asserts that Petitioner fails to identify the same “virtual likeness” of either a sender account holder or a recipient account holder that satisfies each of the “receive,” “associate,” and “render” requirements in limitations 1.2 and 1.3. *Id.* at 17.

Regarding the “virtual likeness” of a sender account holder, Patent Owner asserts that “Stone does not disclose that the photo used for the individualized currency displayed in the interface comes from the user photo that is user identifier 418.” Resp. 18 (citing Ex. 1008 ¶¶ 7, 19; Ex. 2032 ¶¶ 57–58). Patent Owner asserts that Stone discloses that payment server 408 (a) maintains user account information 424 and (b) uses “user identifier 418 (e.g., possibly a photo of the user) to associate user 409 with the user’s account.” *Id.* Patent Owner also asserts that “Stone does not disclose another means for associating any photo with a user’s account.” *Id.*

Further, Patent Owner asserts that “Stone does not disclose that a photo of the user that may be used for the individualized currency display is either user identifier 418 or otherwise associated with a user’s account by payment server 408.” Resp. 18. Therefore, according to Patent Owner, “the photo used for the individualized currency cannot be the same virtual likeness associated with the account as required by claim 1.” *Id.*

Regarding the “virtual likeness” of a recipient account holder, Patent Owner asserts that “Stone does not disclose that the recipient photo 202 that appears in the user interface of Figure 2 is provided to payment server 408 to be associated with a user’s account information 424 maintained on payment server 408.” Resp. 18 (citing Ex. 2032 ¶ 58). Patent Owner also asserts that “Stone does not disclose another means for associating the recipient photo with a user account.” *Id.* Therefore, according to Patent Owner, “recipient

photo 202, like the currency photo, cannot be the same virtual likeness associated with the account as required by claim 1.” *Id.* at 18–19.

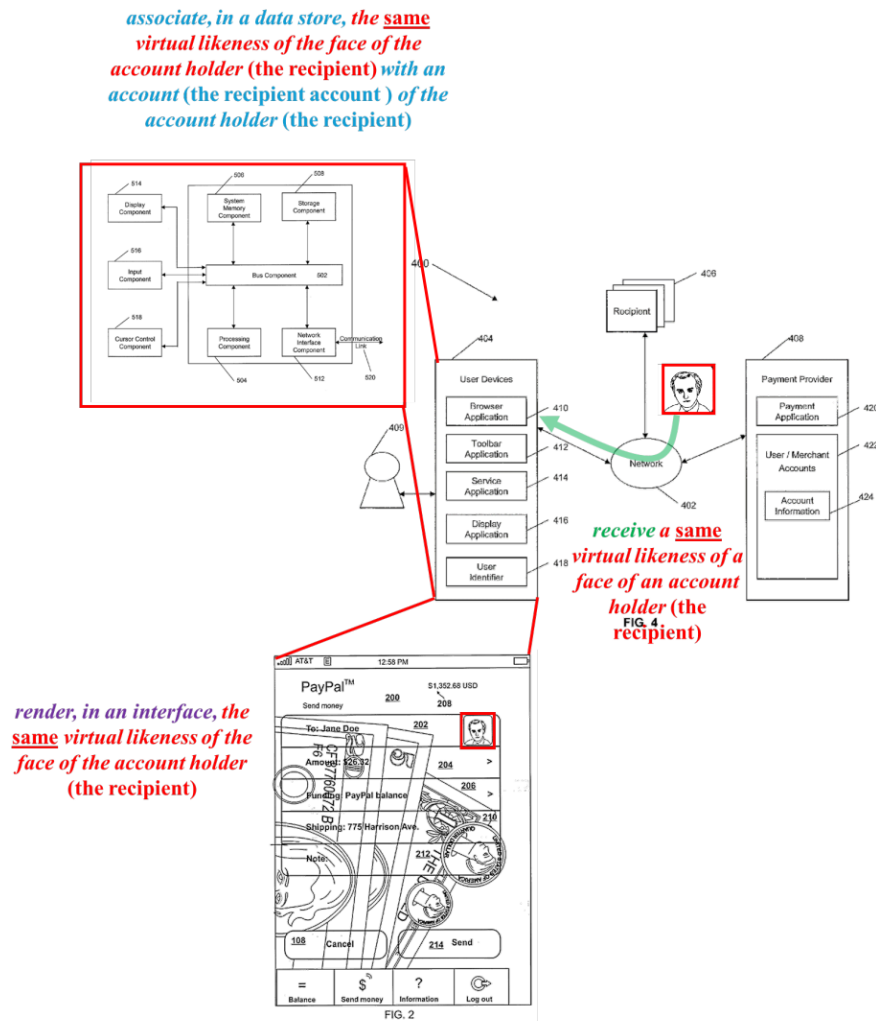
(iii) Petitioner’s Contentions in the Reply

Petitioner contends that in “Stone combined with Hoyos” the image/photo for each of a sender account holder and a recipient account holder satisfies the requirements in limitations 1.2 and 1.3 for “receiv[ing],” “associat[ing],” and “render[ing]” the same “virtual likeness” of an account holder’s face. *See* Reply 2–16. To support its contentions, Petitioner provides the following examples purporting to show how “Stone combined with Hoyos” satisfies those requirements in limitations 1.2 and 1.3:

- example 1.1 where one processor in sender user device 404 “receive[s],” “associate[s],” and “render[s]” the same “virtual likeness” of the face of a recipient account holder;
- example 1.2 where processors in sender user device 404, recipient device 406, and payment provider server 408 together “receive,” “associate,” and “render” the same “virtual likeness” of the face of a recipient account holder;
- example 2.1 where one processor in sender user device 404 “receive[s],” “associate[s],” and “render[s]” the same “virtual likeness” of the face of a sender account holder; and
- example 2.2 where processors in sender user device 404 and payment provider server 408 together “receive,” “associate,” and “render” the same “virtual likeness” of the face of a sender account holder.

Id. at 3–16.

To illustrate example 1.1, Petitioner provides the following composite figure containing Stone's Figures 2, 4, and 5 (Reply 4):



Example 1.1 of Stone Combined with Hoyos
(annotated based on APPL-1008, Stone, FIGS. 2 and 4).

The above composite figure contains Stone's Figures 2, 4, and 5 and includes the following annotations (emphases omitted):

- (1) a picture of the recipient (from name box 202 in Figure 2) below recipient device 406 in Figure 4 with an arrow starting at that picture and directed through network 402 in Figure 4 to sender user device 404 in Figure 4;

- (2) the annotation “receive a same virtual likeness of a face of an account holder (the recipient)” below the arrow directed through network 402 in Figure 4 to sender user device 404 in Figure 4;
- (3) the annotation “associate, in a data store, the same virtual likeness of the face of the account holder (the recipient) with an account (the recipient account) of the account holder (the recipient)” above Figure 5 showing system 500 with system memory component 506 and static storage component 508; and
- (4) the annotation “render, in an interface, the same virtual likeness of the face of the account holder (the recipient)” adjacent to name box 202 in Figure 2 containing a picture of the recipient.

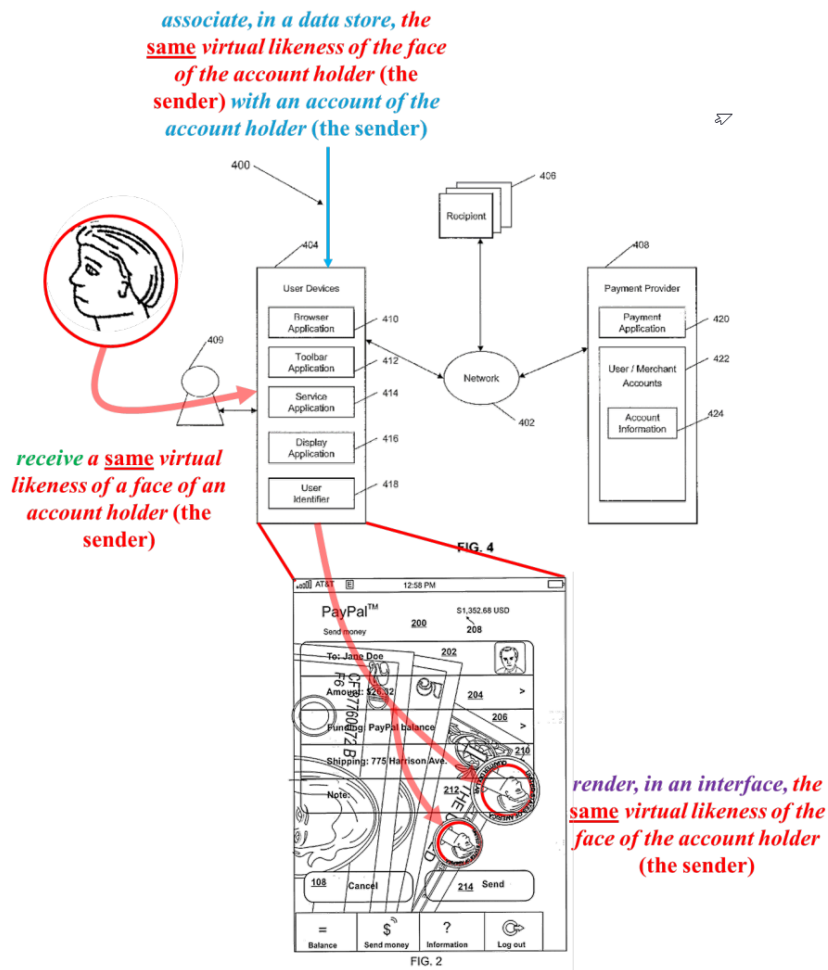
See Reply 4; Ex. 1056 ¶ 5.

Regarding Petitioner’s example 1.1 where one processor in sender user device 404 “receive[s],” “associate[s],” and “render[s]” the same “virtual likeness” of the face of a recipient account holder, Petitioner contends that for sender user device 404 to display the recipient image in the Figure 2 interface, sender user device 404 has to: (1) “receive the recipient image (e.g., through the network from recipient device 406) to display it”; and (2) “associate it with the recipient account for ‘Jane Doe’, such that the recipient image is displayed together with ‘To: Jane Doe’ in the field 202” in the Figure 2 interface. Reply 5 (emphases omitted) (citing Ex. 1008 ¶¶ 20, 46; Ex. 1056 ¶ 6).

Petitioner explains that processor 504 in sender user device 404 “associate[s]” the “virtual likeness of the face of the account holder” (the recipient image in Figure 2) with an “account of the account holder” (the “Jane Doe” recipient account in Figure 2) in a storage component in sender user device storage 404, thus satisfying limitation 1.2. Reply 5–6.

Petitioner also explains that after creating the association in storage, processor 504 in sender user device 404 uses the association in storage to “display the recipient account and recipient image in field 202” in the Figure 2 interface, thus satisfying limitation 1.3. *Id.*

To illustrate example 2.1, Petitioner provides the following composite figure containing Stone’s Figures 2 and 4 (Reply 11):



Example 2.1 of Stone Combined with Hoyos
(annotated based on APPL-1008, Stone, FIGS. 2 and 4).

The above composite figure contains Stone’s Figures 2 and 4 and includes the following annotations (emphases omitted):

- (1) the user's photo (from personalized currency in Figure 2) with an arrow starting at that photo and directed to sender user device 404 in Figure 4;
- (2) the annotation "receive a same virtual likeness of a face of an account holder (the sender)" below the arrow directed to sender user device 404 in Figure 4;
- (3) the annotation "associate, in a data store, the same virtual likeness of the face of the account holder (the sender) with an account of the account holder (the sender)" above an arrow directed to sender user device 404 in Figure 4; and
- (4) the annotation "render, in an interface, the same virtual likeness of the face of the account holder (the sender)" adjacent to personalized currency with the user's photo in Figure 2.

See Reply 11; Ex. 1056 ¶ 11.

Regarding Petitioner's example 2.1 where one processor in sender user device 404 "receive[s]," "associate[s]," and "render[s]" the same "virtual likeness" of the face of a sender account holder, Petitioner contends that processor 504 in sender user device 404 "receives a sender image and associates it with a sender user account (e.g., using a user identifier 418) in a storage of user device 404." Reply 12.

Further, Petitioner asserts that it "would have been obvious to use the already received and associated sender image" that meets limitation 1.2 and "is stored in user device 404 for display on the virtual currency" for "render[ing]" according to limitation 1.3 because "that sender image is already associated with the sender account and stored in the system 400." Reply 12. Petitioner explains that using the "already received, associated, and stored image of the sender would have the benefits of being efficient and reliable and avoid redundancy and unnecessary user effort, compared to a

new separate user image that [Patent Owner] apparently would hypothesize could be separately provided by the user.” *Id.* (citing Ex. 1056 ¶ 13).

(iv) Patent Owner’s Contentions in the Sur-reply

Patent Owner contends that Stone does not disclose that “either recipient photo 202 or the personalized currency rendered” in the Figure 2 interface “is related to the photo that can be used for user identifier 418.” Sur-reply 5. Patent Owner contends that Petitioner identifies only the photo used for user identifier 418 as “a likeness that is associated with the account holder’s account” for limitation 1.2. *Id.*

Patent Owner contends that the Petition “never identifies either the recipient photo 202 or the personalized currency display” for the “receive” and “associate” requirements in limitation 1.2. Sur-reply 6 (citing Pet. 26–28). Therefore, according to Patent Owner, the Board should “ignore Petitioner’s untimely examples” in the Reply and “hold Petitioner to the Grounds as asserted in the Petition, which fail on their face.” *Id.*

Further, Patent Owner asserts that “even if the Board considers Petitioner’s untimely examples,” those examples “fail to disclose a virtual likeness that satisfies” each of the “receive,” “associate,” and “render” requirements in limitations 1.2 and 1.3. Sur-reply 7.

Regarding example 1.1, Patent Owner quotes Petitioner’s contentions that sender user device 404 has to: (1) “receive the recipient image (e.g., through the network from recipient device 406)”; and (2) “associate it with the recipient account for ‘Jane Doe’, such that the recipient image is displayed together with ‘To: Jane Doe’ in the field 202” in the Figure 2 interface. Sur-reply 8–9 (quoting Reply 5). Then, Patent Owner asserts that “Stone does not state that an association between recipient photo 202 and the

recipient's account occurs anywhere on user device 404.” *Id.* at 9 (emphasis omitted). Patent Owner also asserts that nothing in Stone “states that any association of recipient account information occurs in any component of the user device shown in Figure 5.” *Id.*

Patent Owner contends that the “only association of users with specific account information disclosed in Stone occurs on the payment provider server 408 and the association is between user identifier 418 and the user account 422, not recipient photo 202.” Sur-reply 9 (citing Ex. 1008 ¶¶ 45–46; Ex. 2032 ¶¶ 57–58).

According to Patent Owner, example 1.1 “fails on two fronts: (1) recipient photo 202 is never associated with any user account, and (2) even if the recipient photo were associated with a user account, any association would occur on payment server 408—not the user device.” Sur-reply 11.

Regarding example 2.1, Patent Owner quotes Petitioner's assertion that it “would have been obvious to use the already received and associated sender image” that meets limitation 1.2 and “is stored in user device 404 for display on the virtual currency” for “render[ing]” according to limitation 1.3 because “that sender image is already associated with the sender account and stored in the system 400.” Sur-reply 14–15 (quoting Reply 12). Then, Patent Owner contends that Petitioner's justification for why it “would have been obvious to use” one sender image for each of the “receive,” “associate,” and “render” requirements in limitations 1.2 and 1.3 “concedes that the image on the virtual currency, if the user chooses to create one using a photo of the user's face, is actually not associated with the user's account.” *Id.* at 15. Patent Owner contends that “nothing in Stone suggests any link

between the virtual currency and user identifier 418 or that it would be obvious for a user to use the same photo for both.” *Id.*

Further, Patent Owner asserts that Petitioner “ignores the different purposes the virtual currency and user identifier serve.” Sur-reply 15. In particular, the virtual currency “is a way to customize the display by allowing the user to ‘create his own currency for display, such as casino chips, gold bars, personalized currency with the user’s photo, etc.’” *Id.* (quoting Ex. 1008 ¶ 7). In contrast, the user identifier “may be used by payment provider server 408 to associate user 409 with a particular user account maintained by payment provider server 408.” *Id.* at 15–16 (emphasis omitted) (quoting Ex. 1008 ¶ 45). According to Patent Owner, the “difference between a photo for a virtual currency display and user identifier is like the difference between” a social media picture used to express “personal individuality” and a passport photo used “for identification.” *Id.* at 16.

(v) Analysis

For the reasons explained below, we agree with Petitioner that Stone teaches limitations 1.2 and 1.3. *See* Pet. 26–31; Reply 2–16; Ex. 1003 ¶¶ 79–88; Ex. 1056 ¶¶ 3–17.

First, Stone discloses that sender 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; *see* Ex. 1003 ¶ 80. Stone also discloses that user identifiers 418 “may include attributes related to the user,” such as the following:

- (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 ¶ 80. Thus, Stone teaches that sender user device 404 associates a sender “photograph image” with a sender “account number” in user identifiers 418. Ex. 1008 ¶ 45; *see* Ex. 1003 ¶¶ 80, 82.

Second, Stone does not explicitly state that sender user device 404 receives a sender “photograph image.” *See, e.g.*, Ex. 1008 ¶ 45. For sender user device 404 to associate a sender “photograph image” with a sender “account number” in sender user identifiers 418, however, sender user device 404 must have received the sender “photograph image,” as a skilled artisan would have recognized. *See* Ex. 1003 ¶¶ 80–83. An obviousness analysis can “take account of the inferences and creative steps that a person of ordinary skill in the art would employ” because a skilled artisan has “common sense, common wisdom, and common knowledge.” *See KSR*, 550 U.S. at 418; *Elektro Ltd. v. ZAP Surgical Sys., Inc.*, 81 F.4th 1368, 1374 (Fed. Cir. 2023).

Third, Stone discloses that recipient device 406 “may be the same or have the same basic features as [sender] 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 ¶ 80. Thus, Stone teaches that recipient device 406 associates a recipient “photograph image” with a recipient “account number” in recipient user identifiers 418. Ex. 1008 ¶¶ 45–46; *see* Ex. 1003 ¶¶ 80, 82.

Fourth, Stone does not explicitly state that recipient device 406 receives a recipient “photograph image.” *See, e.g.*, Ex. 1008 ¶¶ 45–46. For recipient device 406 to associate a recipient “photograph image” with a recipient “account number” in recipient user identifiers 418, however, recipient device 406 must have received the recipient “photograph image,” as a skilled artisan would have recognized. *See* Ex. 1003 ¶¶ 80–83.

Fifth, Stone discloses that:

- (1) payment provider server 408 may “maintain a plurality of user and recipient accounts 422, each of which may include account information 424 associated with individual users, including user 409, and the one or more recipient device 406”;
- (2) 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, which may be used to facilitate online transactions between user 409 of user device 404 and one or more recipients associated with recipient devices 406”;
- (3) sender user identifiers 418 in sender user device 404
 - (a) “may be passed with a user money transfer request to payment provider server 408” and
 - (b) “may be used by payment provider server 408 to associate user 409 with a particular user account maintained by payment provider server 408”; and
- (4) recipient user identifiers 418 in recipient device 406
 - (a) “may be passed with a money transfer from user 409 to payment provider server 408” and
 - (b) “may be used by payment provider server 408 to associate a particular money transfer with a particular recipient account maintained by payment provider server 408.”

Ex. 1008 ¶¶ 45–46, 48; *see* Ex. 1003 ¶ 82.

Thus, Stone teaches that payment provider server 408 may:

- (1) receive sender user identifiers 418 (including a sender “photograph image”) and then associate the sender user identifiers 418 with a sender “account maintained by payment provider server 408”; and
- (2) receive recipient user identifiers 418 (including a recipient “photograph image”) and then associate the recipient user identifiers 418 with a recipient “account maintained by payment provider server 408.”

Ex. 1008 ¶¶ 45–46, 48; *see* Ex. 1003 ¶ 82.

Accordingly, for the reasons discussed above, Stone teaches that one processor in each of sender user device 404, recipient device 406, and payment provider server 408 “receive[s] a virtual likeness of a face of an account holder; [and] associate[s], in a data store, the virtual likeness of the face of the account holder with an account of the account holder” according to limitation 1.2. *See* Ex. 1003 ¶¶ 80–83; Ex. 1008 ¶¶ 45–46, 48.

Sixth, as illustrated in Petitioner’s example 1.1, Stone teaches that one processor in sender user device 404 “receive[s],” “associate[s],” and “render[s]” the same “virtual likeness” of the face of a recipient account holder according to limitations 1.2 and 1.3. *See* Reply 3–5; Ex. 1056 ¶¶ 5–8. Specifically, Stone discloses that sender user device 404 “may be able to access recipient attributes,” such as “personal and banking information” and “icon information,” for “display or use” by sender user device 404.

Ex. 1008 ¶ 46; *see* Ex. 1056 ¶ 6. For instance, “[w]hen the user is connected to a network with other users, the user display may visually show other users” by displaying “an appropriate icon,” such as a “picture of the person.” Ex. 1008 ¶¶ 20, 36; *see* Ex. 1003 ¶ 87; Ex. 1056 ¶ 6.

Further, Stone's Figure 2 shows that sender user device 404 has:

- (1) accessed and "receive[d]" recipient account information ("Jane Doe" account information) and a "picture of the recipient";
- (2) "associate[d]" the recipient account information ("Jane Doe" account information) and the "picture of the recipient" to permit display together in the Figure 2 interface; and
- (3) "render[ed]" the information "To: Jane Doe" and the "picture of the recipient" together in name box 202 in the Figure 2 interface.

Ex. 1008 ¶¶ 24, 46, Fig. 2; *see* Ex. 1056 ¶¶ 5–7.

Patent Owner's assertion that "Stone does not disclose that the recipient photo 202 that appears in the user interface of Figure 2 is provided to payment server 408 to be associated with a user's account information 424 maintained on payment server 408" disregards the association that occurs on sender user device 404 after sender user device 404 accesses recipient attributes, such as "personal and banking information" and "icon information." *See* Ex. 1008 ¶¶ 24, 46, Fig. 2; Ex. 1056 ¶¶ 5–7; Resp. 18.

As for Patent Owner's assertion that "Stone does not state that an association between recipient photo 202 and the recipient's account occurs anywhere on user device 404," 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." *See KSR*, 550 U.S. at 415, 418; Sur-reply 9. A skilled artisan would have recognized that for sender user device 404 to display the recipient image in

the Figure 2 interface, sender user device 404 must: (1) “receive the recipient image (e.g., through the network from recipient device 406) to display it”; and (2) “associate it with the recipient account for ‘Jane Doe’, such that the recipient image is displayed together with ‘To: Jane Doe’ in the field 202” in the Figure 2 interface. Ex. 1056 ¶ 6 (emphases omitted); *see* Ex. 1008 ¶¶ 20, 24, 46, Fig. 2.

Seventh, as illustrated in Petitioner’s example 2.1, Stone teaches that one processor in sender user device 404 “receive[s],” “associate[s],” and “render[s]” the same “virtual likeness” of the face of a sender account holder according to limitations 1.2 and 1.3. *See* Reply 10–13; Ex. 1056 ¶¶ 11–15. Specifically, as discussed above in this section, Stone discloses that sender user device 404 receives a sender “photograph image” and associates the sender “photograph image” with a sender “account number” in sender user identifiers 418. Ex. 1008 ¶ 45; *see* Ex. 1003 ¶ 80. Additionally, Stone discloses that:

- (1) “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.”; and
- (2) the user’s “personalized currency may be created on” the user’s device.

Ex. 1008 ¶¶ 7, 19, 28; *see id.* ¶ 27; Ex. 1003 ¶ 86.

Using the “already received and associated” sender “photograph image” in sender user identifiers 418 in sender user device 404 to render the “personalized currency with the user’s photo” in the display of sender user device 404 would have been obvious. Ex. 1056 ¶ 13. Doing so would have been “efficient and reliable” and would have “avoid[ed] redundancy and unnecessary user effort.” *Id.*

As for Patent Owner’s assertion that “Stone does not disclose that the photo used for the individualized currency displayed in the interface comes from the user photo that is user identifier 418,” an 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.” *See KSR*, 550 U.S. at 418; Resp. 18. Stone discloses a sender “photograph image” in sender user identifiers 418 in sender user device 404. Ex. 1008 ¶ 45; *see* Ex. 1003 ¶ 80. Stone also discloses displaying “personalized currency with the user’s photo” in the display of sender user device 404. Ex. 1008 ¶¶ 7, 19, 28; *see id.* ¶ 27; Ex. 1003 ¶ 86. An ordinarily skilled artisan would have recognized that using the sender “photograph image” in sender user identifiers 418 to display “personalized currency with the user’s photo” in the display of sender user device 404 would have been “efficient and reliable” and would have “avoid[ed] redundancy and unnecessary user effort.” *See* Ex. 1056 ¶ 13.

Patent Owner’s assertion that Petitioner “ignores the different purposes the virtual currency and user identifier serve” rests on the erroneous premise that the virtual currency and user identifier necessarily serve different purposes. *See* Sur-reply 15–16. A user may want to use a single “photograph image” for all purposes to “avoid redundancy and unnecessary user effort.” *See* Ex. 1056 ¶ 13.

Additionally, we disagree with Patent Owner that the Reply includes “untimely examples” based on the “personalized currency with the user’s photo” and the “picture of the recipient” in name box 202. *See* Sur-reply 6. For the “receive” and “associate” requirements in limitation 1.2, the Petition

identified for “either sender or recipient” the “virtual likeness of a face (‘photograph image’) of an account holder.” Pet. 26–28; *see* Ex. 1003 ¶¶ 80, 82. For the “render” requirement in limitation 1.3, the Petition identified the “personalized currency with the user’s photo” for a sender account holder and the “picture of the recipient” in name box 202 for a recipient account holder. Pet. 29–31; *see* Ex. 1003 ¶¶ 86–87.

The Response argued that the Petition failed to identify the same “virtual likeness” of either a sender account holder or a recipient account holder that satisfies each of the “receive,” “associate,” and “render” requirements in limitations 1.2 and 1.3. Resp. 17; *see id.* at 17–19.

The Reply addressed that argument in the Response by explaining in more detail and using examples based on disclosures relied on generally in the Petition how the “personalized currency with the user’s photo” for a sender account holder and the “picture of the recipient” in name box 202 for a recipient account holder are each the same “virtual likeness” and satisfy each of the “receive,” “associate,” and “render” requirements in limitations 1.2 and 1.3. *See* Reply 2–16.

Petitioner’s explanation in the Reply properly responds to Patent Owner’s argument in the Response about alleged inadequacies in the Petition for limitations 1.2 and 1.3. *See* Resp. 17–19; Reply 2–16; *Rembrandt Diagnostics, LP v. Alere, Inc.*, 76 F.4th 1376, 1384–85 (Fed. Cir. 2023) (determining that motivation-to-combine arguments in a petitioner reply properly addressed arguments in a patent owner response); *Apple Inc. v. Andrea Elecs. Corp.*, 949 F.3d 697, 706–07 (Fed. Cir. 2020) (“*Andrea Elecs.*”) (determining that unpatentability arguments in a petitioner

reply properly addressed arguments in a patent owner response); 37 C.F.R. § 42.23(b).

(d) Limitation 1.4

Claim 1 requires a processor configured to “render a transaction icon associated with an electronic transaction, wherein the transaction icon is rendered in the interface with the virtual likeness of the face of the account holder.” Ex. 1001, 13:64–67 (limitation 1.4).

(i) Petitioner’s Contentions

Petitioner contends that Stone teaches limitation 1.4 because Stone’s Figure 2 illustrates display 200 on an electronic device including the following “control elements” corresponding to “transaction 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 [as] noted in [funds] box 204”;
- (4) “\$ Send money” button at the bottom of the display; and
- (5) currency representing the amount to be transferred, e.g., actual currency or personalized currency.

Pet. 31–32 (citing Ex. 1003 ¶ 90); *see id.* at 49, 71.

Further, Petitioner asserts that “to the extent” Stone does not explicitly describe a “control element” as a “transaction icon,” an ordinarily skilled artisan “would have been motivated to implement the control elements using a transaction icon, because icon and button are alternative design choices for control elements, and using transaction icons provides ‘a more visually rich interface.’” Pet. 32–33 (quoting Ex. 1008 ¶ 16) (citing Ex. 1003 ¶ 91; Ex. 1008 ¶¶ 4, 20, 24–25, 36, 38).

(ii) Patent Owner's Contentions

Patent Owner disputes that Stone teaches limitation 1.4 because limitation 1.4 requires the same “virtual likeness of the face of the account holder” as limitations 1.2 and 1.3 and, according to Patent Owner, Petitioner fails to identify the same “virtual likeness” for each of limitations 1.2, 1.3, and 1.4. *See* Resp. 15–19; Sur-reply 2–7.

(iii) Analysis

For the reasons stated by Petitioner and supported by Dr. Jones's testimony, we agree with Petitioner that Stone teaches limitation 1.4. *See* Pet. 31–33; Ex. 1003 ¶¶ 89–92, 125. For instance, Stone's Figure 2 illustrates display 200 on an electronic device including, among other things, funding source box 206 corresponding to the claimed “transaction icon.” Ex. 1008 ¶ 24, Fig. 2; *see* Ex. 1003 ¶ 90; Ex. 1056 ¶ 37. As representative funding sources, Stone identifies “PayPal, a bank, a credit card, a debit card, etc.” Ex. 1008 ¶ 34; *see* Ex. 1003 ¶ 125. 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 ¶ 125; Ex. 1056 ¶ 38.

Further, Stone's Figure 2 shows funding source box 206 rendered in the same interface that renders “the virtual likeness of the face of the account holder,” i.e., the “personalized currency with the user's photo” for a sender account holder and the “picture of the recipient” in name box 202 for a recipient account holder. Ex. 1008 ¶ 24, Fig. 2; *see* Ex. 1003 ¶¶ 90, 125; Ex. 1056 ¶¶ 5–7, 11, 13–14.

For these reasons and the reasons discussed above for limitations 1.2 and 1.3, we disagree with Patent Owner that Petitioner fails to identify the same “virtual likeness” for each of limitations 1.2, 1.3, and 1.4. *See* Resp. 15–19; Sur-reply 2–7; *supra* § III.D.5(c)(v).

(e) Limitation 1.5

Claim 1 requires a processor configured to “receive an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the account holder.” Ex. 1001, 14:1–4 (limitation 1.5).

(i) Petitioner’s Contentions

Petitioner contends that Stone teaches limitation 1.5 because Stone discloses one or more processors that are configured to “receive an indication of an action taken by a user” for interactions with the “transaction icons” identified for limitation 1.4, such as the “\$ Send money” button, name box 202 indicating the recipient, and funding source box 206 indicating the source or account. Pet. 34–35; *see id.* at 71. Referencing the “\$ Send money” button as an example, Petitioner asserts that “in response to a user interaction with (e.g., clicking/tapping on) the ‘\$ Send Money’ icon, the one or more processors receive an indication of user action for initiating a send money transaction request, and in response, a corresponding interface 200 for a send money transaction is displayed.” *Id.* at 35.

Further, Petitioner asserts that “[i]t was well-known that user clicking/tapping on/sliding/dragging (including from/to) an icon discloses an ‘an interaction by a user with an icon’ as claimed.” Pet. 35 (citing Ex. 1003 ¶ 96; Ex. 1008 ¶¶ 20, 24, 36).

(ii) Patent Owner's Contentions

Patent Owner disputes that Stone teaches limitation 1.5 because limitation 1.5 requires the same “virtual likeness of the face of the account holder” as limitations 1.2, 1.3, and 1.4 and, according to Patent Owner, Petitioner fails to identify the same “virtual likeness” for each of limitations 1.2, 1.3, 1.4, and 1.5. *See* Resp. 15–19; Sur-reply 2–7.

(iii) Analysis

For the reasons stated by Petitioner and supported by Dr. Jones's testimony, we agree with Petitioner that Stone teaches limitation 1.5. *See* Pet. 33–36; Ex. 1003 ¶¶ 90–91, 93–98, 125. For example, Stone explains for funding source box 206 that a user “selects a funding source, such as PayPal, a bank, a credit card, a debit card, etc.” Ex. 1008 ¶ 34, Fig. 3 (step 314); *see* Ex. 1003 ¶¶ 96, 125. Once the user “selects a funding source,” the user device may display (1) “the specific card, such as a PayPal card, Visa, MC, AMEX, etc.,” and (2) “the current balance in the funding source” in balance area 208. Ex. 1008 ¶¶ 24, 34, 38, Fig. 2; *see* Ex. 1003 ¶¶ 91, 125; Ex. 1056 ¶¶ 14, 38. 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.” Ex. 1008 ¶ 35.

When the user “selects a funding source” or “switch[es] the funding source to a different account,” the user interacts with funding source box 206 rendered in the same interface that renders “the virtual likeness of the face of the account holder,” i.e., the “personalized currency with the user's photo” for a sender account holder and the “picture of the recipient” in name box 202 for a recipient account holder. Ex. 1008 ¶¶ 24, 34–35, Figs. 2–3;

see Ex. 1003 ¶¶ 90, 95–96, 125; Ex. 1056 ¶¶ 5–7, 11, 13–14. As Dr. Jones explains, “[i]n response to a user interaction with (e.g., selecting/clicking) funding icon 206, the processor receives an indication of funding resource selection (e.g., block 314 of FIG. 3).” Ex. 1003 ¶ 96.

For these reasons and the reasons discussed above for limitations 1.2, 1.3, and 1.4, we disagree with Patent Owner that Petitioner fails to identify the same “virtual likeness” for each of limitations 1.2, 1.3, 1.4, and 1.5. *See* Resp. 15–19; Sur-reply 2–7; *supra* §§ III.D.5(c)(v), III.D.5(d)(iii).

(f) Limitation 1.6

Claim 1 requires a processor configured to “capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information associated with a user.” Ex. 1001, 14:5–8 (limitation 1.6).

Petitioner contends that the combined disclosures in Stone and Hoyos teach limitation 1.6. *See* Pet. 36–41. Specifically, Petitioner asserts that Hoyos discloses fraud-resistant biometric authentication including:

- (1) “capturing biometric contextual information (e.g., ‘acquiring biometric data from a person’ including images, palm temperature, etc.) used for fraud detection”;
- (2) using “some captured biometric information (e.g., facial images, ‘finger or palm temperature’)” to compute a “probability of liveness”; and
- (3) using “some captured biometric information (e.g., facial images, iris, fingerprint image, finger vein image, palm vein image, or ‘other imagery’)” to compute a “probability of biometric match.”

Id. at 36–37 (quoting Ex. 1013 ¶¶ 12, 21) (citing Ex. 1003 ¶ 100; Ex. 1013 ¶ 17, Fig. 1).

Petitioner also asserts that Hoyos discloses “techniques for capturing the set of biometric information for liveness analysis, where a camera (web-camera 26) is used to capture a set of images.” Pet. 38. As support, Petitioner quotes the following language 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.* (quoting Ex. 1013, claim 7).

Further, as discussed above, Petitioner asserts that an ordinarily skilled artisan would have used Hoyos’s biometric authentication in Stone’s system for financial transactions to achieve various advantages. Pet. 40 (citing Ex. 1003 ¶ 103; Ex. 1013 ¶ 15); *see supra* § III.D.4(a)(i).

Patent Owner makes no arguments specific to limitation 1.6. *See, e.g.*, Resp. 14–34; Sur-reply 2–26.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that the combined disclosures in Stone and Hoyos teach limitation 1.6. *See* Pet. 36–41; Ex. 1003 ¶¶ 99–104.

(g) Limitation 1.7

Claim 1 requires a processor configured to “perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises determining, based at least in part on the captured biometric information, that the user is alive.” Ex. 1001, 14:9–15 (limitation 1.7).

Petitioner contends that the combined disclosures in Stone and Hoyos teach limitation 1.7. *See* Pet. 41–44. Specifically, Petitioner explains that in the proposed combination Hoyos’s biometric authentication would:

- (1) perform “a fraud detection analysis of the captured contextual information that includes determining, based on the captured biometric information, that the user is alive”; and
- (2) provide “an authentication decision based on a combination of liveness analysis (e.g., based on captured images, finger or palm temperatures) and biometric match (e.g., based on captured facial features, iris, fingerprint, finger vein, palm vein, etc.).”

Id. at 41–42 (citing Ex. 1003 ¶¶ 106–107; Ex. 1013 ¶¶ 17–22, 40, claims 1 and 5–8).

To support its contentions, Petitioner provides the following annotated version of Hoyos’s Figure 1 (Pet. 43):

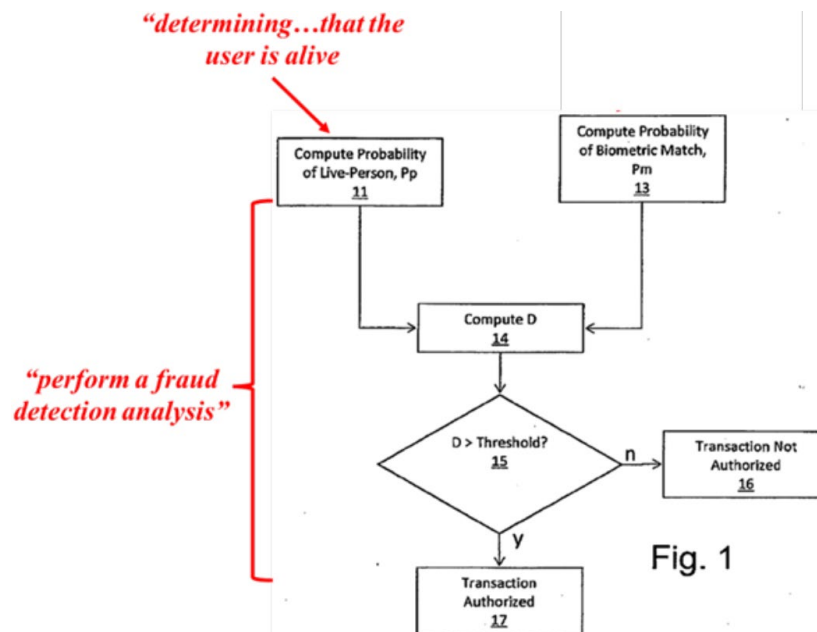


Figure 1 illustrates a flowchart for a biometric authentication system. Ex. 1013 ¶¶ 2, 32–33, Fig. 1. The above annotated version of Figure 1 includes the following annotations:

- (1) the red annotation “*determining . . . that the user is alive*” identifying the flowchart step for computing a probability of liveness, Pp (step 11); and

- (2) the red annotation “*perform a fraud detection analysis*” identifying the flowchart steps for (i) computing a probability of liveness, Pp (step 11), (ii) computing a probability of a match, Pm (step 13), (iii) computing an authentication decision, D, based on a combination of Pp and Pm (step 14), (iv) determining if D exceeds a preset threshold (step 15), (v) not authorizing the transaction if D fails to exceed the preset threshold (step 16), and (vi) authorizing the transaction if D exceeds the preset threshold (step 17).

Pet. 43; *see* Ex. 1003 ¶ 107; Ex. 1013 ¶ 33.

Patent Owner makes no arguments specific to limitation 1.7. *See, e.g.*, Resp. 14–34; Sur-reply 2–26.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that the combined disclosures in Stone and Hoyos teach limitation 1.7. *See* Pet. 41–44; Ex. 1003 ¶¶ 105–110.

(h) Limitation 1.8

Claim 1 requires a processor configured to “complete the electronic transaction” based “at least in part on both the user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the account holder and performing the fraud detection analysis comprising determining that the user is alive based at least in part on the captured biometric information.” Ex. 1001, 14:16–22 (limitation 1.8).

Petitioner contends that the combined disclosures in Stone and Hoyos teach limitation 1.8. *See* Pet. 44–46. Specifically, Petitioner asserts that the combined disclosures in Stone and Hoyos teach the claimed “user interaction with the transaction icon” and the claimed “fraud detection analysis” for the reasons discussed for preceding limitations. *Id.* at 44.

Further, Petitioner asserts that the combined disclosures in Stone and Hoyos teach the claimed “complete the electronic transaction” because Stone’s Figure 3 shows “Transfer Funds” in step 318. Pet. 44–45. Petitioner explains that in the proposed combination “the transaction is completed after and based on” both of the following:

- (1) “the user interaction (e.g., ‘\$ Send money,’ ‘214 Send’/block 316 (‘confirm’)) to indicate that the user initiates, continues, and confirms to complete the transaction”; and
- (2) “the transaction authenticated decision by the fraud detection analysis” according to Hoyos.

Id. at 45–46 (emphasis omitted).

Patent Owner makes no arguments specific to limitation 1.8. *See, e.g.,* Resp. 14–34; Sur-reply 2–26.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, and the reasons discussed above for limitation 1.5 (“user interaction with the transaction icon”) and limitation 1.7 (“fraud detection analysis”), we agree with Petitioner that the combined disclosures in Stone and Hoyos teach limitation 1.8. *See* Pet. 33–36, 41–46; Ex. 1003 ¶¶ 93–98, 105–115, 125; *supra* §§ III.D.5(e)(iii), III.D.5(g).

(i) Limitation 1.9

Claim 1 recites “a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.” Ex. 1001, 14:23–25 (limitation 1.9).

(i) Petitioner’s Contentions

Petitioner contends that Stone teaches limitation 1.9 and alternatively that the combined disclosures in Stone and Hoyos teach limitation 1.9. *See*

Pet. 26, 46–47; Reply 16–19. Specifically, Petitioner asserts that Stone discloses:

- (1) “one or more processors (e.g., processor 504 in user device 404 alone, or in combination with other processors including the processor 504 of payment provider device 408)” configured to “perform processes for an electronic transaction”;
- (2) “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”; and
- (3) “the memory is configured to provide the processor with instructions,” such as “instructions contained in system memory component 506” that “create and display the proper currencies, convert currency, display various types of graphics showing transfer of currency, etc.”

Pet. 46–47 (quoting Ex. 1008 ¶ 50) (citing Ex. 1008 ¶¶ 49, 54, Fig. 5); *see id.* at 24, 78.

Petitioner contends that the claimed “a memory” does not need to provide “instructions” to the “one or more processors” for causing the “one or more processors” to perform each of limitations 1.2–1.8. Reply 18. According to Petitioner, the plain and ordinary meaning of the term “instructions” in light of the patent’s specification is not limited to performing each of limitations 1.2–1.8. *Id.* at 18–19 (citing Ex. 1001, 1:67–2:1, 2:11–13).

Further, Petitioner asserts that even if the claimed “a memory” must provide “instructions” to the “one or more processors” for causing the “one or more processors” to perform each of limitations 1.2–1.8, the “combination of Stone and Hoyos” still renders limitation 1.9 obvious. Reply 16–17. Specifically, for Petitioner’s example 1.1 where one processor

in sender user device 404 “receive[s],” “associate[s],” and “render[s]” the same “virtual likeness” of the face of a recipient account holder, Petitioner explains that if sender user device 404 also performs “client-side authentication,” then one processor in sender user device 404 performs each of limitations 1.2–1.8 according to instructions provided by one memory in sender user device 404. *Id.* at 17. Similarly, for Petitioner’s example 2.1 where one processor in sender user device 404 “receive[s],” “associate[s],” and “render[s]” the same “virtual likeness” of the face of a sender account holder, Petitioner explains that if sender user device 404 also performs “client-side authentication,” then one processor in sender user device 404 performs each of limitations 1.2–1.8 according to instructions provided by one memory in sender user device 404. *Id.*

(ii) Patent Owner’s Contentions

Patent Owner disputes that Stone teaches limitation 1.9. *See* Resp. 19–22; Sur-reply 18–22. In particular, Patent Owner contends that the claimed “a memory” must provide “instructions” to the “one or more processors” for causing the “one or more processors” to perform each of limitations 1.2–1.8. Sur-reply 20–21 (citing Ex. 1050, 59:3–8); *see* Resp. 21–22. Patent Owner also contends that the claimed “a memory” would be “superfluous and otherwise irrelevant to the claim” if the claimed “a memory” did not provide instructions to the “one or more processors” for causing the “one or more processors” to perform each of limitations 1.2–1.8. Sur-reply 21 (citing *Power Mosfet Techs., L.L.C. v. Siemens AG*, 378 F.3d 1396, 1410 (Fed. Cir. 2004)).

Further, Patent Owner asserts that Petitioner relies on the processor in sender user device 404 and the processor in payment provider server 408 for

performing limitations 1.2–1.8 but fails to identify “a single memory coupled to both the processors for the user device and the payment server.” Resp. 21–22; *see* Sur-reply 19–22. Patent Owner also asserts that a “separate memory (506) coupled to the processor (504) of the user device” and a “separate memory (506) coupled to the processor (504) of the payment server” do not satisfy limitation 1.9. Resp. 22.

Additionally, Patent Owner contends that Petitioner’s examples 1.1 and 2.1 with “client-side authentication” do not render limitation 1.9 obvious. *See* Sur-reply 19, 21–22. Specifically, Patent Owner asserts that user device processor 404 does not perform each of limitations 1.2, 1.3, 1.4, and 1.5 and, therefore, “cannot be ‘the one or more processors’ coupled to ‘a memory’” for limitation 1.9. *Id.* at 19 (emphasis omitted); *see id.* at 21–22. Patent Owner also asserts that user device memory 506 “does not provide the necessary instructions to perform” each of limitations 1.2–1.8 to user device processor 504 because user device processor 504 “does not perform these limitations.” *Id.* at 21; *see id.* at 21–22.

(iii) Analysis

For the reasons explained below, we agree with Petitioner that Stone teaches limitation 1.9 and that the combined disclosures in Stone and Hoyos teach limitation 1.9. *See* Pet. 26, 46–47; Reply 16–19; Ex. 1003 ¶¶ 116–119; Ex. 1056 ¶¶ 18–26.

First, we disagree with Patent Owner that limitation 1.9 requires “a single memory coupled to” the “one or more processors.” *See* Resp. 19–22; Sur-reply 1, 19–22. Limitation 1.9 recites “a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.” Ex. 1001, 14:23–25. 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, e.g.*, Resp. 19–22; Sur-reply 18–22. For example, limitations 1.2–1.8 do not reference “the” or “said” memory in limitation 1.9. *See* Ex. 1001, 13:58–14:22. 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 1:63–2:10. 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).

We disagree with Patent Owner’s contention that the claimed “a memory” would be “superfluous and otherwise irrelevant to the claim” if the claimed “a memory” did not provide instructions to the “one or more

processors” for causing the “one or more processors” to perform each of limitations 1.2–1.8. *See* Sur-reply 21. If one or more memories provided instructions to the “one or more processors” for causing the “one or more processors” to perform each of limitations 1.2–1.8, that would not render the claimed “a memory” “superfluous and otherwise irrelevant to the claim” because the claimed “a memory” encompasses one or more memories. *See KCJ*, 223 F.3d at 1356.

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 ¶ 75. 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 ¶ 118. 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 ¶ 118. 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 ¶ 118.

Third, for the reasons discussed above, the combined disclosures in Stone and Hoyos teach limitations 1.2–1.8 performed by “one or more processors” according to limitation 1.1. *See supra* §§ III.D.5(b)–(h). To permit the “one or more processors” to perform limitations 1.2–1.8, one or more memories in the proposed Stone-Hoyos combination provide the “one or more processors” with instructions. *See* Ex. 1003 ¶¶ 117–119. 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 ¶¶ 75, 118. Hence, in the proposed Stone-Hoyos 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 ¶¶ 117–119; Ex. 1056 ¶¶ 5–7, 9–11, 13–14, 16–22, 26.

Fourth, even if claim 1 required that one processor perform each of limitations 1.2–1.8 according to instructions provided by one memory, the combined disclosures in Stone and Hoyos teach that arrangement. *See* Ex. 1056 ¶¶ 5–7, 11, 13–14, 19–21, 26. Specifically, for Petitioner’s example 1.1 where one processor in sender user device 404 “receive[s],” “associate[s],” and “render[s]” the same “virtual likeness” of the face of a recipient account holder, if sender user device 404 also performs “client-side authentication,” then one processor in sender user device 404 performs each of limitations 1.2–1.8 according to instructions provided by one memory in sender user device 404. *Id.* ¶¶ 5–7, 19–21, 26. Similarly, for Petitioner’s example 2.1 where one processor in sender user device 404 “receive[s],” “associate[s],” and “render[s]” the same “virtual likeness” of the face of a sender account holder, if sender user device 404 also performs “client-side authentication,” then one processor in sender user device 404 performs each of limitations 1.2–1.8 according to instructions provided by one memory in sender user device 404. *Id.* ¶¶ 11, 13–14, 19–21, 26.

(j) Conclusion Concerning Obviousness/Nonobviousness for Claim 1

For the reasons discussed above, the combined disclosures in Stone and Hoyos teach claim 1's subject matter. *See supra* §§ III.D.5(a)–(i). Moreover, an ordinarily skilled artisan would have been motivated to combine Hoyos's teachings with Stone's teachings in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.D.4(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 and Hoyos.

6. INDEPENDENT CLAIMS 9 AND 17

Claim 9 recites a “method” in its preamble and includes limitations similar to claim 1. *Compare* Ex. 1001, 13:56–14:25 (claim 1), *with id.* at 14:43–15:7 (claim 9). Claim 17 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 13:56–14:25 (claim 1), *with id.* at 15:25–16:4 (claim 17).

Petitioner identifies disclosures in Stone corresponding to claim 9's preamble and claim 17's preamble. Pet. 53–55. For a “method” according to claim 9's preamble, Petitioner asserts that Stone's Figure 3 illustrates steps in a “method for fund transfer.” *Id.* at 53–54 (citing Ex. 1008 ¶¶ 29–36, Fig. 3). For a “computer program product embodied in a non-transitory computer readable storage medium” according to claim 17'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 55 (citing Ex. 1003 ¶ 149; Ex. 1008 ¶ 54).

Patent Owner makes no arguments specific to claim 9's preamble or claim 17's preamble. *See, e.g.*, Resp. 14–36, 15 n.1; Sur-reply 2–27.

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 9 and 17 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 9 and 17. *See* Pet. 53–55; Ex. 1003 ¶¶ 134–136, 148–150.

Additionally, Petitioner contends that the combined disclosures in Stone and Hoyos teach the subject matter in claims 9 and 17 for the reasons that the combined disclosures teach claim 1's subject matter. *See* Pet. 54–56. Dr. Jones's testimony supports Petitioner's contentions. *See* Ex. 1003 ¶¶ 137–143, 151–157.

Patent Owner disputes that the combined disclosures in Stone and Hoyos teach the subject matter in claims 9 and 17 for the same reasons Patent Owner disputes that the combined disclosures teach claim 1's subject matter. *See* Resp. 14–34, 15 n.1; Sur-reply 2–26.

For the reasons discussed above, we consider Patent Owner's patentability arguments about claim 1 unavailing. *See supra* §§ III.D.4(c), III.D.5(b)(iii), III.D.5(c)(v), III.D.5(d)(iii), III.D.5(e)(iii), III.D.5(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 and Hoyos teach the subject matter in claims 9 and 17. *See* Pet. 53–56; Ex. 1003 ¶¶ 134–143, 148–157; *supra* §§ III.D.5(a)–(i). Moreover, an ordinarily skilled artisan would have been motivated to combine Hoyos's teachings with Stone's teachings in the way

Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.D.4(c). Hence, Petitioner has shown by a preponderance of the evidence that claims 9 and 17 are unpatentable under § 103(a) because the claims would have been obvious over Stone and Hoyos.

7. DEPENDENT CLAIMS 2, 4–6, 10, 12–14, 20, 21, AND 23

(a) Claims 2 and 10

Claim 2 depends directly from claim 1 and specifies that “the transaction icon includes a graphical representation of an amount of money.” Ex. 1001, 14:26–27. Claim 10 depends directly from claim 9 and includes a limitation similar to claim 2. *Id.* at 15:8–9.

Petitioner contends that Stone teaches the limitations in claims 2 and 10 because Stone discloses “transaction icons” including “virtual currency” that appears on a user device’s display as “a graphical representation of an amount of money.” Pet. 47, 55; *see id.* at 31–32. As support, Petitioner quotes Stone’s disclosure that a user device may display “currency representing the entered amount,” such as “one twenty dollar bill, one five dollar bill, one one dollar bill, one quarter, one nickel, and two pennies.” *Id.* at 47–48 (emphasis omitted) (quoting Ex. 1008 ¶¶ 6, 23).

As further support, Petitioner provides the following annotated version of Stone's Figure 2 (Pet. 48):

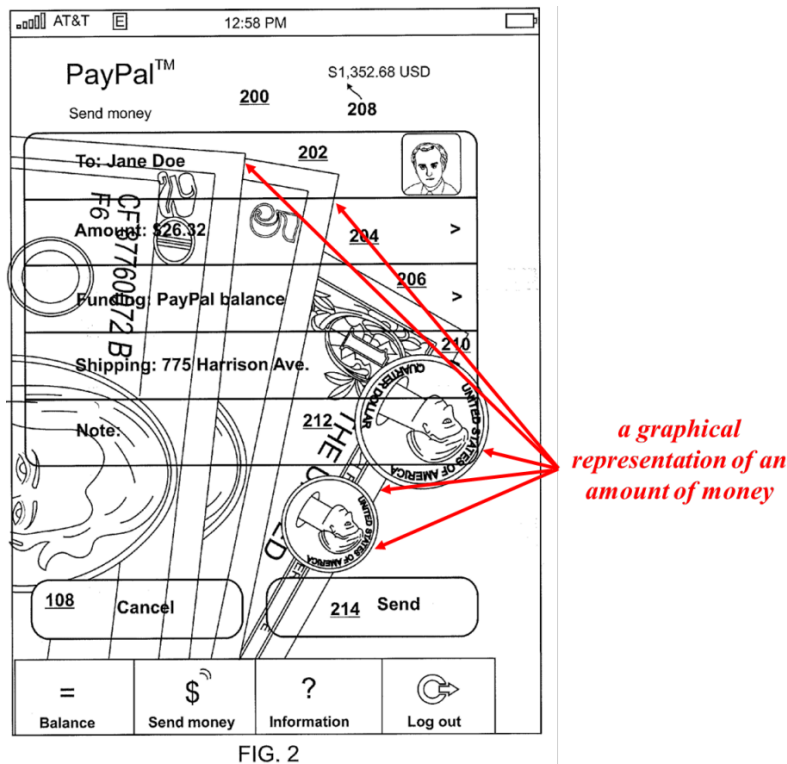


Figure 2 illustrates display 200 on an electronic device including various display elements. Ex. 1008 ¶¶ 11, 24, Fig. 2. The above annotated version of Figure 2 includes the red annotation “a graphical representation of an amount of money” identifying “personalized currency with the user’s photo” indicating “the amount entered by the user” in the background of the display. Pet. 48; *see* Ex. 1003 ¶ 122; Ex. 1008 ¶¶ 7, 16.

Patent Owner makes no arguments specific to claims 2 and 10. *See, e.g.,* Resp. 34–36; Sur-reply 26–27.

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 10. *See* Pet. 47–48, 55; Ex. 1003 ¶¶ 120–123, 144.

(b) Claims 4 and 12

Claim 4 depends directly from claim 1 and specifies that “the transaction icon includes a graphical representation of a payment form.” Ex. 1001, 14:30–31. Claim 12 depends directly from claim 9 and includes a limitation similar to claim 4. *Id.* at 15:12–13.

(i) Petitioner’s Contentions

Petitioner contends that Stone teaches the limitations in claims 4 and 12 because Stone discloses:

- (1) funding source box 206 in Figure 2 corresponding to the claimed “transaction icon”;
- (2) step 314 for “Enter Funding Source” in Figure 3 related to funding source box 206 in Figure 2;
- (3) the user “clicking 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. 49, 55 (emphasis omitted) (quoting Ex. 1008 ¶ 35) (citing Ex. 1008 ¶¶ 4, 24, 34, Fig. 2); *see* Reply 23 (citing Ex. 1056 ¶ 37). Further, Petitioner asserts that funding source box 206 may represent “a payment form,” such as “PayPal, a bank, a credit card, a debit card, etc.” Pet. 49 (quoting Ex. 1008 ¶ 34).

Additionally, Petitioner contends that Stone teaches “a graphical representation of a payment form” for a selected funding source 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. 49 (emphasis omitted) (quoting Ex. 1008 ¶ 38); Reply 23 (quoting Ex. 1008 ¶ 38).

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. 49–50 (citing Ex. 1003 ¶ 125; Ex. 1008 ¶ 4); *see* Reply 23–24 (citing Ex. 1056 ¶ 38).

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. 50 (citing Ex. 1003 ¶ 126); *see* Reply 24 (citing Ex. 1056 ¶ 39).

(ii) Patent Owner’s Contentions

Patent Owner disputes that Stone teaches the limitations in claims 4 and 12. *See* Resp. 34–35; Sur-reply 26–27. In particular, Patent Owner contends that “[n]either Stone nor Hoyos discloses that a transaction icon can be a payment form.” Resp. 34.

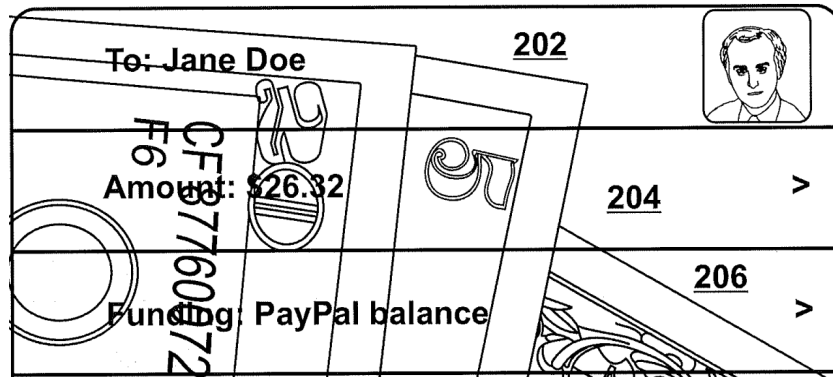
Patent Owner also contends that Petitioner provides “no explanation or justification why” it would have been obvious to an ordinarily skilled artisan to “implement the funding source selection [of Stone Fig. 2] using an icon” representing “a payment form” without working “backward” from the claims using hindsight. Resp. 34–35 (alteration by Patent Owner) (quoting Pet. 49) (citing Ex. 2032 ¶ 63); *see* Sur-reply 26–27.

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 “nothing more than hindsight.” Resp. 35 (citing Ex. 2032 ¶¶ 62–64).

(iii) Analysis

We agree with Petitioner that Stone teaches the limitations in claims 4 and 12. *See* Pet. 49–51; Reply 22–24; Ex. 1003 ¶¶ 124–127, 145; Ex. 1056 ¶¶ 36–40; Tr. 42:9–43:9. Specifically, Stone’s Figure 2 illustrates display 200 on an electronic device including, among other things, funding source box 206 corresponding to the claimed “transaction icon.” Ex. 1008 ¶ 24, Fig. 2; *see* Ex. 1003 ¶¶ 90, 125; Ex. 1056 ¶ 37. As representative funding sources, Stone identifies “PayPal, a bank, a credit card, a debit card, etc.” Ex. 1008 ¶ 34; *see* Ex. 1003 ¶ 125. 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 ¶ 125; Ex. 1056 ¶ 38. When funding source box 206 displays “the specific card, such as a PayPal card, Visa, MC, AMEX, etc.,” “the transaction icon includes a graphical representation of a payment form” according to claims 4 and 12. *See* Ex. 1003 ¶ 125; Ex. 1056 ¶¶ 37–38; Tr. 42:9–43:9.

For example, the following excerpt from Stone's Figure 2 shows that funding source box 206 includes "a graphical representation of a payment form":



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 graphical representation of a payment form" according to claims 4 and 12. *See* Tr. 42:9–43:9.

We disagree with Patent Owner that Petitioner worked "backward" from the claims using hindsight. *See* Resp. 34–35; Sur-reply 26–27. Petitioner provides an explicit analysis about how Stone teaches the limitations in claims 4 and 12 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. 49–50; Reply 23–24; Ex. 1003 ¶ 125; Ex. 1056 ¶¶ 37–38.

(c) Claims 5 and 13

Claim 5 depends directly from claim 1 and specifies that “the virtual likeness comprises a photograph of the account holder.” Ex. 1001, 14:32–33. Claim 13 depends directly from claim 9 and includes a limitation similar to claim 5. *Id.* at 15:14–15.

Petitioner contends that Stone teaches the limitations in claims 5 and 13 because Stone discloses a user device that displays (1) a “picture of the recipient” in name box 202 and (2) “personalized currency with the user’s photo” indicating “the amount entered by the user” in the background of the display. Pet. 29–31, 47–48, 51–52 (emphasis omitted).

Patent Owner makes no arguments specific to claims 5 and 13. *See, e.g.*, Resp. 34–36; Sur-reply 26–27.

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 13. *See* Pet. 29–31, 47–48, 51–52; Ex. 1003 ¶¶ 86, 122, 128–130, 146.

(d) Claims 6 and 14

Claim 6 depends directly from claim 1 and specifies that “the virtual likeness comprises an avatar selected by the account holder.” Ex. 1001, 14:34–35. Claim 14 depends directly from claim 9 and includes a limitation similar to claim 6. *Id.* at 15:16–17.

(i) Petitioner’s Contentions

Petitioner contends that Stone renders the limitations in claims 6 and 14 obvious because (1) “Stone’s electronic transaction system provides a social networking aspect for connecting people” and (2) a “user-selected avatar [was] a well-known user icon option for online identity” as an

alternative to a photograph of an account holder. Pet. 52–53, 55 (citing Ex. 1003 ¶ 132); Reply 24.

Further, Petitioner asserts that an ordinarily skilled artisan “would have been motivated to provide the option of user selection of an avatar as a user icon (e.g., for profile icon as sender, recipient, or other users, or on visual currency)” because:

- (1) an “avatar was a well-known alternative design choice of pictures for user icon”;
- (2) an “avatar has the benefits of providing an online identity that balances personal expression and privacy”; and
- (3) a “user picture has the benefits of enhanced personal recognition and trust.”

Pet. 53 (citing Ex. 1003 ¶ 132; Ex. 1047, 801);¹¹ *see* Reply 24–25.

(ii) Patent Owner’s Contentions

Patent Owner disputes that Stone renders the limitations in claims 6 and 14 obvious. *See* Resp. 35–36; Sur-reply 27. Regarding Petitioner’s assertion that a “user-selected avatar [was] a well-known user icon option for online identity,” Patent Owner contends that “[t]he fact that a claim element is well known does not render it obvious.” Resp. 36. Patent Owner also contends that Petitioner offers “no justification why it would be obvious to use an avatar for an electronic payment system.” *Id.*

Further, Patent Owner asserts that replacing any of the images that Petitioner relies on from Stone with an avatar would not meet the

¹¹ For Exhibit 1047 (paper titled “Avatars in Social Media: Balancing Accuracy, Playfulness and Embodied Messages”), we cite to the page numbers that appear in the publication instead of the page numbers that Petitioner applied to the exhibit.

requirements in claims 6 and 14 because “Stone fails to disclose a single virtual likeness that meets all the requirements” in claims 1 and 9.

Sur-reply 27.

(iii) Analysis

We agree with Petitioner that Stone renders the limitations in claims 6 and 14 obvious. *See* Pet. 52–53; Reply 24–25; Ex. 1003 ¶¶ 131–133, 147; Ex. 1056 ¶¶ 42–43. As Petitioner asserts, a “user-selected avatar [was] a well-known user icon option for online identity” as an alternative to a photograph of an account holder. *See* Pet. 52–53; Ex. 1003 ¶ 132; Ex. 1009, 1:21–31, 9:30–36; Ex. 1046 ¶ 34 (describing a user’s “profile information” as including “an image,” including “any type of a graphic representation, avatar, photo, etc.”); Ex. 1047, 801; Ex. 1056 ¶ 42.

As Petitioner also asserts, an ordinarily skilled artisan “would have been motivated to provide the option of user selection of an avatar as a user icon” instead of the “photograph image” disclosed in Stone because an “avatar has the benefits of providing an online identity that balances personal expression and privacy.” *See* Pet. 53; Ex. 1003 ¶ 132; Ex. 1047, 801; Ex. 1056 ¶¶ 42–43. For instance, a 2008 paper titled “Avatars in Social Media: Balancing Accuracy, Playfulness and Embodied Messages” explains that avatars not only “maintain users’ privacy” but also “give expressive freedom over an otherwise static online identity.” Ex. 1047, 801. Because “using a user selected avatar and using a picture are the alternative predictable solutions for implementing the user icon in Stone-Hoyos,” an ordinarily skilled artisan would have had “a good reason for using an avatar for an electronic payment system.” Ex. 1056 ¶ 42.

Accordingly, we disagree with Patent Owner that Petitioner offers “no justification why it would be obvious to use an avatar for an electronic payment system.” *See* Resp. 36.

As for Patent Owner’s assertion that replacing any of the images that Petitioner relies on from Stone with an avatar would not meet the requirements in claims 6 and 14 because “Stone fails to disclose a single virtual likeness that meets all the requirements” in claims 1 and 9, we disagree. *See* Sur-reply 27. For the reasons discussed above for limitations 1.2, 1.3, 1.4, and 1.5, Stone discloses “a single virtual likeness that meets all the requirements” in claims 1 and 9. *See supra* §§ III.D.5(c)–(e).

(e) Claim 20

Claim 20 depends directly from claim 1 and specifies that “the captured biometric information associated with the user includes a fingerprint.” Ex. 1001, 16:18–19.

Petitioner contends that the combined disclosures in Stone and Hoyos teach claim 20’s limitation. Pet. 56–57. Specifically, Petitioner asserts that Hoyos discloses “capturing biometric information associated with a user for fraud detection,” including “fingerprint matching.” *Id.* at 56 (citing Ex. 1013 ¶¶ 12, 15, 17–22). As support, Petitioner quotes Hoyos’s disclosure about “biometric recognition systems using fingerprint” or other imagery. *Id.* (emphasis omitted) (quoting Ex. 1013 ¶ 12). Further, Petitioner asserts that “use of a fingerprint is also consistent with Stone’s disclosure of ‘biometric id,’ which is well-known to include fingerprint identification information for fingerprint recognition.” *Id.* (citing Ex. 1003 ¶ 160; Ex. 1008 ¶ 45; Ex. 1010 ¶ 79).

Therefore, according to Petitioner, an ordinarily skilled artisan “would have been motivated to implement capturing fingerprint for fraud detection analysis, as taught by Hoyos, for improved security, because fingerprint authentication has high accuracy, is less intrusive than face images, and is a mature and well-tested technology.” Pet. 56–57.

Patent Owner makes no arguments specific to claim 20. *See, e.g.*, Resp. 34–36; Sur-reply 26–27.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that the combined disclosures in Stone and Hoyos teach claim 20’s limitation. *See* Pet. 56–57; Ex. 1003 ¶¶ 158–161.

(f) Claim 21

Claim 21 depends directly from claim 1 and specifies that (1) “the captured biometric information comprises a plurality of photographs” and (2) “the fraud detection analysis comprises an analysis of the plurality of photographs to determine that the user is alive.” Ex. 1001, 16:20–24.

Petitioner contends that the combined disclosures in Stone and Hoyos teach claim 21’s limitations for the reasons that the combined disclosures teach limitations 1.7 and 1.8. Pet. 57. Petitioner also quotes the following language 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.* (emphases omitted) (quoting Ex. 1013, claim 7).

Patent Owner makes no arguments specific to claim 21. *See, e.g.*, Resp. 34–36; Sur-reply 26–27.

For the reasons stated by Petitioner and supported by Dr. Jones's testimony, we agree with Petitioner that the combined disclosures in Stone and Hoyos teach claim 21's limitations. *See* Pet. 57; Ex. 1003 ¶¶ 162–164; *supra* §§ III.D.5(f)–(h).

(g) Claim 23

Claim 23 reads as follows (with bracketed numbers added for reference purposes):¹²

23. [23.0] The system of claim 1 wherein the account holder comprises a first account holder, wherein the account comprises a first account, and wherein the one or more processors are further configured to:

[23.1] receive a virtual likeness of a face of a second account holder; associate, in the data store, the virtual likeness of the face of the second account holder with a second account of the second account holder; and

[23.2] render a destination image comprising the virtual likeness of the face of the second account holder; and

[23.3] wherein completing the electronic transaction based at least in part on both the user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the first account holder and performing the fraud detection analysis comprising determining that the user is alive based at least in part on the captured biometric information comprises transferring funds between the first account of the first account holder and the second account of the second account holder for which the destination image comprising the virtual likeness of the face of the second account holder was rendered.

Ex. 1001, 16:31–53.

¹² We use the same reference numbers that Petitioner uses to identify the claim language. *See* Pet. xii (Listing of Challenged Claims).

Petitioner contends that the combined disclosures in Stone and Hoyos teach claim 23's limitations for several related reasons. *See* Pet. 57–60. First, Petitioner asserts that Stone discloses a sender account holder corresponding to “a first account holder” required by limitation 23.0. *Id.* at 57 (citing Ex. 1003 ¶ 165).

Second, Petitioner asserts that Stone discloses a recipient account holder corresponding to “a second account holder” required by limitation 23.1. Pet. 57–58 (citing Ex. 1003 ¶ 166).

Third, Petitioner asserts that Stone discloses the “receive” and “associate” requirements in limitation 23.1 for the reasons that Stone discloses the “receive” and “associate” requirements in limitation 1.2 for a recipient account holder. Pet. 57–58 (citing Ex. 1003 ¶ 166).

Fourth, Petitioner asserts that Stone discloses limitation 23.2 because Stone's Figure 2 includes “the virtual likeness of the face” of a recipient account holder in name box 202 containing a “picture of the recipient.” Pet. 58. As support, Petitioner provides the following annotated version of Stone's Figure 2 (Pet. 58):

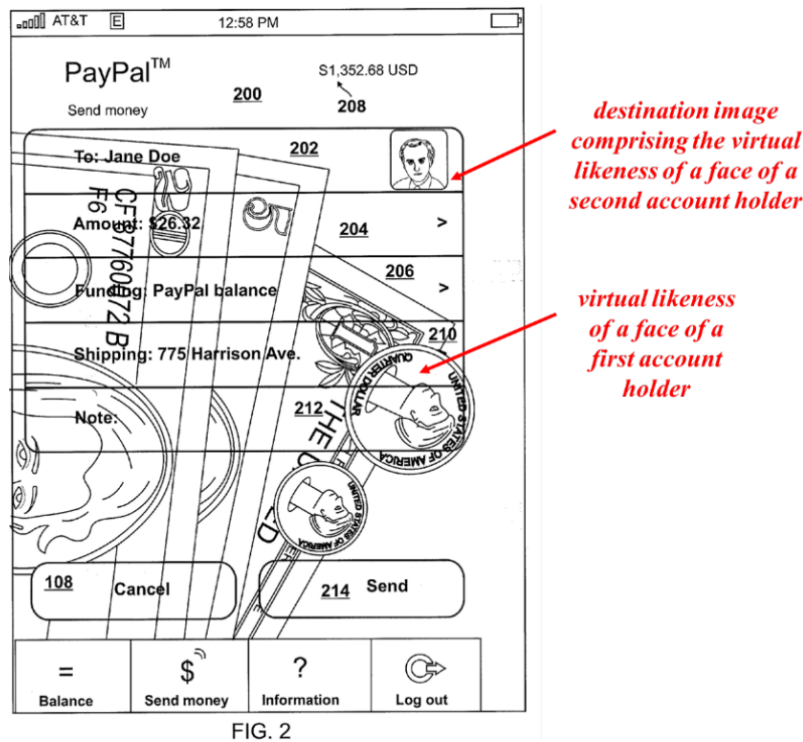


Figure 2 illustrates display 200 on an electronic device including various display elements. Ex. 1008 ¶¶ 11, 24, Fig. 2. The above annotated version of Figure 2 includes the following annotations:

- (1) the red annotation “destination image comprising the virtual likeness of a face of a second account holder” identifying a “picture of the recipient” in name box 202; and
- (2) the red annotation “virtual likeness of a face of a first account holder” identifying “personalized currency with the user’s photo” indicating “the amount entered by the user” in the background of the display.

Pet. 58; see Ex. 1003 ¶ 168; Ex. 1008 ¶¶ 7, 16, 24.

Fifth, Petitioner asserts that the combined disclosures in Stone and Hoyos teach limitation 23.3 for the reasons that the combined disclosures teach limitation 1.8. Pet. 59–60 (citing Ex. 1003 ¶¶ 170–174; Ex. 1008 ¶ 35, Figs. 2–3).

Patent Owner makes no arguments specific to claim 23. *See, e.g.*, Resp. 34–36; Sur-reply 26–27.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that the combined disclosures in Stone and Hoyos teach claim 23’s limitations. *See* Pet. 57–60; Ex. 1003 ¶¶ 165–174; *supra* §§ III.D.5(c)(v), III.D.5(h).

(h) Summary for Dependent Claims 2, 4–6, 10, 12–14, 20, 21, and 23

For the reasons discussed above, the combined disclosures in Stone and Hoyos teach the limitations in claims 2, 4–6, 10, 12–14, 20, 21, and 23. *See supra* §§ III.D.7(a)–(g). Moreover, an ordinarily skilled artisan would have been motivated to combine Hoyos’s teachings with Stone’s teachings in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.D.4(c). Hence, Petitioner has shown by a preponderance of the evidence that claims 2, 4–6, 10, 12–14, 20, 21, and 23 are unpatentable under § 103(a) because the claims would have been obvious over Stone and Hoyos.

*E. Alleged Obviousness over Stone, Hoyos,
and Varghese: Claims 7, 15, and 22*

Petitioner contends that claims 7, 15, and 22 are unpatentable under § 103(a) because the claims would have been obvious over Stone, Hoyos, and Varghese. *See* Pet. 6, 60–68; Reply 25–26. Patent Owner disputes Petitioner’s contentions. *See* Resp. 36–40; Sur-reply 27–28.

Above, we provided overviews of Stone and Hoyos. *See supra* §§ III.D.1–III.D.2. Below, we provide an overview of Varghese. Then, we consider the obviousness issues. For the reasons explained below, we agree with Petitioner that claims 7, 15, and 22 are unpatentable under § 103(a)

because the claims would have been obvious over Stone, Hoyos, and Varghese.

1. 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”:

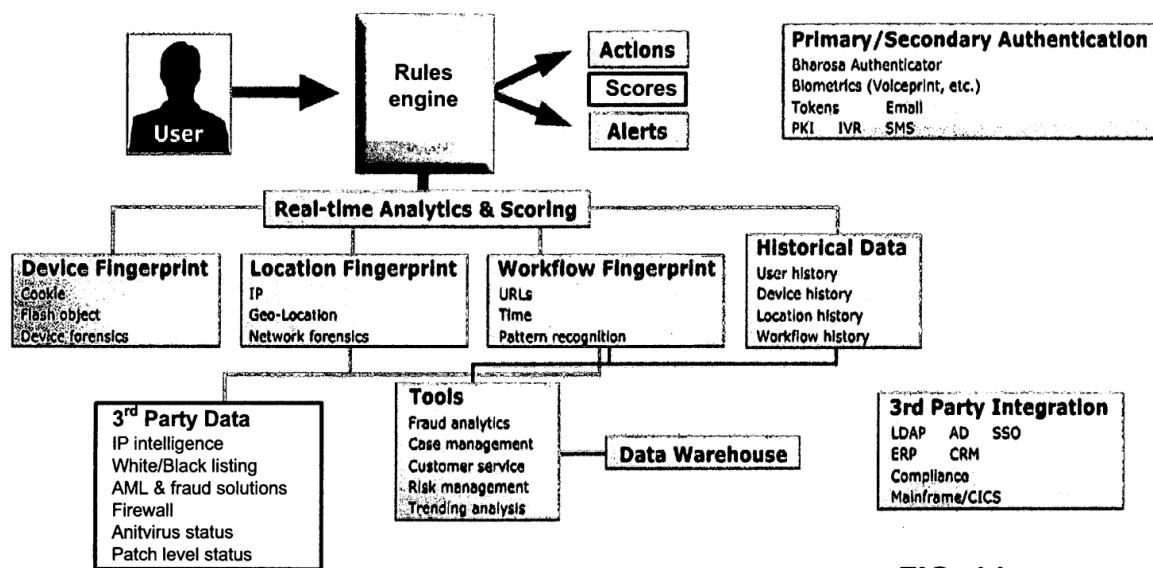


FIG. 14

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.”¹³ *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 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

¹³ The acronym “PKI” stands for “public key infrastructure.” The acronym “IVR” stands for “interactive voice response.” The acronym “SMS” stands for “short message service.”

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.”

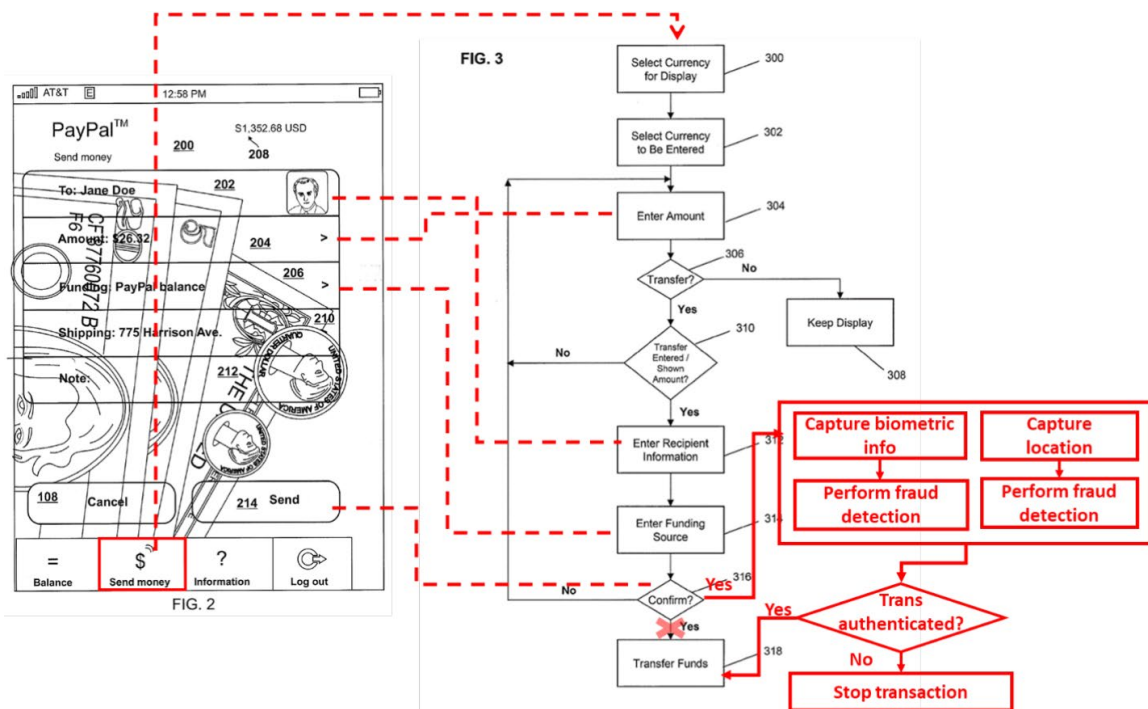
Id. ¶ 110.

2. 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. 62):



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. 62; *see* Ex. 1003 ¶ 178; Ex. 1008 ¶¶ 11–12, 16, 23–24, 29–35, Figs. 2–3.

- (ii) 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 “multifactor real-time authentication” including “location authentication for user transaction requests” with the Stone-Hoyos system to provide “improved security for financial transactions.” Pet. 60–61 (citing Ex. 1003 ¶¶ 175–183); *see id.* at 66–67.

According to Petitioner, combining Varghese’s “multifactor real-time authentication” including “location authentication for user transaction requests” with the Stone-Hoyos system would have achieved various advantages including:

- (1) “detecting and preventing access attempts from locations commonly associated with cyber threats”;
- (2) “providing cross-checking with a user location for a transaction request”; and
- (3) “providing additional security without significant additional inconvenience to the user.”

Pet. 61–62 (citing Ex. 1003 ¶ 177; Ex. 1016 ¶ 43).

Petitioner asserts that an ordinarily skilled artisan “would have been motivated to implement Varghese’s multifactor real-time authentication (including capturing authentication data and performing fraud detection thereupon) for user transaction request (also referred to as ‘post-authentication’) after a user confirms a user transaction request.” Pet. 62 (emphasis omitted); *see id.* at 63 (citing Ex. 1003 ¶ 181). More specifically, Petitioner explains that in the proposed combination Varghese’s multifactor real-time authentication would occur “at least after the user interaction with the icon (e.g., user clicking the ‘\$ Send money’ icon of FIG. 2) to initiate the transaction request, and after user interactions with icons to continue (e.g., blocks 300–314) and confirm (e.g., 316) the transaction request.” *Id.* at 62–63 (citing Ex. 1003 ¶ 179; Ex. 1010 ¶¶ 91, 97–99, 148; Ex. 1013 ¶ 28; Ex. 1015, Fig. 4; Ex. 1016 ¶¶ 36, 43, 73, Fig. 3; Ex. 1035, 4:60–62, 4:66–67) (emphasis omitted).

According to Petitioner, an ordinarily skilled artisan would have recognized that implementing Varghese’s multifactor real-time authentication after a user confirms a user transaction request would produce benefits similar to those produced by implementing Hoyos’s biometric authentication after a user confirms a user transaction request, e.g., performing “risk-based contextual authentication adaptive to a particular transaction request and its assessed risk.” Pet. 21, 62–63.

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 26 (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.*

(iii) Reasonable Expectation of Success

Petitioner asserts that an ordinarily skilled artisan “would have reasonably expected to succeed in configuring Stone-Hoyos-Varghese to leverage Varghese’s multifactor real-time authentication functionality since its implementation would have required only routine knowledge well within” the artisan’s skill. Pet. 63 (citing Ex. 1003 ¶ 181). Petitioner explains, among other things, that (1) “Stone already describes detection of user location, e.g., using GPS or other location-determining method,” and (2) “Varghese describes capturing location data (e.g., IP address) and determining location based thereon (e.g., using a ‘geolocation service’).” *Id.* at 63–64 (citing Ex. 1008 ¶ 26; Ex. 1010 ¶¶ 93, 140).

(b) Patent Owner’s Contentions

Patent Owner disputes that an ordinarily skilled artisan would have been motivated to combine Varghese’s teachings with the teachings of Stone and Hoyos. *See* Resp. 36–40; Sur-reply 27–28. 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.” Resp. 36–37 (citing Ex. 1010 ¶¶ 5–6; Ex. 2032 ¶ 85); Sur-reply 27–28. Patent Owner asserts that “for the reasons explained in the analysis of Stone-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. 37 (citing Ex. 2032 ¶ 85); *see* Sur-reply 28.

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. 37–38 (emphasis omitted) (quoting Ex. 1010 ¶ 22) (citing Ex. 1010 ¶¶ 17, 21–22; Ex. 2032 ¶ 86); *see* Sur-reply 28. According to Patent Owner, “Varghese’s goal of a software-only solutions [sic] mandates a client-server structure.” Resp. 37 (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. 38; *see* Sur-reply 28. 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. 38 (citing Ex. 2032 ¶ 87).

Further, Patent Owner asserts that “Varghese teaches away from applying a location check as a final step of fraud detection analysis” according to the claimed inventions. Resp. 39. 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.”

Id. at 39–40 (alteration by Patent Owner) (emphasis omitted) (quoting Ex. 1010 ¶ 89) (citing Ex. 1010 ¶¶ 74, 65, 90; Ex. 2032 ¶ 90).

Patent Owner contends that Varghese does not disclose collecting location data during post-authentication. *See* Tr. 104:3–5, 104:23–105:3. According to Patent Owner, location data used for post-authentication was already collected for pre-authentication, not newly collected for post-authentication. *See id.*

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. 40 (bracketed text added by Patent Owner) (emphasis omitted) (citing Ex. 2032 ¶ 90).

(c) Analysis

(i) 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 “multifactor real-time authentication” including “location authentication for user transaction requests” with the Stone-Hoyos system in the way Petitioner proposes. *See* Pet. 60–63, 66–67. Dr. Jones’s testimony supports Petitioner’s positions. *See* Ex. 1003 ¶¶ 175–180, 190; Ex. 1056 ¶¶ 44–45.

In particular, as Petitioner contends, combining Varghese’s “multifactor real-time authentication” including “location authentication for user transaction requests” with the Stone-Hoyos system would have “improved security for financial transactions,” for example by:

- (1) “detecting and preventing access attempts from locations commonly associated with cyber threats”;
- (2) “providing cross-checking with a user location for a transaction request”; and
- (3) “providing additional security without significant additional inconvenience to the user.”

See Ex. 1003 ¶¶ 175, 177–180, 190; Pet. 61–62, 66–67.

Also, as Petitioner asserts, an ordinarily skilled artisan would have recognized that implementing Varghese’s multifactor real-time authentication after a user confirms a user transaction request would produce:

- (1) benefits similar to those produced by implementing Hoyos’s biometric authentication after a user confirms a user transaction request, e.g., from performing “risk-based contextual authentication adaptive to a particular transaction request and its assessed risk”; and

- (2) additional benefits, e.g., from 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.”

See Ex. 1003 ¶¶ 64–65, 178–180; Pet. 21, 62–63; *supra* § III.D.4(c)(i).

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. 40 (bracketed text added by Patent Owner) (emphasis omitted).

Additionally, we disagree with Patent Owner that when post-authentication according to Varghese uses location data, the location data was already collected for pre-authentication, not newly collected for post-authentication. *See* 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 ¶ 186. 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 ¶¶ 46, 186. 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. 51 (quoting Ex. 1010 ¶ 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 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 ¶ 186.

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 ¶ 46. 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 ¶ 186. Figure 14 illustrates a “Location Fingerprint” including “IP, Geo-Location, Network forensics.” Ex. 1010, Fig. 14; *see* Ex. 1003 ¶ 186.

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 ¶ 187; *see* Ex. 1010 ¶¶ 38–39, 74–75, 77, 79, 88, 91, 97, 109, 140, 142, 148, claim 14, Fig. 14.

Patent Owner’s assertion that “Varghese teaches away from applying a location check as a final step of fraud detection analysis” according to the claimed inventions lacks merit. *See* Resp. 39. 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 1314, 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. 36–40; Sur-reply 27–28.

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 26; Ex. 1056 ¶ 44. 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 ¶ 44. Additionally, Varghese’s Figure 14 depicts “Primary/Secondary Authentication” including “Biometrics (Voiceprint, etc.).” Ex. 1010, Fig. 14; *see* Ex. 1003 ¶ 186. 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 ¶¶ 44–45.

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. 61–63; Resp. 38. Petitioner does not propose modifying Varghese’s analytics-and-scoring system based on Hoyos’s teachings. *See* Pet. 61–63. 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 for the Stone-Hoyos challenge. *See* Resp. 37; *supra* § III.D.4(c)(i).

(ii) 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 “would have reasonably expected to succeed in configuring Stone-Hoyos-Varghese to leverage Varghese’s multifactor real-time authentication functionality since its implementation would have required only routine knowledge well within” the artisan’s skill. *See* Pet. 63–64; Ex. 1003 ¶¶ 181–182.

3. WHETHER VARGHESE TEACHES THE
LIMITATIONS IN DEPENDENT CLAIMS 7, 15, AND 22

(a) Claims 7 and 15

Claim 7 depends directly from claim 1 and specifies that “the captured contextual information further comprises at least one of physical location information and information spoken by the user.” Ex. 1001, 14:36–38. Claim 15 depends directly from claim 9 and includes a limitation similar to claim 7. *Id.* at 15:18–20.

Petitioner contends that Varghese teaches the limitations in claims 7 and 15 because Varghese discloses capturing:

- (1) “physical location information” for “location authentication” in real time; and
- (2) “information spoken by the user” for “voice authentication” in real time.

Pet. 64–66.

According to Petitioner, the captured “physical location information” is “used to determine a user physical location for fraud analysis.” Pet. 64–65; *see id.* at 66. As support, Petitioner cites Varghese’s Figure 14 showing “Real-time Analytics & Scoring” for authentication based on, among other things, “Location Fingerprint” including “IP, Geo-Location, Network forensics.” *Id.* at 65 (quoting Ex. 1010, Fig. 14) (citing Ex. 1003 ¶ 186; Ex. 1010 ¶¶ 74, 97–99, 140).

For “information spoken by the user,” Petitioner cites Varghese’s Figure 14 showing “Primary/Secondary Authentication” including “Biometrics (Voiceprint, etc.).” Pet. 65.

Patent Owner makes no arguments specific to claims 7 and 15. *See, e.g.,* Resp. 36–40; Sur-reply 27–28.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that Varghese teaches the limitations in claims 7 and 15. *See* Pet. 64–66; Ex. 1003 ¶¶ 184–189, 191–192.

(b) Claim 22

Claim 22 depends directly from claim 1 and specifies that “the captured contextual information further comprises captured physical location information associated with the user” and “performing the fraud detection analysis further comprises determining a physical location of the user based

at least in part on the captured physical location information.” Ex. 1001, 16:25–30.

Petitioner contends that Varghese teaches claim 22’s limitations because “Varghese’s location authentication describes determining a physical location of the user based at least in part on the captured physical location information.” Pet. 67. As support, Petitioner quotes Varghese’s disclosure about obtaining geolocation by IP address, i.e., “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.* (quoting Ex. 1010 ¶ 140).

Patent Owner makes no arguments specific to claim 22. *See, e.g.*, Resp. 36–40; Sur-reply 27–28.

For the reasons stated by Petitioner and supported by Dr. Jones’s testimony, we agree with Petitioner that Varghese teaches claim 22’s limitations. *See* Pet. 67–68; Ex. 1003 ¶¶ 193–195.

4. CONCLUSION ABOUT OBVIOUSNESS/NONOBVIOUSNESS

For the reasons discussed above, the combined disclosures in Stone, Hoyos, and Varghese teach the limitations in claims 7, 15, and 22. *See supra* §§ III.E.3(a)–(b). Moreover, an ordinarily skilled artisan would have been motivated to combine Varghese’s teachings with the teachings of Stone and Hoyos in the way Petitioner proposes and would have reasonably expected to succeed. *See supra* § III.E.2(c). Hence, Petitioner has shown by a preponderance of the evidence that claims 7, 15, and 22 are unpatentable under § 103(a) because the claims would have been obvious over Stone, Hoyos, and Varghese.

*F. Alleged Obviousness over Stone and the Guidance:
Claims 1, 2, 4–7, 9, 10, 12–15, 17, and 20–23*

Petitioner contends that claims 1, 2, 4–7, 9, 10, 12–15, 17, and 20–23 are unpatentable under § 103(a) because the claims would have been obvious over Stone and the Guidance. *See* Pet. 6, 68–85; Reply 26–29. Patent Owner disputes Petitioner’s contentions. *See* Resp. 40–45; Sur-reply 28–31.

For the reasons discussed above, the challenges based on Stone, Hoyos, and Varghese resolve the patentability questions for claims 1, 2, 4–7, 9, 10, 12–15, 17, and 20–23 favorable to Petitioner. *See supra* §§ III.D–III.E. Hence, we need not reach the challenge based on Stone and the Guidance. *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:

- (1) claims 1, 2, 4–6, 9, 10, 12–14, 17, 20, 21, and 23 are unpatentable under § 103(a) because the claims would have been obvious over Stone and Hoyos; and
- (2) claims 7, 15, and 22 are unpatentable under § 103(a) because the claims would have been obvious over Stone, Hoyos, and Varghese.

In summary:¹⁴

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1, 2, 4–6, 9, 10, 12–14, 17, 20, 21, 23	103(a)	Stone, Hoyos	1, 2, 4–6, 9, 10, 12–14, 17, 20, 21, 23	
7, 15, 22	103(a)	Stone, Hoyos, Varghese	7, 15, 22	
1, 2, 4–7, 9, 10, 12–15, 17, 20–23	103(a)	Stone, Guidance ¹⁵		
Overall Outcome			1, 2, 4–7, 9, 10, 12–15, 17, 20–23	

¹⁴ 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).

¹⁵ In view of our determination that claims 1, 2, 4–7, 9, 10, 12–15, 17, and 20–23 are unpatentable based on other challenges, we do not reach this challenge to those claims. *See supra* § III.F.

V. ORDER

Accordingly, it is

ORDERED that claims 1, 2, 4–7, 9, 10, 12–15, 17, and 20–23 in the '010 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.

IPR2024-00329
Patent 9,972,010 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