

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner.

IPR2024-00331
Patent 11,526,886 B1

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

AMUNDSON, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Apple Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1–12, 14–18, and 20–23 in U.S. Patent No. 11,526,886 B1 (Exhibit 1001, “the ’886 patent”) 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.

Under 37 C.F.R. § 42.4(a), we have authority to determine whether to institute an *inter partes* review. We may institute an *inter partes* review only if “the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a) (2018). The “reasonable likelihood” standard is “a higher standard than mere notice pleading” but “lower than the ‘preponderance’ standard to prevail in a final written decision.” *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-01039, Paper 29 at 13 (PTAB Dec. 20, 2019) (precedential).

Based on the current record and for the reasons explained below, Petitioner has shown that there is a reasonable likelihood that it would prevail with respect to at least one of the challenged claims. Thus, we institute an *inter partes* review of claims 1–12, 14–18, and 20–23 in the ’886 patent on all challenges included in the Petition.

II. BACKGROUND

A. 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.

B. 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) (the “Texas case”). Pet. 1; Paper 3, 2.

C. The ’886 Patent (Exhibit 1001)

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

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

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

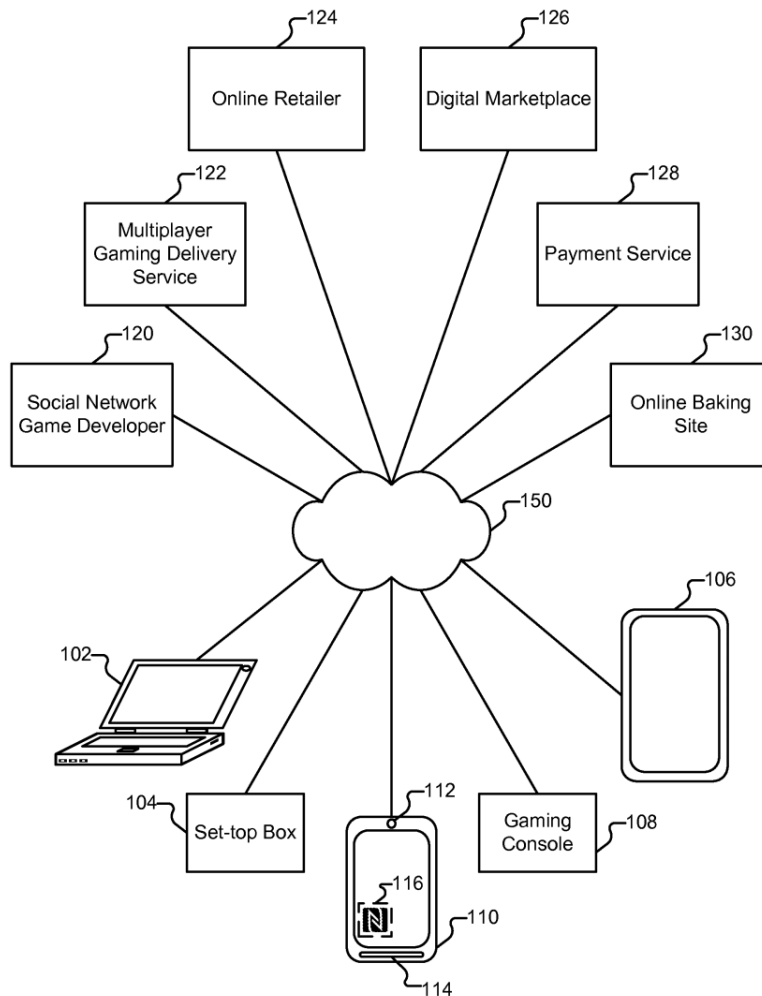


FIG. 1

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

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

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

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

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

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

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

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

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

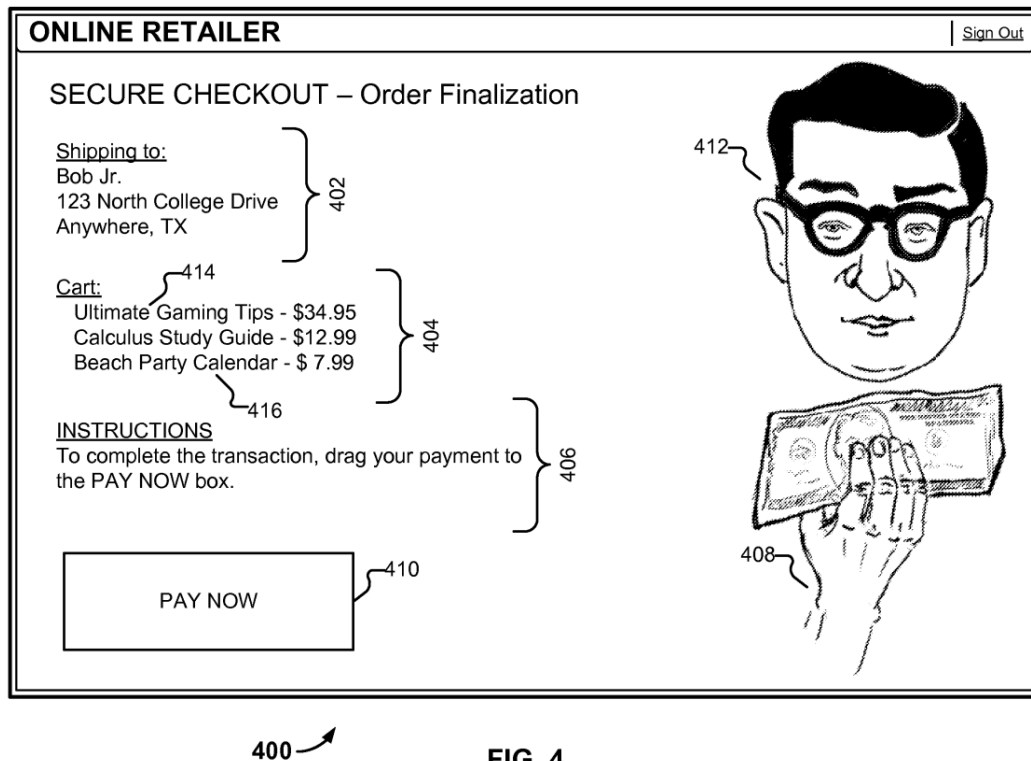


Figure 4 "illustrates an embodiment of an interface" as "rendered in a browser application of a personal computer." Ex. 1001, 1:52, 6:29–31, Fig. 4. In particular, "Bob has specifically told Bob Jr. that it is ok for Bob Jr. to purchase schoolbooks using Bob's account with online retailer 124" in Figure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

The Figure 4 interface includes the following display elements:

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

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

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

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

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

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

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

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

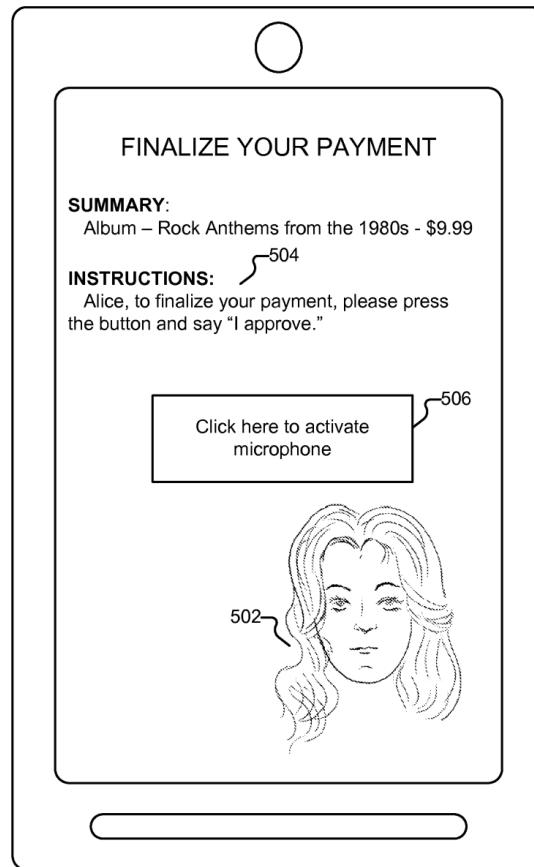


FIG. 6

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

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

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

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

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

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

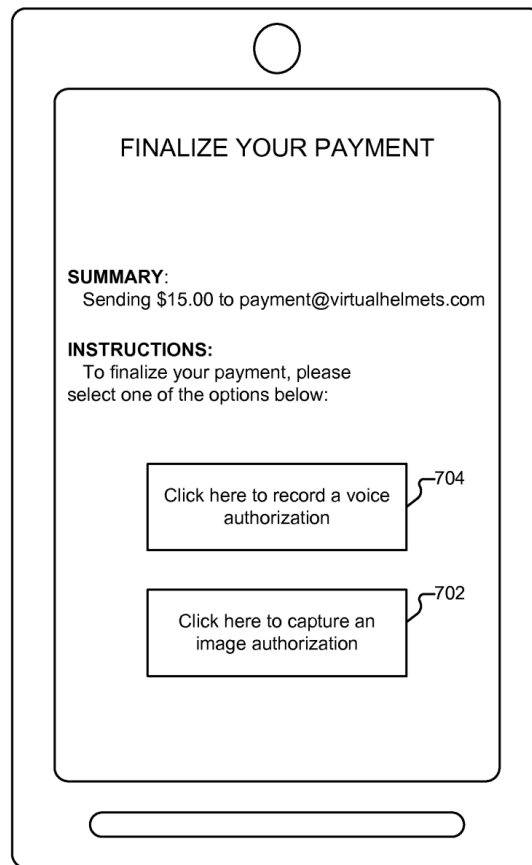


FIG. 7

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

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

Techniques for “confirming that the object being photographed is alive (e.g., by taking multiple photographs in rapid succession) can be employed to help make sure that the fraudster isn’t using camera 112 to photograph a printed picture of the legitimate user.” Ex. 1001, 8:66–9:4.

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

D. The Challenged Claims

Petitioner challenges the following claims in the ’886 patent:

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

Pet. 5–6, 14–91.

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

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

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

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

Ex. 1001, 14:2–27.

E. The Asserted References

For its challenges, Petitioner relies on the following references:

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

Pet. 5–6, 14–91.

Petitioner asserts that:

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

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

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

At this stage of the proceeding, and as explained below, Patent Owner disputes that Stone qualifies as prior art. *See infra* § IV.D.4(b). In particular, Patent Owner contends that “Stone is not analogous art.” Prelim. Resp. 17, 35, 54; *see id.* at 2; Prelim. Sur-reply 3. At this stage of the proceeding, Patent Owner does not dispute that Varghese, Hoyos, Campbell, and the Guidance qualify as prior art. *See, e.g.*, Prelim. Resp. 29–54; Prelim. Sur-reply 1–3.

F. The Asserted Challenges to Patentability

Petitioner asserts the following challenges to patentability:

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

Pet. 5–6, 14–91.

G. Testimonial Evidence

To support its challenges, Petitioner relies on the declaration of Creed F. Jones III, Ph.D. (Exhibit 1003). 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

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

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.

At this stage of the proceeding, Patent Owner does not introduce testimonial evidence concerning the patentability issues.

III. DISCRETIONARY DENIAL IN VIEW OF PARALLEL LITIGATION

Under § 314(a), the Director possesses “broad discretion” in deciding whether to institute an *inter partes* review. *See* 35 U.S.C. § 314(a); *Saint Regis Mohawk Tribe v. Mylan Pharms. Inc.*, 896 F.3d 1322, 1327 (Fed. Cir. 2018). The Director is “permitted, but never compelled,” to institute an *inter partes* review. *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1367 (Fed. Cir. 2016). The Board decides whether to institute an *inter partes* review on the Director’s behalf. 37 C.F.R. § 42.4(a) (2024).

Based on *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential) (“*Fintiv*”), Patent Owner argues that we should exercise our discretion under § 314(a) to deny institution in view of the Texas case. *See* Prelim. Resp. 1–2, 17–29; *supra* § II.B. Petitioner argues that we should decline to exercise our discretion under § 314(a) to deny institution. *See* Pet. 91–94.

A. Nonexclusive Factors to Consider

When deciding whether to exercise discretion under § 314(a) to deny institution, the Board has considered the status of litigation involving the parties in light of the AIA’s objective “to provide an effective and efficient alternative to district court litigation.” *NHK Spring Co. v. Intri-Plex Techs., Inc.*, IPR2018-00752, Paper 8 at 12, 19–20 (PTAB Sept. 12, 2018)

(precedential) (“*NHK*”). The Board has set forth the following nonexclusive factors to consider when determining whether to exercise discretion under § 314(a) to deny institution due to the advanced state of parallel litigation:

- (1) whether the court granted a stay or evidence exists that one may be granted if the Board institutes a trial;
- (2) the proximity of the court’s trial date to the Board’s projected statutory deadline for a final written decision;
- (3) the investment in the parallel litigation by the court and the parties;
- (4) the overlap in the issues raised by the petition and the issues in the parallel litigation;
- (5) whether the petitioner and the defendant in the parallel litigation are the same party; and
- (6) other circumstances that impact the Board’s exercise of discretion, including the merits.

Fintiv, IPR2020-00019, Paper 11 at 5–6.

These factors “relate to whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding.” *Fintiv*, IPR2020-00019, Paper 11 at 6. Further, *Fintiv* instructs that the Board should take “a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review.” *Id.*; see PTAB Consolidated Trial Practice Guide at 55–56, 58 (Nov. 2019).⁴

⁴ Available at <https://www.uspto.gov/TrialPracticeGuideConsolidated>.

We also follow the Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (June 21, 2022) (“Interim Procedure”).⁵

B. Analysis

The Interim Procedure instructs that “the PTAB will not discretionarily deny institution in view of parallel district court litigation where a petitioner presents a stipulation not to pursue in a parallel proceeding the same grounds or any grounds that could have reasonably been raised before the PTAB.” Interim Procedure at 3 (citing *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020) (precedential as to § II.A)); *see id.* at 7, 9. The Interim Procedure also explains that such a stipulation (a *Sotera* stipulation) “mitigates concerns of potentially conflicting decisions and duplicative efforts between the district court and the PTAB.” *Id.* at 7.

Petitioner presents a *Sotera* stipulation. Ex. 1048, 1. Specifically, Petitioner stipulates as follows:

Petitioner Apple Inc. (“Apple”) hereby stipulates that if the Patent Trial and Appeal Board (PTAB) institutes the IPR based on the grounds identified below [ground 1—Stone, Hoyos, and Varghese; ground 2—Stone and the Guidance; ground 3—Stone, Hoyos, Varghese, and Campbell; and ground 4—Stone, the Guidance, and Campbell], then it (i) will not pursue the grounds identified below in the Parallel District Court Litigation [the Texas case] and (ii) will not pursue any other ground that reasonably could have been raised during the

⁵ Available at https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621.pdf.

IPR (should it be instituted) in the Parallel District Court Litigation.

Id. After that stipulation, Petitioner provides a table that (1) identifies four grounds of unpatentability and (2) substantially matches the table set forth above in section II.F. *Id.*

Patent Owner does not dispute that Petitioner presents a *Sotera* stipulation. *See, e.g.*, Prelim. Resp. 25–26; Prelim. Sur-reply 1–3.

Because Petitioner presents a *Sotera* stipulation, we decline to exercise our discretion under § 314(a) to deny institution in view of the Texas case. *See* Interim Procedure at 3, 7, 9; Ex. 1048, 1.

IV. 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.⁶ *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

⁶ The parties do not address objective indicia of nonobviousness. *See, e.g.*, Pet. 14–91; Prelim. Resp. 29–54.

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.

B. Level of Ordinary Skill in the Art

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

Petitioner asserts that a person of ordinary skill in the art at the time of the alleged invention would have had “a bachelor’s degree in electrical engineering, computer engineering, computer science, or a related field, and at least two years of experience in the research, design, development, and/or testing of biometric authentication techniques, and related firmware and software, or the equivalent, with additional education substituting for experience and vice versa.” Pet. 4. Petitioner also asserts that “a person with less formal education but more experience, or more formal education but less experience, could have also met the relevant standard” for an

ordinarily skilled artisan. *Id.* Dr. Jones’s testimony supports Petitioner’s assertions. *See* Ex. 1003 ¶¶ 19–20.

Patent Owner asserts that the Preliminary Response “does not depend on the skill level Petitioner has identified.” Prelim. Resp. 14. Patent Owner accepts Petitioner’s description of an ordinarily skilled artisan for purposes of the Preliminary Response. *Id.*

Based on the current record and for purposes of this decision, we adopt 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. Otherwise, Petitioner’s description of an ordinarily skilled artisan comports with the technology and claims of the ’886 patent as well as the asserted references. *See* Ex. 1003 ¶ 20.

C. Claim Construction

We construe claim terms “using the same claim construction standard” that district courts use to construe claim terms in civil actions under 35 U.S.C. § 282(b). *See* 37 C.F.R. § 42.100(b). Under that standard, claim terms “are given their ordinary and customary meaning, which is the meaning the term would have to a person of ordinary skill in the art at the time of the invention.” *Power Integrations, Inc. v. Fairchild Semiconductor Int’l, Inc.*, 904 F.3d 965, 971 (Fed. Cir. 2018) (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc)). The meaning of claim terms may be determined by “look[ing] principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic*

Sofamor Danek, Inc., 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).

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

Patent Owner “accepts Petitioner’s position that none of the claim terms of the ’886 Patent requires construction.” Prelim. Resp. 14 (citing Pet. 4–5).

“[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). Based on the current record, we determine that no claim term requires an explicit construction to decide whether Petitioner satisfies the “reasonable likelihood” standard for instituting trial.

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

Petitioner contends that claims 1–12, 14–18, and 20–23 are unpatentable under § 103(a) as obvious over Stone, Hoyos, and Varghese. See Pet. 5, 14–67; Prelim. Reply 3–5. Patent Owner disputes Petitioner’s contentions. See Prelim. Resp. 29–45; Prelim. Sur-reply 1–3.

Below, we provide overviews of Stone, Hoyos, and Varghese. Then, we consider the obviousness issues. For the reasons explained below, Petitioner establishes sufficiently for purposes of institution that the combined disclosures in Stone, Hoyos, and Varghese teach the subject matter in claims 1–12, 14–18, and 20–23.

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:

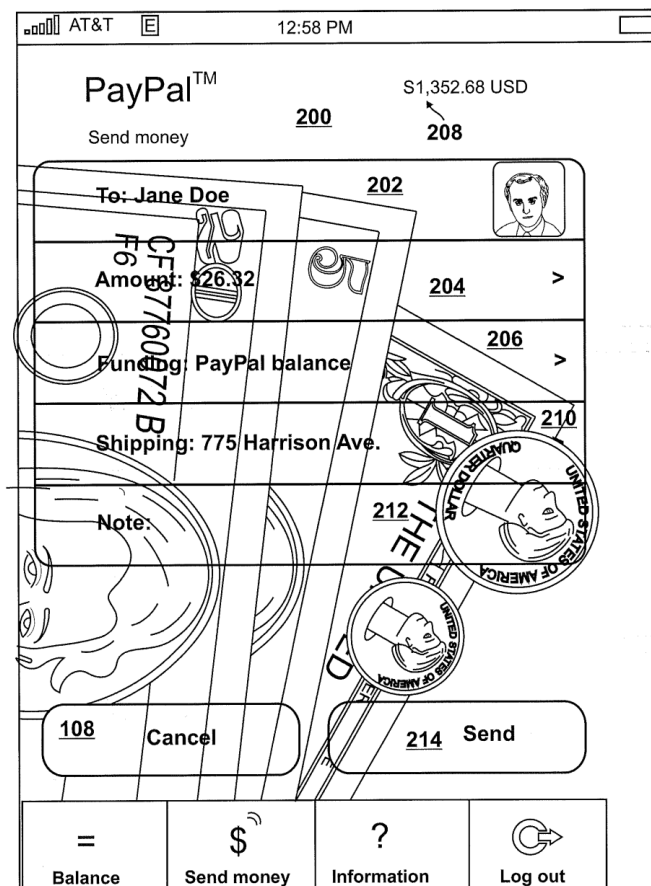


Figure 2 illustrates display 200 on an electronic device including the following display elements:

- (1) “name box 202 indicating the recipient of funds”;
- (2) a picture of the recipient in name box 202;
- (3) “funds box 204 indicating the amount of funds to be transferred”;
- (4) “funding source box 206, indicating the source or account where the user’s funds will be transferred from”;
- (5) “balance area 208, indicating the current balance of the funding account”;
- (6) “address box 210, indicating the address of the recipient”;
- (7) “note box 212 for the user to type in any notes to the recipient”;
- (8) “send button 214 to transfer the funds [as] noted in [funds] box 204”;
- (9) “cancel button 108”;
- (10) additional buttons labeled “= Balance,” “\$ Send money,” “? Information,” and “Log out” at the bottom of the display; and
- (11) the “actual currency representing the amount entered by the user” in the background of the display.

Ex. 1008 ¶¶ 11, 16, 23–24, Fig. 2.

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

After “the user decides to send the funds,” the display may indicate this with “some movement of the actual currency.” Ex. 1008 ¶ 25, Fig. 2. For example, the actual currency may “simply disappear,” “slowly fade

away,” or “move off the display,” such as “a lateral movement to the right.”
Id. ¶¶ 25, 37, Fig. 2.

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

FIG. 3

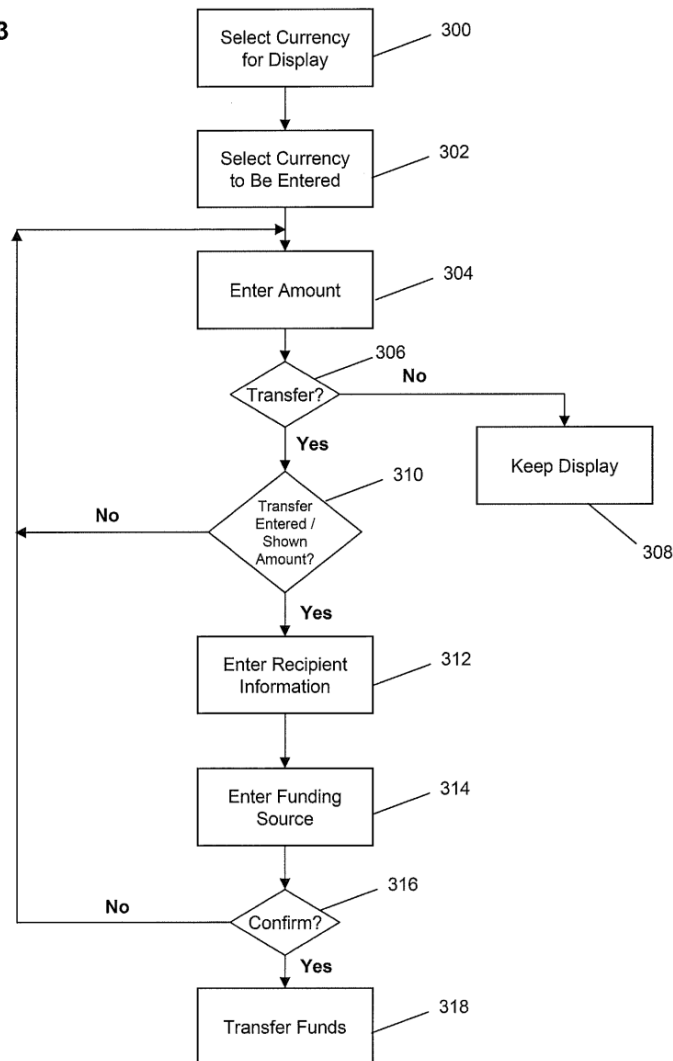


Figure 3 illustrates steps 300 through 318 for transferring funds to a recipient. *See* Ex. 1008 ¶¶ 29–35, Fig. 3.

In step 300, “the user selects the desired currency for display, such as U.S. dollar, Mexican peso, British pound, European Euro, Japanese yen, South Korean won, etc.” Ex. 1008 ¶ 29, Fig. 3. In step 302, the user selects

the type of currency that “will be entered.” *Id.* ¶ 30, Fig. 3. For example, “if the user wishes to see how \$126.34 U.S. dollars in South Korean won looks like, the user would select South Korean won in step 300 and U.S. dollars in step 302.” *Id.* ¶ 30.

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

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

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

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

If the user decides to proceed with the transaction, “the user confirms the transaction” in step 316. Ex. 1008 ¶ 35, Fig. 3. After “the user confirms the transaction,” the “shown funds are transferred to the desired recipient” in step 318. *Id.* ¶ 35, Fig. 3.

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

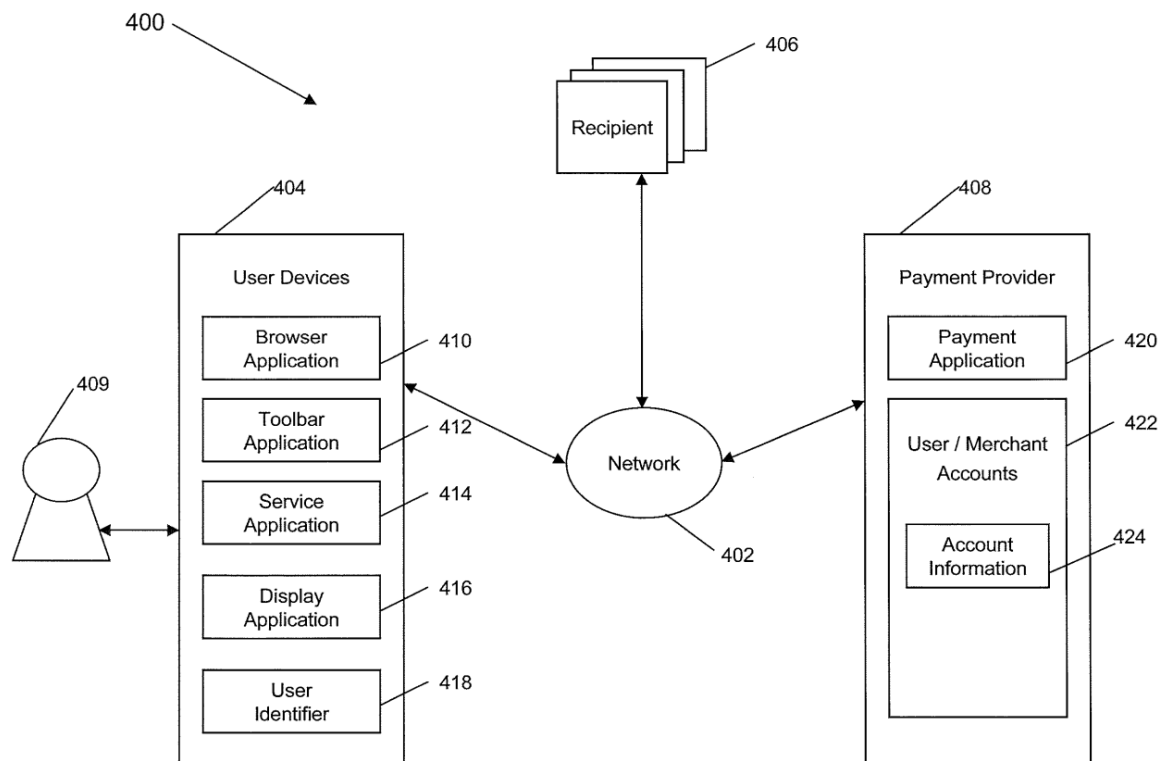


FIG. 4

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

User device 404 may include “any appropriate combination of hardware and/or software configured for wired and/or wireless communication over network 402.” Ex. 1008 ¶ 42, Fig. 4. For example, a bus or other communication mechanism in user device 404 may interconnect “subsystems and components, such as a processing component,” e.g., “processor, micro-controller, digital signal processor (DSP), etc.” *Id.* ¶ 49.

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

User device 404 may include “one or more user identifiers 418,” such as “operating system registry entries, cookies associated with browser application 410, identifiers associated with hardware of user device 404, or various other appropriate identifiers.” Ex. 1008 ¶ 45, Fig. 4. User identifiers 418 may include “attributes related to the user, such as personal information (e.g., a user name, password, photograph image, biometric id, address, phone number, etc.) and banking information (e.g., banking institution, credit card issuer, user account numbers, security information, etc.).” *Id.* ¶ 45.

Recipient devices 406 may have “the same basic features as user device 404” and “the same or similar graphics that show when funds are

transferred to the recipient's account by displaying actual currency.”

Ex. 1008 ¶¶ 8, 46; *see id.* ¶ 39.

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

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 P_p and P_m .”

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

Preferably, the authentication decision, D , is calculated according to the formula $D = P_p * (K + P_m)$ 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, P_p , 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, P_p , 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, P_m , may be calculated “in any way which is desired.” Ex. 1013 ¶ 22. The methods for calculating the probability of a match, P_m , include “iris recognition, fingerprint image recognition, finger vein image recognition, or palm vein image recognition, face recognition, [and] token match.” *Id.* ¶ 22, claim 10; *see id.* ¶ 12.

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

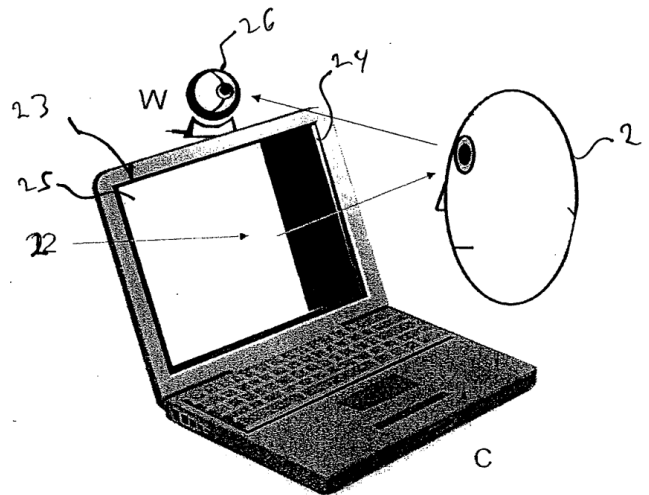


Fig. 2

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

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

By combining the two probabilities P_p and P_m to make a decision in a transaction, “the reject rate of true authentications can be designed to be greatly reduced.” Ex. 1013 ¶ 26. With the threshold for D set appropriately, “the

transaction will be authorized even though the biometric match is not high.”
Id. ¶ 28; *see id.* ¶ 39.

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

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

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

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

3. OVERVIEW OF VARGHESE (EXHIBIT 1010)

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

Varghese identifies deficiencies in conventional security measures for electronic financial transactions. *See* Ex. 1010 ¶¶ 7–13. For instance, "certain geographic locations are known to contain an inordinate number of identity thieves." *Id.* ¶ 12. "IP addresses are one readily available source of location information." *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 endeavors to address those deficiencies by providing systems and methods with "improved authentication services." Ex. 1010 ¶ 24; *see id.* ¶¶ 25–30. The 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.

Fraud-detection inputs include 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 output “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 discloses “real-time risk scoring” for “each online login and transaction,” including during the post-authentication stage, e.g., to “re-authenticate the user or request” for “transactions that may be high risk.” *See, e.g.,* Ex. 1010 ¶¶ 25, 38–39, 74–75, 77, 79, 88, 91, 97, 109, 142, 148,

Fig. 14. The “real-time risk scoring” depends on, among other things, location data. *See id.* ¶¶ 77, 88, 140, 142, 181, claim 14.

Varghese’s Figure 14 (reproduced below) depicts a preferred functional configuration:

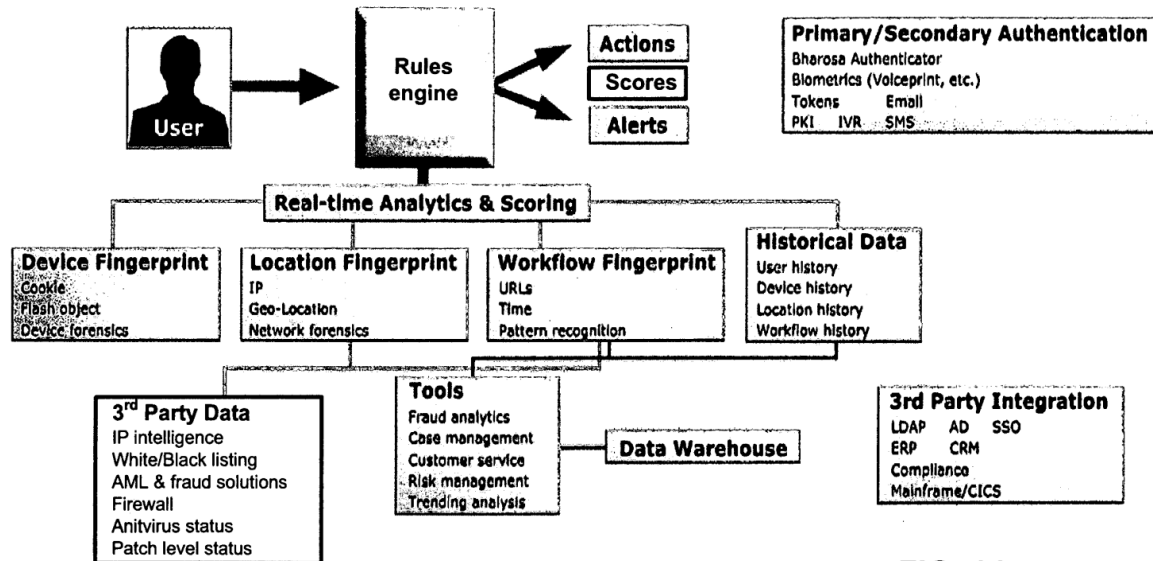


FIG. 14

Figure 14 illustrates “Real-time Analytics & Scoring” for authenticating a user transaction request where the request attributes “are condensed into fingerprints” that “are then processed to generate actions, alerts, and scores.” Ex. 1010 ¶¶ 91, 97, Fig. 14. The actions resulting from the real-time analytics and scoring include primary authentication and secondary authentication, i.e., shown in Figure 14 as “Primary/Secondary Authentication” including “Biometrics (Voiceprint, etc.), Tokens, Email, PKI, IVR, SMS.” *Id.* ¶ 91, Fig. 14; *see id.* ¶¶ 39, 78–79.

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.

Figure 14 shows the following fingerprints:

- (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 ¶ 91, Fig. 14.

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

4. WHETHER PETITIONER ESTABLISHES A REASONABLE LIKELIHOOD THAT 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). 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.

At the institution stage of an *inter partes* review, the statutory “reasonable likelihood” standard for institution applies to the issue whether a reference is analogous art. *Cf. Hulu*, IPR2018-01039, Paper 29 at 12 (precedential) (citing 35 U.S.C. § 314(a)).

(b) Patent Owner’s Contentions

Patent Owner contends that “Stone is not analogous art.” Prelim. Resp. 17, 35, 54; *see id.* at 2; Prelim. Sur-reply 3. Specifically, Patent Owner asserts that the field of endeavor for the ’886 patent is “prevent[ing] and detect[ing] fraud, particularly within electronic transactions.” Prelim. Resp. 35–36. Patent Owner asserts that Stone concerns a different field of endeavor because “Stone never discusses fraud.” *Id.* at 36; *see id.* at 2, 33. Further, Patent Owner asserts that “Stone is not pertinent” to the “problem of electronic payment fraud.” *Id.* at 36–37 (citing Ex. 1001, 14:2–27

(claim 1)); *see id.* at 17. According to Patent Owner, “Stone does not even recognize payment fraud as a problem needing to be solved.” *Id.* at 37; *see id.* at 33.

(c) Petitioner’s Contentions

Petitioner contends that Stone is in the same field of endeavor as the ’886 patent, i.e., “electronic financial transactions.” Pet. 13; *see id.* at 6–7; Prelim. Reply 3, 5. According to Petitioner, “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).

Petitioner also contends that Stone is “reasonably pertinent to a problem with which the inventor of the ’886 patent was involved,” such as “fraud detection in electronic financial transactions.” Pet. 13. As examples of “reasonably pertinent” references, Petitioner asserts that:

- (1) the Examiner cited “user interface art,” e.g., Gaw and Fujioka,⁷ during the prosecution of an ancestor of the ’886 patent, i.e., U.S. Patent No. 9,972,010 B1; and
- (2) the ’886 patent lists additional “user interface art” in the References Cited section.

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

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

(d) Analysis

Based on the current record, Petitioner establishes a reasonable likelihood that Stone is analogous art because Stone is “reasonably pertinent to the particular problem with which the inventor is involved.” *See* Ex. 1001, 4:39–41, 5:4–6, 5:27–29; Ex. 1003 ¶¶ 58, 162; Ex. 1008 ¶¶ 6, 8, 16, 22–25, 31, 33, 39, code (57), Figs. 1–2; *Bigio*, 381 F.3d at 1325.

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.” Ex. 1001, 4:39–41, 5:4–6, 5:27–29. Stone addresses that problem by disclosing an electronic device with a display screen that shows the “actual currency” for an electronic financial transaction. Ex. 1008 ¶¶ 6, 8, 10–11, 16, 22–25, 31, 33, 39, code (57), Figs. 1–2; *see* Ex. 1003 ¶ 162. 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.

Also, as Petitioner asserts, the Examiner cited “user interface art” during the ’886 patent’s prosecution and the prosecution of the patent’s ancestors. Ex. 1002, 97, 196, 199; Ex. 1006, 22; Ex. 1007, 87–91, 94, 146–58, 161, 290, 292, 342–50, 353, 454; Ex. 1030, 105, 107–08; *see* Ex. 1001, code (56); Prelim. Reply 4–5. Consistent with this, the patent’s Figure 4 “illustrates an embodiment of an interface,” the patent’s Figure 6 “illustrates an embodiment of an interface,” and the patent’s Figure 7 “illustrates an embodiment of an interface.” Ex. 1001, 1:52, 1:56–57, 6:29–32, 7:60–63, 8:56–58, Figs. 4, 6–7. Stone’s Figures 1 and 2 also

illustrate embodiments of an interface, in particular, embodiments that show the “actual currency” for an electronic financial transaction. Ex. 1008 ¶¶ 10–11, 22–25, code (57), Figs. 1–2.

For these reasons, Petitioner establishes a reasonable likelihood that Stone is at least “reasonably pertinent” analogous art.

5. INDEPENDENT CLAIM 1

(a) Whether an Ordinarily Skilled Artisan Would Have Been Motivated to Combine the Teachings of the References with a Reasonable Expectation of Success

(i) Petitioner’s Proposed Combination

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

Additionally, Petitioner contends that “it was well-known that financial transaction systems of Stone had a need for authentication for fraud detection (e.g., with higher levels of security for higher-risk transactions).” Pet. 16 (citing Ex. 1003 ¶ 66; Ex. 1010 ¶ 148; Ex. 1013 ¶¶ 9, 11; Ex. 1016 ¶ 73, Fig. 3; Ex. 1022, 1; Ex. 1037, 1). Petitioner asserts that an ordinarily skilled artisan would have been motivated to use Hoyos’s biometric

authentication in 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. *Id.* at 16–17 (quoting Ex. 1013 ¶ 15) (citing Ex. 1003 ¶¶ 64–73; Ex. 1013 ¶¶ 17–22); *see id.* at 44, 52–53 (quoting Ex. 1013 ¶ 15).

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

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

Pet. 17, 45 (quoting Ex. 1013 ¶¶ 24, 26–27, 29).

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

confirmation had various benefits over the alternative design choice of using only previously captured input data before user transaction request confirmation.” *Id.* at 18–19. According to Petitioner, those “various benefits” include (1) performing “risk-based contextual authentication (e.g., specific authentication level requiring specific types of contextual data to capture) based on the specific transaction and assessed risk thereof for improved fraud detection,” (2) providing “improved fraud detection and security” by “capturing real-time, more accurate data,” and (3) “avoiding imposters from communicating based on stolen biometric data.” *Id.* at 19–20 (citing Ex. 1003 ¶ 70); *see id.* at 46.

Regarding risk-based contextual authentication, Petitioner explains that “a large transaction amount would typically be considered higher risk than a small transaction amount.” Pet. 19. Petitioner also explains that:

an apparently unrelated overseas recipient or a person, account or banking institution on a watch list would presumably be considered a higher risk transaction than a transfer to an account owned by another customer of the same financial institution or to a person/account to whom the sender has previously transferred funds.

Id. at 19–20.

Further, Petitioner asserts that an ordinarily skilled artisan would have been motivated to use Varghese’s “real-time multifactor authentication (including location authentication combined with biometrics (e.g., voice, fingerprints, retinal scans, etc.))” in the Stone-Hoyos system to provide “improved security for financial transactions.” Pet. 21 (citing Ex. 1003 ¶¶ 74–84; Ex. 1010 ¶ 79); *see id.* at 38–39, 49. Petitioner also asserts that an ordinarily skilled artisan would have understood that:

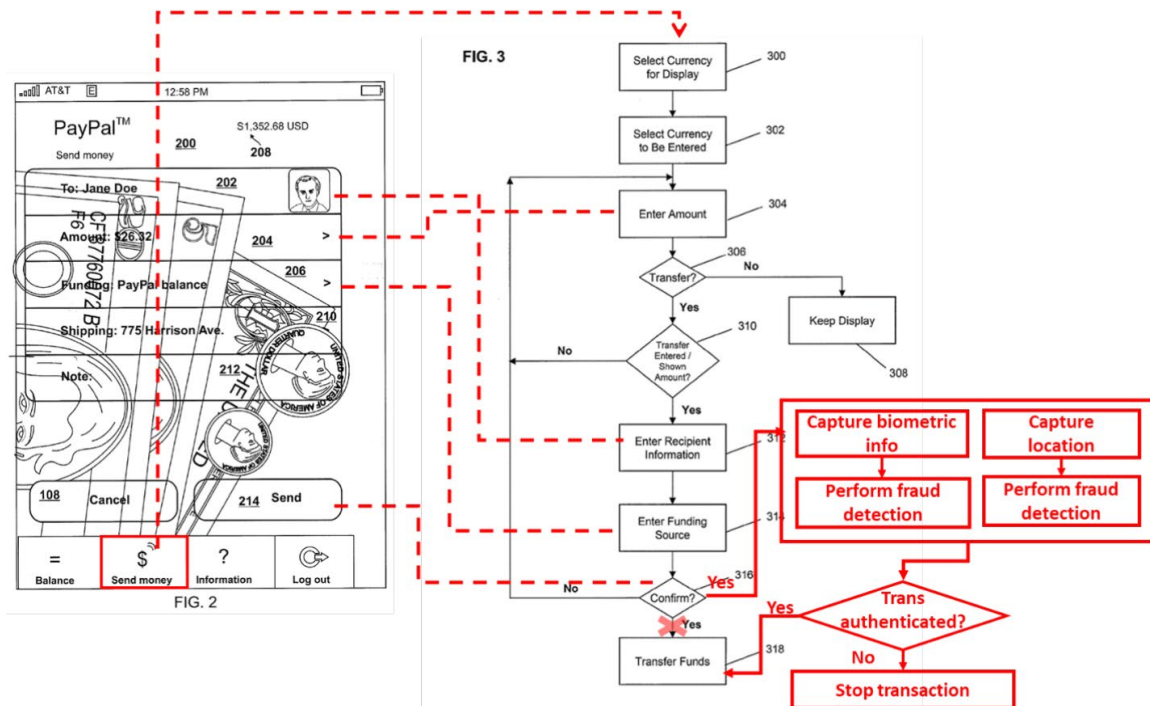
- (1) real-time authentication “as described in Varghese includes both real-time capture and real-time analysis of input authentication data for transaction authentication, which provides more accurate fraud analysis by using more accurate, real-time input data”; and
- (2) “multifactor authentication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

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

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

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

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



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

- (1) a dashed line from the "\$ Send money" button in Figure 2 to step 300 for "Select Currency for Display" in Figure 3;
- (2) a dashed line from name box 202 in Figure 2 to step 312 for "Enter Recipient Information" in Figure 3;
- (3) a dashed line from funds box 204 in Figure 2 to step 304 for "Enter Amount" in Figure 3;
- (4) a dashed line from funding source box 206 in Figure 2 to step 314 for "Enter Funding Source" in Figure 3;
- (5) a dashed line from the "Send" button 214 in Figure 2 to step 316 for "Confirm?" in Figure 3; and
- (6) additional steps after a "Yes" determination in step 316 for "Confirm?" as follows: (i) "Capture biometric info" followed by "Perform fraud detection"; (ii) "Capture

location” followed by “Perform fraud detection”;
(iii) “Trans authenticated?”; and (iv) “Stop transaction.”

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

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

Dr. Jones’s testimony supports Petitioner’s positions. *See* Ex. 1003 ¶¶ 59–84, 113–118, 126–130, 135, 141.

(ii) Patent Owner’s Contentions

Patent Owner contends that Petitioner does not provide a “persuasive justification” why an ordinarily skilled artisan would have combined the teachings of Stone, Hoyos, and Varghese to yield the claimed invention. Prelim. Resp. 29–30; *see id.* at 2, 30–34, 44–46. Patent Owner also contends that Petitioner does not provide an explanation why an ordinarily skilled artisan “would have believed the combination would have succeeded.” *Id.* at 29–30.

Additionally, Patent Owner asserts that an ordinarily skilled artisan would not have combined Hoyos’s teachings with Stone’s teachings because:

- (1) “Stone does not identify fraud in electronic transactions as a problem” or “even discuss fraud or security”; and

- (2) “Hoyos is focused narrowly on techniques and formulas for authenticating transactions based on probabilities of biometric matching and liveness, not location.”

Prelim. Resp. 33; Prelim. Sur-reply 2.

Patent Owner asserts that an ordinarily skilled artisan would not have combined Hoyos’s teachings with Stone’s teachings for another reason: Stone, Hoyos, and Varghese “teach away from or conflict with each other in material ways.” Prelim. Resp. 37; *see id.* at 2, 30, 37–43. Specifically, Patent Owner asserts that:

- (1) Stone uses “a client-server structure for communication to populate the currency display and complete electronic transactions”;
- (2) Hoyos discloses biometric authentication that occurs “only on the client device” and “does not mention applying its authentication techniques to a client-server structure”; and
- (3) “Varghese, like Stone, envisions a client-server structure” and “authentication in Varghese involves information transferred from the client to the server.”

Id. at 37–38, 42 (citing Ex. 1008 ¶¶ 40–48; Ex. 1010 ¶¶ 5–6; Ex. 1013 ¶¶ 16–20).

Patent Owner also asserts that an ordinarily skilled artisan would not have used Hoyos’s biometric authentication in a client-server structure because that technique employs a “computationally intensive” method for face recognition “intended to handle a much smaller number of users.” Prelim. Resp. 38. As support, Patent Owner cites Hoyos’s reference to U.S. Patent No. 5,164,992, titled “Face Recognition System” to Turk et al. (“Turk”). *Id.* (citing Ex. 1013 ¶ 38); *see* Ex. 2028 (Turk), codes (54), (75). According to Patent Owner, using Hoyos’s biometric authentication in a

client-server structure with authentication occurring “on the client device would use considerable processing power and memory, which a client-server model, as Stone envisions, is meant to conserve.” Prelim. Resp. 41.

Citing Stone’s paragraph 46, Patent Owner asserts that an ordinarily skilled artisan would not have used Hoyos’s biometric authentication in Stone’s system in the manner Petitioner proposes because doing so would require a second authentication after a first authentication needed to view a user’s account balance. Prelim. Resp. 40 (citing Ex. 1008 ¶ 46). Patent Owner asserts that a second authentication would be “redundant” and “inefficient” and “would slow down the transaction time, which undermines a goal of Hoyos (transaction speed).” *Id.* at 41.

Further, Patent Owner asserts that Varghese provides a “purely software based solution to identify theft” that conflicts with the “hardware-based biometrics collection and authentication techniques described in Hoyos.” Prelim. Resp. 42–43 (quoting Ex. 1010 ¶ 22). According to Patent Owner, Varghese’s software-only goal “excludes the use of many sensor-based biometrics, such as fingerprints and facial biometrics, both of which need hardware sensors to function (e.g., fingerprint scanners and forward-facing cameras).” *Id.* at 42.

Additionally, Patent Owner contends that Varghese discloses collecting location data in a pre-authentication stage for authenticating “a user logging into a web application,” for example, but not in a post-authentication stage for completing “monetary electronic transactions.” Prelim. Resp. 45–46 (emphasis omitted) (citing Ex. 1010 ¶¶ 65, 74, 89–90). For this reason too, according to Patent Owner, combining Varghese’s

teachings with Stone’s teachings would not yield the claimed invention. *Id.* at 45.

(iii) Analysis

Based on the current record, Petitioner establishes sufficiently that an ordinarily skilled artisan would have had reasons to combine the teachings of Stone, Hoyos, and Varghese in the way Petitioner proposes. *See* Pet. 14–23, 36–39, 44–46, 49, 52–53; Ex. 1003 ¶¶ 59–70, 74–81, 113–118, 126–130, 135, 141. Further, based on the current record, Petitioner establishes sufficiently that an ordinarily skilled artisan would have had a reasonable expectation of success in combining the teachings of the references. *See* Pet. 20, 22–23; Ex. 1003 ¶¶ 71–73, 82–84.

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 identifies several advantages from using Hoyos’s biometric authentication in Stone’s system for financial transactions. *See* Pet. 16–20, 44–45, 52–53; Ex. 1008 ¶¶ 45, 48. Those advantages include “improved fraud resistancy by addressing spoofing,” “improved deterren[ce] against attempted fraudulent transactions,” and “decreased rejection of valid customers” as taught by Hoyos. Pet. 16–17, 44–45, 52–53 (quoting Ex. 1013 ¶ 15) (citing Ex. 1003 ¶¶ 64–73, 126, 141; Ex. 1013 ¶¶ 17–22); *see id.* at 17–20; Ex. 1003 ¶¶ 64–70, 126–127, 141. The “desire to enhance commercial opportunities by improving a product or process is universal” *DyStar Textilfarben GmbH v. C.H. Patrick Co.*, 464 F.3d 1356, 1368 (Fed. Cir. 2006).

A motivation to combine “can be found explicitly or implicitly in the prior art references themselves, in market forces, in design incentives, or in

‘any need or problem known in the field of endeavor at the time of invention and addressed by the patent.’” *Forest Lab ’ys, LLC v. Sigmapharm Lab ’ys, LLC*, 918 F.3d 928, 934 (Fed. Cir. 2019) (quoting *Arctic Cat Inc. v. Bombardier Recreational Prods. Inc.*, 876 F.3d 1350, 1359 (Fed. Cir. 2017)). Here, Petitioner identifies a motivation to combine “in the prior art references themselves,” i.e., in Hoyos’s disclosures about the advantages of Hoyos’s techniques, such as “improved deterren[ce] against attempted fraudulent transactions” and “decreased rejection of valid customers.” Pet. 16–17, 44–45, 52–53 (quoting Ex. 1013 ¶¶ 15, 24, 26–27, 29); *see* Ex. 1003 ¶¶ 64, 67, 126–127, 141; Ex. 1013 ¶¶ 15, 24, 26–27, 29.

Moreover, “[t]here is a motivation to combine when a known technique ‘has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way,’ using the ‘prior art elements according to their established functions.’” *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1380–81 (Fed. Cir. 2023) (citations omitted) (quoting *KSR*, 550 U.S. at 417; *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 784, 799–800 (Fed. Cir. 2021)). Here, Petitioner identifies Hoyos’s known techniques used to improve authentication for financial transactions that would improve authentication for financial transactions in Stone’s system in the same way when used according to Hoyos’s teachings. *See* Pet. 16–20, 44, 52–53; Ex. 1003 ¶¶ 64–70, 126–127, 141.

Regarding reasons to combine Varghese’s teachings with the teachings of Stone and Hoyos, Petitioner identifies several advantages from using Varghese’s real-time multifactor authentication in the Stone-Hoyos system. *See* Pet. 21, 36–39, 49. Those advantages include “improved

security for financial transactions” by providing “more accurate fraud analysis by using more accurate, real-time input data” and “additional security” due to multifactor authentication. Pet. 21–22, 36–37, 49; *see* Ex. 1003 ¶¶ 74–81, 114–118, 135.

Additionally, Petitioner explains why an ordinarily skilled artisan would have implemented Hoyos’s biometric authentication and Varghese’s real-time multifactor authentication after a user confirms a transaction request, e.g., to perform “risk-based contextual authentication” for “improved fraud detection.” *See* Pet. 18–19, 22, 38–40, 46; Ex. 1003 ¶¶ 69–70, 79–81, 116–120, 129–130.

For these reasons, we disagree with Patent Owner that Petitioner does not provide a “persuasive justification” why an ordinarily skilled artisan would have combined the teachings of Stone, Hoyos, and Varghese to yield the claimed invention. *See* Prelim. Resp. 29–30.

We also disagree with Patent Owner that Petitioner does not provide an explanation why an ordinarily skilled artisan “would have believed the combination would have succeeded.” *See* Prelim. Resp. 29–30. Patent Owner disregards Dr. Jones’s explanations that:

- (1) “Stone and Hoyos each reference the financial transaction system performed using user devices with a camera for obtaining photographs for face biometric”; and
- (2) “Stone and Varghese each reference the financial transaction system performed using user devices that provide location data.”

Ex. 1003 ¶¶ 71, 82 (citing Ex. 1008 ¶¶ 4, 26; Ex. 1009, 15:22–23; Ex. 1010 ¶ 93; Ex. 1013 ¶ 7, code (54), claims 13–14).

Patent Owner’s assertion that Stone, Hoyos, and Varghese “teach away from or conflict with each other in material ways” rests on unsupported attorney argument. *See* Prelim. Resp. 37–43. Attorney argument “cannot take the place of evidence.” *In re Pearson*, 494 F.2d 1399, 1405 (CCPA 1974). Attorney argument does not rebut Petitioner’s evidence. *See Gemtron Corp. v. Saint-Gobain Corp.*, 572 F.3d 1371, 1380 (Fed. Cir. 2009).

As for Hoyos’s citation to Turk, Hoyos explains that Turk discloses a particular method for calculating the probability of a match, P_m , for face recognition. Ex. 1013 ¶ 38; *see id.* ¶ 4 (discussing Turk in detail). But Hoyos also explains that the probability of a match, P_m , may be calculated “in any way which is desired.” *Id.* ¶ 22. The other methods for calculating the probability of a match, P_m , include “iris recognition, fingerprint image recognition, finger vein image recognition, or palm vein image recognition, . . . [and] token match.” *Id.* ¶ 22, claim 10. Patent Owner does not address whether the other methods are “computationally intensive” and “would use considerable processing power and memory.” *See, e.g.*, Prelim. Resp. 37–41.

Further, even if biometric authentication occurs “only on the client device” in Hoyos, as Patent Owner asserts, on this record we discern nothing preventing an ordinarily skilled artisan from configuring a server to perform the authentication in a client-server structure. *See* Prelim. Resp. 38. “Combining the *teachings* of references does not involve an ability to combine their specific structures.” *In re Nievelt*, 482 F.2d 965, 968 (CCPA 1973) (emphasis in original).

Consistent with configuring a server to perform the authentication, Hoyos contemplates broad implementation by explaining that the “invention is capable of considerable modification, alteration and equivalents in form and function.” Ex. 1013 ¶ 40. Also, if Hoyos’s methods for calculating the probability of a match, P_m , were too “computationally intensive” for a client device, that would prompt an ordinarily skilled artisan to configure a server to perform the authentication.

Additionally, Dr. Jones explains that in the proposed combination Hoyos’s biometric authentication could occur “locally” on a client device or “remotely” on a “payment provider device, or another remote device,” such as a server. Ex. 1003 ¶ 72 (citing Ex. 1016 ¶¶ 40, 42, 76); *see id.* ¶ 83 (providing a similar explanation for Varghese’s real-time multifactor authentication). Consistent with this, a 2003 paper titled “Privacy Preserving Multi-Factor Authentication with Biometrics” states: “Biometric authentication can be implemented through systems performing the matching either on the server or on the client side.” Ex. 1038, 64 (emphases omitted);⁸ *see* Ex. 1003 ¶ 73 (quoting Ex. 1038, 64). Patent Owner does not address Dr. Jones’s explanation that in the proposed combination Hoyos’s biometric authentication could occur “locally” or “remotely.” *See, e.g.*, Prelim. Resp. 37–41.

Also, consistent with Dr. Jones’s explanation that in the proposed combination Hoyos’s biometric authentication could occur “locally” or “remotely,” Stone explains that user device 404 may include “one or more

⁸ 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.

toolbar applications 412” that “provide client-side processing for performing tasks in response to operations selected by user 409.” Ex. 1008 ¶ 43, Fig. 4.

When asserting that an ordinarily skilled artisan would not have used Hoyos’s biometric authentication in Stone’s system in the manner Petitioner proposes because doing so would require a second authentication after a first authentication needed to view a user’s account balance, Patent Owner cites Stone’s paragraph 46. Prelim. Resp. 40 (citing Ex. 1008 ¶ 46). But paragraph 46 does not discuss an authentication needed to view a user’s account balance. *See* Ex. 1008 ¶ 46.

In any event, a “given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine.” *See Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed Cir. 2006). The “benefits, both lost and gained, should be weighed against one another.” *Winner Int’l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 n.8 (Fed. Cir. 2000).

Here, a first authentication needed to view a user’s account balance followed by a second authentication needed to transfer funds may have advantages that offset the disadvantages Patent Owner alleges. *See* Prelim. Resp. 40–41. As an example, Varghese explains that 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.” Ex. 1010 ¶ 148. Additionally, “different authentication levels may be necessary for different transactions” based on “the context of the transaction.” Ex. 1016 ¶¶ 36, 73. This issue is better resolved at trial on a more developed record.

Patent Owner's assertion that Varghese provides a "purely software based solution to identify theft" that conflicts with the "hardware-based biometrics collection and authentication techniques described in Hoyos" lacks merit. *See* Prelim. Resp. 42–43. Varghese 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. Additionally, Varghese's Figure 14 depicts "Primary/Secondary Authentication" including "Biometrics (Voiceprint, etc.)." *Id.*, Fig. 14.

Patent Owner's contention that Varghese discloses collecting location data in a pre-authentication stage for authenticating "a user logging into a web application," for example, but not in a post-authentication stage for completing "monetary electronic transactions" also lacks merit. *See* Prelim. Resp. 45–46 (emphasis omitted). Varghese discloses "real-time risk scoring" for "each online login and transaction," including during the post-authentication stage, e.g., to "re-authenticate the user or request" for "transactions that may be high risk." *See, e.g.*, Ex. 1010 ¶¶ 25, 38–39, 74–75, 77, 79, 88, 91, 97, 109, 142, 148, Fig. 14. The "real-time risk scoring" depends on, among other things, location data. *See id.* ¶¶ 77, 88, 140, 142, 181, claim 14.

For instance, Varghese's analytics-and-scoring system may collect location data from "geolocation data services providing [the] likely geographical source" during "the course of a valid already-authenticated session" when a transaction request involves "large amounts of money." *See* Ex. 1010 ¶¶ 74–75, 77, 142, 148. Further, Varghese's Figure 14 shows "Real-time Analytics & Scoring" for authentication based on, among other

things, “Location Fingerprint” including “IP, Geo-Location, Network forensics.” *Id.*, Fig. 14.

(b) Preamble 1.0

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

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

At this stage of the proceeding, Patent Owner makes no arguments specific to claim 1’s preamble. *See, e.g.*, Prelim. Resp. 29–46; Prelim. Sur-reply 1–3. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

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, based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that Stone teaches claim 1’s preamble. *See* Pet. 23–24; Ex. 1003 ¶¶ 85–88.

(c) Limitation 1.1

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

Petitioner contends that Stone teaches limitation 1.1 and alternatively that the combined disclosures in Stone, Hoyos, and Varghese teach limitation 1.1. *See* Pet. 24–26. Specifically, Petitioner asserts that Stone’s system 400 includes “one or more processors (e.g., processor 504 in user device 404 alone, or in combination with processors 504 of [other] devices in the system) configured to perform processes for a transaction.” *Id.* at 25 (citing Ex. 1008 ¶ 49, Figs. 4–5). According to Petitioner, Stone discloses the following examples for processor 504: “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, Hoyos, and Varghese teach a processor configured to perform the processes recited in limitations 1.2.1–1.4.2, including “initiating, authenticating, and completing the electronic transaction.” Pet. 26 (citing Ex. 1003 ¶ 93).

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1.1. *See, e.g.*, Prelim. Resp. 29–46; Prelim. Sur-reply 1–3.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that Stone teaches “one or more processors” according to limitation 1.1. *See* Pet. 24–26; Ex. 1003 ¶¶ 89–94.

(d) Limitation 1.2.1

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

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

Second, Petitioner asserts that Stone’s Figure 2 shows the photo of the recipient in name box 202. Pet. 28 (citing Ex. 1008 ¶¶ 20, 24, 36, Fig. 2).

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1.2.1. *See, e.g.*, Prelim. Resp. 29–46; Prelim. Sur-reply 1–3.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that Stone teaches limitation 1.2.1. *See* Pet. 26–29; Ex. 1003 ¶¶ 95–99.

(e) Limitation 1.2.2

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

Petitioner contends that Stone teaches limitation 1.2.2. *See* Pet. 29–32, 70. Specifically, Petitioner asserts that Stone discloses:

- (1) “the account holder (user 409) registers using user device 404 with the payment provider 408 with a user account 422” during enrollment/registration; and

- (2) “the user identifier 418 (including ‘photograph image’ selected by the user for display on virtual currency, profile icon, etc.) is generated and stored” on user device 404.

Id. at 29–30 (quoting Ex. 1008 ¶ 45). Petitioner also asserts that “[s]imilar features apply to [a] recipient account holder using recipient device 406.”

Id. at 30 (citing Ex. 1003 ¶¶ 101–102; Ex. 1008 ¶¶ 45–46, 48).

Further, Petitioner asserts that Stone’s “user registration/enrollment includes biometric enrollment, because it was well-known that ‘biometric id’ of its user identifier 418 was captured and stored during biometric enrollment, where the stored biometric id is used (and as such referred to) as ‘enrollment data’ for comparison with the later captured data for authentication.” Pet. 30–31 (emphases omitted) (quoting Ex. 1008 ¶ 45).

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

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1.2.2. *See, e.g.*, Prelim. Resp. 29–46; Prelim. Sur-reply 1–3.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that Stone teaches limitation 1.2.2. *See* Pet. 29–32; Ex. 1003 ¶¶ 100–107.

(f) Limitation 1.3.1

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

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

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

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

Further, Petitioner asserts that Stone’s Figure 3 illustrates steps or blocks that an ordinarily skilled artisan would have implemented with icons serving as visual indicators to the user for “various user interactions to

continue/confirm the transaction.” Pet. 34 (citing Ex. 1003 ¶ 111; Ex. 1008 ¶¶ 24–25).

Petitioner also asserts that to the extent Stone does not explicitly describe Figure 2’s control elements and Figure 3’s blocks as an “icon,” an ordinarily skilled artisan “would have been motivated to implement the control items/blocks using an icon, because icon and button are alternative design choices for control elements/blocks, and using icons provides ‘a more visually rich interface.’” Pet. 34–35 (quoting Ex. 1008 ¶ 16) (citing Ex. 1008 ¶¶ 4, 35, 38).

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

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

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1.3.1. *See, e.g.*, Prelim. Resp. 29–46; Prelim. Sur-reply 1–3.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that “Stone in view of Hoyos and Varghese” teaches limitation 1.3.1. *See* Pet. 32–40; Ex. 1003 ¶¶ 108–120.

(g) Limitation 1.3.2

Claim 1 requires a processor configured to “capture a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images” subsequent to “an interaction by a user with an icon rendered in the one or more interfaces.” Ex. 1001, 14:8–9, 14:13–15 (limitation 1.3.2).

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

Petitioner asserts that Hoyos discloses “capturing a set of biometric information for performing biometric authentication including fraud detection (including blocks 11 and 13 of FIG. 1).” Pet. 41 (citing Ex. 1003 ¶ 123; Ex. 1013 ¶ 17). According to Petitioner, Hoyos’s biometric information includes “a set of user facial images (e.g., portion thereof containing a representation of a human eye) captured using a camera (e.g., web-camera 26).” *Id.* at 42 (citing Ex. 1003 ¶ 124; Ex. 1011, code (57); Ex. 1012, code (57); Ex. 1013 ¶¶ 3, 12, 18–22, 40). As support, Petitioner

quotes the following limitations in Hoyos’s claim 7: (1) “obtaining [a] first image of a user positioned in front of a computer screen from a first perspective”; and (2) “obtaining a second image of the user positioned in front of the computer screen from a second perspective.” *Id.* at 42–43 (quoting Ex. 1013, claim 7).

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

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1.3.2. *See, e.g.*, Prelim. Resp. 29–46; Prelim. Sur-reply 1–3.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that “Stone in view of Hoyos and Varghese” teaches limitation 1.3.2. *See* Pet. 41–47; Ex. 1003 ¶¶ 121–131.

(h) Limitation 1.4.1

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

Petitioner contends that “Stone in view of Hoyos and Varghese” teaches limitation 1.4.1. *See* Pet. 47–49. Specifically, Petitioner explains that in the proposed combination Stone’s user device 404 would “capture information including location information and biometric information, and

these captured information (e.g., location data usable to determine a physical location associated with the user, the set of biometric information including a set of images) are provided to facilitate a fraud detection analysis.” *Id.* at 47. According to Petitioner, “the fraud detection analysis provides a decision regarding whether the transaction is authenticated/authorized.” *Id.*

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

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1.4.1. *See, e.g.*, Prelim. Resp. 29–46; Prelim. Sur-reply 1–3.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that “Stone in view of Hoyos and Varghese” teaches limitation 1.4.1. *See* Pet. 47–49; Ex. 1003 ¶¶ 132–135.

(i) Limitation 1.4.2

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

Petitioner contends that “Stone in view of Hoyos and Varghese” teaches limitation 1.4.2. *See* Pet. 50–53. Specifically, Petitioner asserts that

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

Further, Petitioner asserts that Hoyos discloses “facilitating and performing fraud detection by performing an analysis of the set of captured biometric information.” Pet. 50 (citing Ex. 1003 ¶ 138; Ex. 1013 ¶¶ 17–22, 40, claims 1 and 5–8). Petitioner also asserts that Hoyos’s biometric authentication includes determining whether the user is alive “based at least in part on an analysis of the set of images, including computing the probability, P_p of a live person being presented (e.g., block 11 of FIG. 1) based on analysis of the set of captured images (e.g., as described with reference to FIGS. 2–4).” *Id.* at 51 (citing Ex. 1003 ¶ 139; Ex. 1013, Fig. 1); *see id.* at 51–52.

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1.4.2. *See, e.g.*, Prelim. Resp. 29–46; Prelim. Sur-reply 1–3.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that “Stone in view of Hoyos and Varghese” teaches limitation 1.4.2. *See* Pet. 50–53; Ex. 1003 ¶¶ 136–142.

(j) Limitation 1.5

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

Petitioner contends that Stone teaches limitation 1.5 because Stone discloses “a memory (memory component 506 of FIG. 5) coupled to a processor 504 in each device of the system including e.g., user devices 404.” Pet. 54; *see id.* at 81. According to Petitioner, “the memory is configured to provide the processor with instructions,” such as “instructions to create and display the proper currencies, convert currency, display various types of graphics showing transfer of currency, etc.” *Id.* at 54 (quoting Ex. 1008 ¶ 50) (citing Ex. 1008 ¶ 49, Fig. 5).

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1.5. *See, e.g.*, Prelim. Resp. 29–46; Prelim. Sur-reply 1–3.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that Stones teaches limitation 1.5. *See* Pet. 53–54; Ex. 1003 ¶¶ 143–146.

(k) Preliminary Conclusion About Obviousness/Nonobviousness

As discussed above, Petitioner’s analysis addresses how the combined disclosures in Stone, Hoyos, and Varghese teach claim 1’s subject matter. *See supra* §§ IV.D.5(b)–(j). Additionally, Petitioner provides reasons with rational underpinnings as to why an ordinarily skilled artisan would have been motivated to combine the teachings of Stone, Hoyos, and Varghese in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § IV.D.5(a)(iii). Hence, Petitioner demonstrates a

reasonable likelihood of proving that claim 1 is unpatentable under § 103(a) as obvious over Stone, Hoyos, and Varghese.

6. INDEPENDENT CLAIMS 6 AND 11

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

Petitioner identifies disclosures in Stone corresponding to claim 6’s preamble and claim 11’s preamble. Pet. 60–62. Additionally, Petitioner contends that the combined disclosures in Stone, Hoyos, and Varghese teach claim 6’s subject matter and claim 11’s subject matter for the reasons that the combined disclosures teach claim 1’s subject matter. *See id.* at 61–63. Dr. Jones’s testimony supports Petitioner’s contentions. *See* Ex. 1003 ¶¶ 95–142, 164–172, 177–185.

At this stage of the proceeding, Patent Owner makes no arguments specific to claim 6 or claim 11. *See, e.g.,* Prelim. Resp. 29–46; Prelim. Sur-reply 1–3.

Based on the current record and for (1) the reasons stated by Petitioner and supported by Dr. Jones’s testimony and (2) the reasons discussed above for claim 1, Petitioner establishes sufficiently that the combined disclosures in Stone, Hoyos, and Varghese teach claim 6’s subject matter and claim 11’s subject matter. *See* Pet. 60–63; Ex. 1003 ¶¶ 95–142, 164–172, 177–185; *supra* §§ IV.D.5(c)–(i). Additionally, as discussed above, Petitioner provides reasons with rational underpinnings as to why an ordinarily skilled

artisan would have been motivated to combine the teachings of Stone, Hoyos, and Varghese in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § IV.D.5(a)(iii). Hence, Petitioner demonstrates a reasonable likelihood of proving that claims 6 and 11 are unpatentable under § 103(a) as obvious over Stone, Hoyos, and Varghese.

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

Claims 2–5, 12, and 14–17 depend directly or indirectly from claim 1. Ex. 1001, 14:28–38, 15:32–35, 16:1–15. Claims 7–10, 18, and 20–23 depend directly or indirectly from claim 6. *Id.* at 14:62–15:5, 16:16–19, 16:24–38.

For claims 2–5, 7–10, 12, 14–18, and 20–23, Petitioner provides an analysis supported by Dr. Jones’s testimony about how the combined disclosures in Stone, Hoyos, and Varghese teach the claimed subject matter. *See* Pet. 52–60, 62–67; Ex. 1003 ¶¶ 147–163, 173–176, 186–204.

At this stage of the proceeding, Patent Owner makes no arguments specific to any of claims 2–5, 7–10, 12, 14–18, and 20–23. *See, e.g.*, Prelim. Resp. 29–46; Prelim. Sur-reply 1–3.

Based on the current record and for (1) the reasons stated by Petitioner and supported by Dr. Jones’s testimony and (2) the reasons discussed above for claims 1 and 6, Petitioner establishes sufficiently that the combined disclosures in Stone, Hoyos, and Varghese teach the subject matter in claims 2–5, 7–10, 12, 14–18, and 20–23. *See* Pet. 52–60, 62–67; Ex. 1003 ¶¶ 147–163, 173–176, 186–204; *supra* §§ IV.D.5–IV.D.6. Hence, Petitioner demonstrates a reasonable likelihood of proving that claims 2–5, 7–10, 12,

14–18, and 20–23 are unpatentable under § 103(a) as obvious over Stone, Hoyos, and Varghese.

E. Alleged Obviousness over Stone, Hoyos, Varghese, and Campbell: Claims 15–17 and 21–23

Petitioner contends that claims 15–17 and 21–23 are unpatentable under § 103(a) as obvious over Stone, Hoyos, Varghese, and Campbell. *See* Pet. 5–6, 87–91; Prelim. Reply 3–5. Patent Owner disputes Petitioner’s contentions. *See* Prelim. Resp. 29–46; Prelim. Sur-reply 1–3.

Above, we provided overviews of Stone, Hoyos, and Varghese. *See supra* §§ IV.D.1–IV.D.3. Below, we provide an overview of Campbell. Then, we consider the obviousness issues. For the reasons explained below, Petitioner establishes sufficiently for purposes of institution that the combined disclosures in Stone, Hoyos, Varghese, and Campbell teach the subject matter in claims 15–17 and 21–23.

1. OVERVIEW OF CAMPBELL (EXHIBIT 1033)

Campbell is a paper titled “Speaker Recognition: A Tutorial” by Joseph P. Campbell, Jr., published in the Proceedings of the IEEE in September 1997. Ex. 1033, 1437.⁹ Campbell explains that automatic speaker verification (also called voice verification, speaker authentication, voice authentication, talker authentication, and talker verification) uses “a machine to verify a person’s claimed identity” from the person’s voice. *Id.* “Prior to a verification session, users must enroll in the system (typically under supervised conditions).” *Id.* “During this enrollment, voice models

⁹ For Exhibit 1033 (Campbell), we follow Petitioner’s practice and cite to the page numbers that appear in the publication instead of the page numbers that Petitioner applied to the exhibit.

are generated and stored (possibly on a smart card) for use in later verification sessions.” *Id.* at 1437–38.

Campbell explains that a “generic” approach to automatic speaker verification consists of five steps as follows: “digital speech data acquisition, feature extraction, pattern matching, making an accept/reject decision, and enrollment to generate speaker reference models.” Ex. 1033, 1438.

Campbell’s Figure 3 (reproduced below) is a block diagram of a “generic” speaker-verification system:

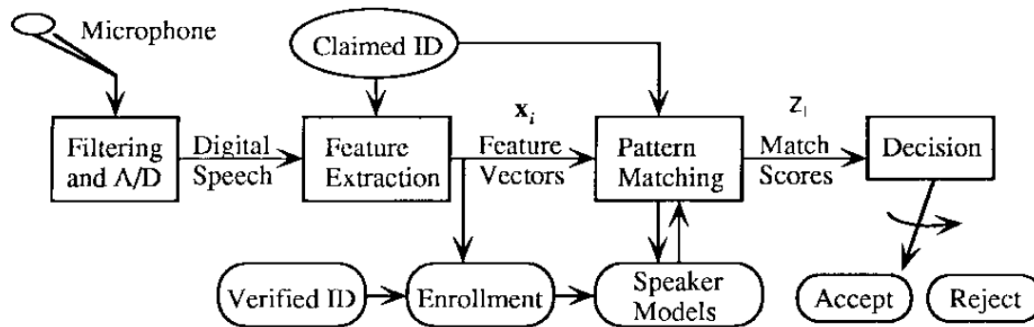


Fig. 3. Generic speaker-verification system.

Figure 3 illustrates a speaker-verification system where:

- (1) digital speech data acquisition involves a person speaking into a microphone followed by signal processing to produce digital speech, i.e., converting analog signals resulting from acoustic waves into digital signals;
- (2) feature extraction uses digital speech to map “each interval of speech to a multidimensional feature space” to produce feature vectors x_i ;
- (3) pattern matching compares feature vectors x_i to “models of the claimed speaker or feature vector patterns for the claimed speaker” to produce a match score z_i that measures similarity; and

- (4) decision making determines whether to “accept or reject the claimant according to the match score or sequence of match scores.”

See id. at 1437–38, 1440–41.

Campbell describes a speech-processing technique called the “mel-warped cepstrum” as “a very popular feature domain” that “has been demonstrated to work well in speaker-recognition systems.” Ex. 1033, 1445. “The mel warping transforms the frequency scale to place less emphasis on high frequencies” due to “the nonlinear human perception of the frequency of sounds.” *Id.* “The cepstrum can be considered as the spectrum of the log spectrum.” *Id.*

The “mel-warped cepstrum” may be computed as follows:

- (1) “window the signal”;
- (2) “take the fast Fourier transform (FFT)”;
- (3) “take the magnitude”;
- (4) “take the log”;
- (5) “warp the frequencies according to the mel scale”; and
- (6) “take the inverse FFT.”

Ex. 1033, 1445.

2. WHETHER CAMPBELL TEACHES THE LIMITATIONS IN CLAIMS 15–17 AND 21–23

Claims 15–17 depend directly or indirectly from claim 1 and read as follows:

15. The system recited in claim 1, wherein the set of captured biometric information further comprises an audio sample.

16. The system recited in claim 15, wherein facilitating the fraud detection analysis to determine whether the electronic transaction associated with the account holder is allowed to

proceed is further based at least in part on a determination of whether the audio sample matches a previously recorded voice sample.

17. The system recited in claim 16, wherein the determination of whether the audio sample matches the previously recorded voice sample is based at least in part on performing a Fast Fourier Transform.

Ex. 1001, 16:4–15. Claims 21–23 depend directly or indirectly from claim 6 and include limitations similar to claims 15–17, respectively. *Id.* at 16:27–38.

Petitioner contends that Campbell teaches the limitations in claims 15–17 and 21–23 because Campbell discloses:

- (1) “the well-known fundamental knowledge that captured biometric information for voice authentication includes an audio sample”;
- (2) “the well-known fundamental knowledge of matching the captured audio sample with a previously recorded voice sample for voice authentication in ‘enrollment’”; and
- (3) “using FFT-based feature extraction for matching to implement voice authentication.”

Pet. 88–91 (citing Ex. 1003 ¶¶ 299–300, 303–305; Ex. 1033, 1438, 1440, 1445).

At this stage of the proceeding, Patent Owner makes no arguments specific to any of claims 15–17 and 21–23. *See, e.g.*, Prelim. Resp. 29–54; Prelim. Sur-reply 1–3.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that Campbell teaches the limitations in claims 15–17 and 21–23. *See* Pet. 88–91; Ex. 1003 ¶¶ 293–306.

3. ALLEGED REASON TO COMBINE
THE TEACHINGS OF THE REFERENCES

Petitioner asserts that an ordinarily skilled artisan would have been motivated to:

- (1) “implement multifactor authentications including voice authentication for improved security”; and
- (2) use Campbell’s speaker-verification techniques, including “FFT-based feature extraction,” in the Stone-Hoyos-Varghese system to “achieve better performance for reducing fraudulent transactions.”

Pet. 87 (citing Ex. 1003 ¶¶ 288–292; Ex. 1010 ¶ 145; Ex. 1016 ¶¶ 36, 40–41, Fig. 4; Ex. 1018, 51:12–15, 52:20–24; Ex. 1033, 1438). As support, Petitioner quotes Campbell’s description of the “mel warped cepstrum” as a “very popular” speaker-recognition technique that had “been demonstrated to work well in speaker-recognition systems.” *Id.* at 88 (quoting Ex. 1033, 1445).

Dr. Jones’s testimony supports Petitioner’s positions. *See* Ex. 1003 ¶¶ 288, 290–292.

At this stage of the proceeding, Patent Owner makes no arguments against combining Campbell’s teachings with the teachings of Stone, Hoyos, and Varghese. *See, e.g.*, Prelim. Resp. 29–54; Prelim. Sur-reply 1–3.

Based on the current record, Petitioner establishes sufficiently that an ordinarily skilled artisan would have had a reason to combine Campbell’s teachings with the teachings of Stone, Hoyos, and Varghese in the way Petitioner proposes, e.g., to “achieve better performance for reducing fraudulent transactions.” *See* Pet. 87–88; Ex. 1003 ¶¶ 288, 290–292.

4. PRELIMINARY CONCLUSION ABOUT OBVIOUSNESS/NONOBVIOUSNESS

As discussed above, Petitioner's analysis addresses how the combined disclosures in Stone, Hoyos, Varghese, and Campbell teach the subject matter in claims 15–17 and 21–23. *See supra* §§ IV.D.5–IV.D.6, IV.E.2. Additionally, Petitioner provides a reason with rational underpinning as to why an ordinarily skilled artisan would have been motivated to combine Campbell's teachings with the teachings of Stone, Hoyos, and Varghese in the way Petitioner proposes. *See supra* § IV.E.3. Hence, Petitioner demonstrates a reasonable likelihood of proving that claims 15–17 and 21–23 are unpatentable under § 103(a) as obvious over Stone, Hoyos, Varghese, and Campbell.

F. Alleged Obviousness over Stone and the Guidance: Claims 1–12, 14–18, and 20–23

Petitioner contends that claims 1–12, 14–18, and 20–23 are unpatentable under § 103(a) as obvious over Stone and the Guidance. *See* Pet. 5, 67–86; Prelim. Reply 3–5. Patent Owner disputes Petitioner's contentions. *See* Prelim. Resp. 46–54; Prelim. Sur-reply 1–3.

Above, we provided an overview of Stone. *See supra* § IV.D.1. Below, we provide an overview of the Guidance. Then, we consider the obviousness issues. For the reasons explained below, Petitioner establishes sufficiently for purposes of institution that the combined disclosures in Stone and the Guidance teach the subject matter in claims 1–12, 14–18, and 20–23.

1. OVERVIEW OF THE GUIDANCE (EXHIBIT 1037)

The Guidance is a publication titled “Authentication in an Internet Banking Environment” issued in October 2005 by the FFIEC agencies.¹⁰ Ex. 1037, 1; Ex. 1039, 1; Ex. 1040, 1. For financial institutions “offering Internet-based financial services, the [G]uidance describes enhanced authentication methods that regulators expect banks to use when authenticating the identity of customers using the on-line products and services.” Ex. 1039, 1. The Guidance “specifically addresses why financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services.” Ex. 1037, 1. Among other things, the Guidance reflects “the introduction of improved authentication technologies.” Ex. 1040, 1; *see* Ex. 1037, 1.

“The [G]uidance is divided into two parts.” Ex. 1040, 1. The main portion “provides financial institutions with guidance on authentication and discusses appropriate risk assessments, customer authentication, verification of new customers, and monitoring and reporting.” *Id.* An appendix “provides more detail about various authentication technologies.” *Id.*

The Guidance explains that “[a]n effective authentication system is necessary for compliance with requirements to safeguard customer information, to prevent money laundering and terrorist financing, to reduce

¹⁰ The FFIEC agencies include the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. *See* Ex. 1040, 2.

fraud, to inhibit identity theft, and to promote the legal enforceability of their electronic agreements and transactions.” Ex. 1037, 2 (footnotes omitted).

The Guidance notes that existing authentication methods involve three basic “factors” as follows:

- “Something the user *knows* (e.g., password, PIN);
- “Something the user *has* (e.g., ATM card, smart card);
and
- “Something the user *is* (e.g., biometric characteristic, such as a fingerprint).”

Ex. 1037, 3 (emphases in original); *see id.* at 7.

Because multifactor authentication methods are “more difficult to compromise” than single-factor authentication methods, “properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents.” Ex. 1037, 3; *see id.* at 4, 6–7. “The selection and use of any technique should be based upon the assessed risk associated with a particular electronic banking product or service.” *Id.* at 8.

The Guidance explains that biometric identifiers are “most commonly used as part of a multifactor authentication system, combined with a password (something a person knows) or a token (something a person has).” Ex. 1037, 10 (emphases omitted). The Guidance identifies the following biometric techniques: fingerprint recognition; face recognition; voice recognition; keystroke recognition; handwriting recognition; finger and hand geometry; retinal scan; and iris scan. *Id.* Also, some face-recognition applications include “tests for liveness, such as blinking eyes.” *Id.* at 11. “Testing for liveness reduces the chance that the person requesting access is using a photograph of an authorized individual.” *Id.*

Additionally, the Guidance describes geo-location technology as “another technique to limit Internet users by determining where they are or, conversely, where they are not.” Ex. 1037, 12. More specifically, geo-location software “inspects and analyzes the small bits of time required for Internet communications to move through the network” and then converts the electronic travel times into cyberspace distances. *Id.* The cyberspace distances for a user are compared with cyberspace distances for known locations. *Id.* “If the comparison is considered reasonable, the user’s location can be authenticated.” *Id.* “If the distance is considered unreasonable or for some reason is not calculable, the user will not be authenticated.” *Id.*

2. INDEPENDENT CLAIM 1

(a) Whether an Ordinarily Skilled Artisan Would Have Been Motivated to Combine the Teachings of the References with a Reasonable Expectation of Success

(i) Petitioner’s Proposed Combination

Petitioner asserts that an ordinarily skilled artisan would have been motivated to use the Guidance’s teachings about multifactor, real-time, risk-based authentication in Stone’s system for financial transactions to obtain:

- (1) the benefits of “improved security and boosted customer confidence” for service providers of financial transactions resulting from multifactor, real-time, risk-based authentication for fraud analysis; and
- (2) the additional benefits of “FFIEC compliance” for federally supervised financial institutions.

See Pet. 68, 73–74 (citing Ex. 1003 ¶¶ 206–209, 222; Ex. 1037, 1–2, 10, 12). According to Petitioner, an ordinarily skilled artisan would have understood that “the Guidance was a recognized driver for implementing multifactor

authentication,” as shown in “numerous articles and patent disclosures.” *Id.* at 68–69 (citing Ex. 1003 ¶ 52; Ex. 1010 ¶ 148; Ex. 1013 ¶¶ 9, 11; Ex. 1016 ¶ 73, Fig. 3).

Petitioner asserts that “physical location authentication would [have been] selected for benefits” 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. 73 (citing Ex. 1003 ¶ 221; Ex. 1010 ¶¶ 12, 35; Ex. 1016 ¶ 43). Petitioner further asserts that “biometrics authentication using facial recognition with liveness test would [have been] selected along with the physical location authentication for the benefits of contactless and hygienic authentication using easy to acquire (e.g., using a camera) facial images and spoof-proofing.” *Id.* (citing Ex. 1013 ¶ 7; Ex. 1037, 11).

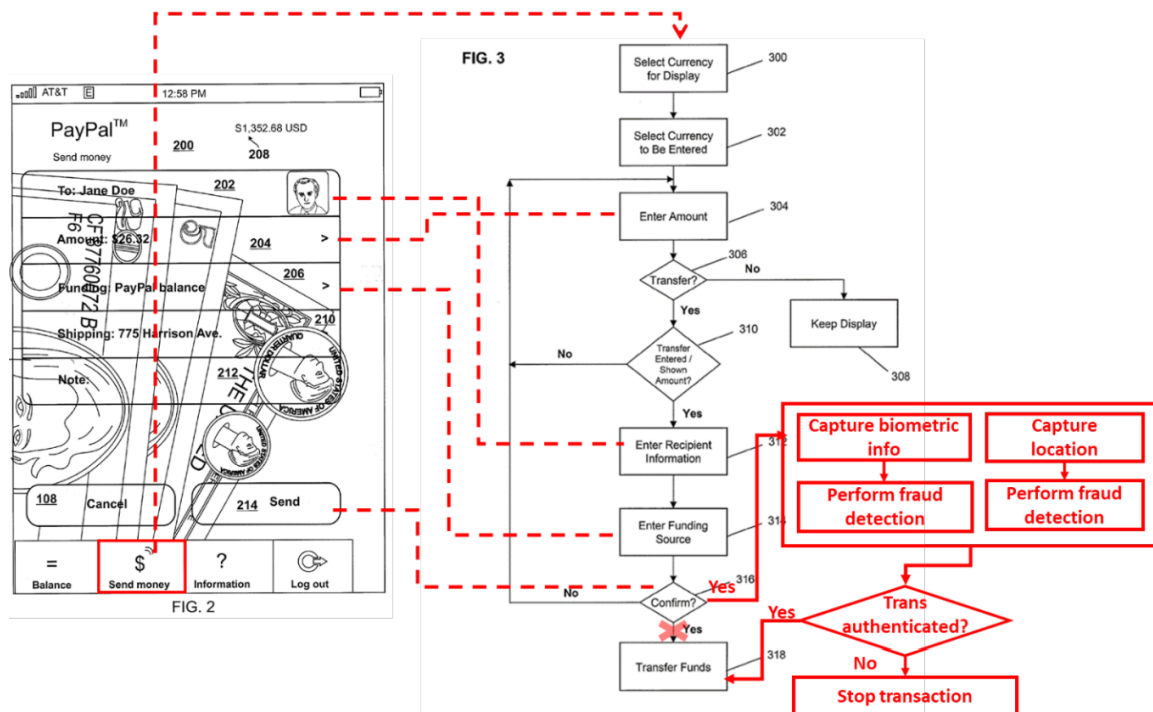
Petitioner explains that in the proposed combination multifactor, real-time, risk-based authentication according to the Guidance would occur after a user confirms a transaction request, i.e., after (1) user interaction with an icon to initiate a transaction, such as a user actuating the “\$ Send money” button in Stone’s display, and (2) user interactions with additional icons in Stone’s display to continue the transaction and confirm the transaction request. Pet. 75.

According to Petitioner, performing multifactor, real-time, risk-based authentication after a user confirms a transaction request achieves various advantages, including:

- (1) “enabling contextual authentication adaptive for the specific transaction based on transaction information (e.g., type, amount) for improved fraud detection”;
- (2) “providing more accurate and updated real-time information for real-time authentication”; and
- (3) “performing fraud analysis based on location match (e.g., between locations captured before and after confirmation at 316) for improved security.”

Pet. 75–76 (citing Ex. 1010 ¶¶ 91, 148, Fig. 14; Ex. 1015, Fig. 4; Ex. 1016 ¶ 43).

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 the Guidance (Pet. 75):



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.”

See Pet. 75; Ex. 1003 ¶ 223; Ex. 1008 ¶¶ 11–12, 16, 23–24, 29–35, Figs. 2–3.

Further, Petitioner asserts that an ordinarily skilled artisan “would have reasonably expected to succeed in configuring Stone to implement the multifactor real-time risk-based authentication functionality taught by [the] Guidance, since its implementation would have required only routine knowledge well within” the artisan’s skill. Pet. 69 (citing Ex. 1003 ¶ 209).

Dr. Jones’s testimony supports Petitioner’s positions. *See* Ex. 1003 ¶¶ 206–209, 221–225.

(ii) Patent Owner’s Contentions

Patent Owner contends that Petitioner’s motivation-to-combine assertions are “conclusory and provide no actual explanation” why an ordinarily skilled artisan “would have combined Stone and the Guidance.”

Prelim. Resp. 53; *see id.* at 52; Prelim. Sur-reply 2. Patent Owner also contends that:

- (1) Stone “is not concerned with security of transactions” and “does not view fraud as a problem that needs to be addressed”;
- (2) Stone “is concerned with providing an improved display for the user and ‘richer interface’ that provides a currency display”;
- (3) the Guidance “is not concerned with conveying amounts of funds or visual representations of currency or providing a digital interface” and “never discusses using multifactor or biometric authentication with a digital interface”; and
- (4) Stone and the Guidance “are compartmentalized references concerned with different objectives—Stone (currency display and an improved interface) and [the] Guidance (providing a high-level overview of multifactor authentication techniques, including biometrics).”

Prelim. Resp. 53–54 (quoting Ex. 1008 ¶ 16); Prelim. Sur-reply 2.

According to Patent Owner, “[t]he teachings of these references do not overlap.” Prelim. Resp. 54.

Also, Patent Owner argues that the Board should give little or no weight to Dr. Jones’s declaration because his “analysis of the motivation to combine and the reasonable expectation of success is virtually identical to the analysis in the Petition.” Prelim. Resp. 46–47, 52; *see id.* at 47–51 (citing Pet. 68–70; Ex. 1003 ¶¶ 206–209); Prelim. Sur-reply 1, 3. As support, Patent Owner cites the following cases where the Board gave an expert’s declaration little or no weight because, according to Patent Owner, the declaration “contained arguments that were identical to arguments set forth in the petition”: *Kinetic Technologies, Inc. v. Skyworks Solutions, Inc.*,

IPR2014-00529, Paper 8 at 14–15 (PTAB Sept. 23, 2014); *Volkswagen Group of America, Inc. v. StratosAudio, Inc.*, IPR2021-00717, Paper 12 at 36–38 (PTAB Nov. 12, 2021); and *Samsung Electronics Co., Ltd. v. RightQuestion, LLC*, IPR2022-00251, Paper 17 at 24 (PTAB June 9, 2022). Prelim. Resp. 46–47, 51.

(iii) Analysis

Based on the current record, Petitioner establishes sufficiently that an ordinarily skilled artisan would have had reasons to combine the Guidance’s teachings with Stone’s teachings in the way Petitioner proposes. *See* Pet. 68–69, 73–76; Ex. 1003 ¶¶ 206–208, 221–225. Further, based on the current record, Petitioner establishes sufficiently that an ordinarily skilled artisan would have had a reasonable expectation of success in combining the teachings of the references. *See* Pet. 69–70; Ex. 1003 ¶ 209.

Regarding reasons to combine the Guidance’s teachings with Stone’s teachings, Stone contemplates security measures for financial transactions, such as using a “password” or “biometric id,” and Petitioner identifies several advantages from using the Guidance’s teachings in Stone’s system for financial transactions. *See* Pet. 68–69, 73–76; Ex. 1008 ¶¶ 45, 48. Those advantages include “improved security and boosted customer confidence” for service providers of financial transactions resulting from multifactor, real-time, risk-based authentication for fraud analysis. Pet. 68, 73–74; *see* Ex. 1003 ¶¶ 206, 221, 223–224.

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*, 61 F.4th at 1380–81. Here, Petitioner identifies the Guidance’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 the Guidance’s teachings. *See* Pet. 68, 73–74; *see* Ex. 1003 ¶¶ 206, 221, 223–224.

Hence, we disagree with Patent Owner that Petitioner’s motivation-to-combine assertions are “conclusory and provide no actual explanation” why an ordinarily skilled artisan “would have combined Stone and the Guidance.” *See* Prelim. Resp. 53.

As for Patent Owner’s contentions concerning the weight we should give to Dr. Jones’s declaration, they lack merit. *See* Prelim. Resp. 46–52. In *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 at 15–16 (PTAB Aug. 24, 2022) (precedential), the Board accorded little weight to a proffered expert’s declaration that (1) repeated verbatim a conclusory statement in a petition and (2) did not “cite to any additional supporting evidence or provide any technical reasoning to support” the conclusory statement.

But verbatim duplication between a brief and a declaration does not require giving the declarant’s testimony little or no weight. *See Unified Patents, LLC v. Togail Techs., Ltd.*, IPR2023-00338, Paper 7 at 11 (PTAB Aug. 18, 2023) (declining to give “little or no weight” to declaration testimony “simply because it is verbatim to” statements in a petition); *Hum Indus. Tech., Inc. v. Amsted Rail Co.*, IPR2023-00540, Paper 10 at 37 (PTAB Aug. 11, 2023) (explaining that “[i]f declaration testimony is supported sufficiently and, in turn, supports contentions in the Petition, we do not give it little to no weight simply because it is repeated in the

Petition”); *Epic Games, Inc. v. IngenioShare, LLC*, IPR2022-00202, Paper 29 at 9 (PTAB May 19, 2023) (declining to disregard a declarant’s testimony that mirrored a brief). The Board decisions that Patent Owner cites do not hold otherwise. *See Kinetic*, IPR2014-00529, Paper 8 at 14–16; *Volkswagen*, IPR2021-00717, Paper 12 at 34–38; *Samsung*, IPR2022-00251, Paper 17 at 23–26; Prelim. Resp. 46–47, 51; Prelim. Reply 1–2.

In *Kinetic*, the Board determined that the petition failed to establish a reason to combine references and that a proffered expert’s declaration with identical text also failed to establish a reason to combine references. *Kinetic*, IPR2014-00529, Paper 8 at 14–16. In *Volkswagen* and *Samsung*, the Board determined that the petition failed to explain how a reference taught a claim limitation and that a proffered expert’s declaration with identical or virtually identical text also failed to explain how the reference taught the claim limitation. *Volkswagen*, IPR2021-00717, Paper 12 at 34–38; *Samsung*, IPR2022-00251, Paper 17 at 23–26. As Petitioner asserts, these decisions “stand for the proposition that conclusory, unsupported arguments by a party in its substantive paper(s) do not acquire greater evidentiary weight in mere repetition by an expert of the conclusory, unsupported arguments.” *See* Prelim. Reply 1.

Moreover, in contrast to *Xerox*, Petitioner and Dr. Jones provide technical reasoning regarding a motivation to combine and a reasonable expectation of success and cite supporting evidence. *See* Pet. 68–70; Ex. 1003 ¶¶ 206–209.

(b) Preamble 1.0 and Limitations 1.1, 1.2.1, 1.2.2, and 1.5

Petitioner explains that its analysis of Stone for the Stone-Guidance challenge is “substantially similar” to its analysis of Stone for the Stone-

Hoyos-Varghese challenge. Pet. 67. For the Stone-Guidance challenge, Petitioner identifies disclosures in Stone corresponding to claim 1's preamble and limitations 1.1, 1.2.1, 1.2.2, and 1.5. *Id.* at 70, 81; *see id.* at 23–32, 53–54.

At this stage of the proceeding, Patent Owner makes no arguments specific to claim 1's preamble or limitations 1.1, 1.2.1, 1.2.2, and 1.5. *See, e.g.,* Prelim. Resp. 46–54; Prelim. Sur-reply 1–3. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones's testimony, Petitioner establishes sufficiently that Stone teaches claim 1's preamble and limitations 1.1, 1.2.1, 1.2.2, and 1.5. *See* Pet. 23–32, 53–54, 70, 81; Ex. 1003 ¶¶ 85–107, 143–146, 210–216, 240.

(c) Limitation 1.3.1

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

Petitioner contends that the combined disclosures in Stone and the Guidance teach limitation 1.3.1 for several related reasons. *See* Pet. 71–76. Specifically, Petitioner asserts that Stone teaches “an interaction by a user with an icon rendered in the one or more interfaces” because Stone's Figure 2 illustrates display 200 on an electronic device including the following “control elements” or icons that a user interacts with:

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

See id. at 71–72.

Additionally, Petitioner contends that the Guidance discloses multifactor, real-time, risk-based authentication for financial transactions, including “location authentication” and “biometric authentication.” Pet. 72–73 (citing Ex. 1003 ¶¶ 219–220; Ex. 1010 ¶ 35; Ex. 1037, 3, 11–12). According to Petitioner, the Guidance “describes selecting from the various authentication techniques based on risk assessment of the transaction request.” *Id.* at 73.

Further, Petitioner asserts that “location authentication” involves “capturing contextual information including location data usable to determine a physical location associated with the user.” Pet. 72. Petitioner asserts that “biometric authentication” according to the Guidance includes “face recognition (‘Something a person is’/‘something you are’) with testing for liveness, based on the risk of the transaction.” *Id.* at 72–73 (quoting Ex. 1010 ¶ 35; Ex. 1037, 7).

Also, as discussed above, Petitioner explains that in the proposed combination multifactor, real-time, risk-based authentication according to the Guidance would occur after a user confirms a transaction request by interacting with an icon rendered in an interface. Pet. 69–70, 74–75; *see supra* § IV.F.2(a)(i).

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1.3.1. *See, e.g.*, Prelim. Resp. 46–54; Prelim. Sur-reply 1–3.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that the combined disclosures in Stone and the Guidance teach limitation 1.3.1. *See* Pet. 71–76; Ex. 1003 ¶¶ 217–226.

(d) Limitation 1.3.2

Claim 1 requires a processor configured to “capture a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images” subsequent to “an interaction by a user with an icon rendered in the one or more interfaces.” Ex. 1001, 14:8–9, 14:13–15 (limitation 1.3.2).

Petitioner contends that the combined disclosures in Stone and the Guidance teach limitation 1.3.2. *See* Pet. 76–77. Specifically, Petitioner asserts that the combined disclosures teach “an interaction by a user with an icon rendered in the one or more interfaces” and “biometric authentication” for the reasons discussed for limitation 1.3.1. *Id.* at 77.

Additionally, Petitioner asserts that the Guidance discloses:

- (1) “biometric authentication using face recognition with liveness tests using facial scans captured by a camera,” such as (a) “a still camera to capture a sequence of images at different times” and (b) “a video camera to capture a video with subsequent frames” with “each frame being an image”; and
- (2) “the facial scans are analyzed for ‘tests for liveness, such as blinking eyes.’”

Pet. 77 (emphasis omitted) (quoting Ex. 1037, 11).

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1.3.2. *See, e.g.*, Prelim. Resp. 46–54; Prelim. Sur-reply 1–3.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that the combined disclosures in Stone and the Guidance teach limitation 1.3.2. *See* Pet. 76–77; Ex. 1003 ¶¶ 227–230.

(e) Limitation 1.4.1

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

Petitioner contends that the combined disclosures in Stone and the Guidance teach limitation 1.4.1. *See* Pet. 77–80. Specifically, Petitioner asserts that the Guidance discloses “fraud detection analysis” because the Guidance describes “transaction authentication for an electronic transaction including ‘movement of funds’ and ‘bill payment.’” *Id.* at 78 (quoting Ex. 1037, 4, 6). According to Petitioner, “the fraud detection analysis provides a decision regarding whether the electronic transaction is authenticated/authorized.” *Id.*

Additionally, Petitioner asserts that the Guidance discloses “authentication based on ‘geo-location technology’ to ‘limit Internet users by determining where they are.’” Pet. 79 (quoting Ex. 1037, 12). Petitioner also asserts that it “was well-known that geo-location technology captures location data (e.g., IP address and other associated network information) for

determining the physical location of the user.” *Id.* at 79–80 (citing Ex. 1010 ¶ 140).

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1.4.1. *See, e.g.*, Prelim. Resp. 46–54; Prelim. Sur-reply 1–3.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that the combined disclosures in Stone and the Guidance teach limitation 1.4.1. *See* Pet. 77–80; Ex. 1003 ¶¶ 231–235.

(f) Limitation 1.4.2

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

Petitioner contends that the combined disclosures in Stone and the Guidance teach limitation 1.4.2. *See* Pet. 80–81. Specifically, Petitioner asserts that the Guidance “describes that in biometric authentication, face recognition systems use facial images from a camera with ‘tests for liveness, such as blinking eyes.’” *Id.* at 80 (emphasis omitted) (quoting Ex. 1037, 11). According to Petitioner, tests for liveness based on “a plurality of facial images from a camera (still or video camera)” were well known. *Id.*

Additionally, Petitioner asserts that an ordinarily skilled artisan “would have been motivated to apply the face recognition with liveness test in the multifactor real-time authentication as applied in Stone-Guidance because ‘[t]esting for liveness reduces the chance that the person requesting access is using a photograph of an authorized individual.’” Pet. 80–81 (quoting Ex. 1037, 11).

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1.4.2. *See, e.g.*, Prelim. Resp. 46–54; Prelim. Sur-reply 1–3.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that the combined disclosures in Stone and the Guidance teach limitation 1.4.2. *See* Pet. 80–81; Ex. 1003 ¶¶ 236–239.

(g) Preliminary Conclusion About Obviousness/Nonobviousness

As discussed above, Petitioner’s analysis addresses how the combined disclosures in Stone and the Guidance teach claim 1’s subject matter. *See supra* §§ IV.F.2(b)–(f). Additionally, Petitioner provides reasons with rational underpinnings as to why an ordinarily skilled artisan would have been motivated to combine the Guidance’s teachings with Stone’s teachings in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § IV.F.2(a)(iii). Hence, Petitioner demonstrates a reasonable likelihood of proving that claim 1 is unpatentable under § 103(a) as obvious over Stone and the Guidance.

3. INDEPENDENT CLAIMS 6 AND 11

Claim 6 recites a “method” in its preamble and includes limitations similar to claim 1. *Compare* Ex. 1001, 14:2–27 (claim 1), *with id.*

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

Petitioner identifies disclosures in Stone corresponding to claim 6’s preamble and claim 11’s preamble. Pet. 60–62, 83. Additionally, Petitioner contends that the combined disclosures in Stone and the Guidance teach claim 6’s subject matter and claim 11’s subject matter for the reasons that the combined disclosures teach claim 1’s subject matter. *See id.* at 83. Dr. Jones’s testimony supports Petitioner’s contentions. *See* Ex. 1003 ¶¶ 95–107, 164–168, 177–181, 253–259, 264–270.

At this stage of the proceeding, Patent Owner makes no arguments specific to claim 6 or claim 11. *See, e.g.,* Prelim. Resp. 46–54; Prelim. Sur-reply 1–3.

Based on the current record and for (1) the reasons stated by Petitioner and supported by Dr. Jones’s testimony and (2) the reasons discussed above for claim 1, Petitioner establishes sufficiently that the combined disclosures in Stone and the Guidance teach claim 6’s subject matter and claim 11’s subject matter. *See* Pet. 60–62, 83; Ex. 1003 ¶¶ 95–107, 164–168, 177–181, 253–259, 264–270; *supra* §§ IV.F.2(b)–(f). Additionally, as discussed above, Petitioner provides reasons with rational underpinnings as to why an ordinarily skilled artisan would have been motivated to combine the Guidance’s teachings with Stone’s teachings in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § IV.F.2(a)(iii). Hence, Petitioner demonstrates a reasonable likelihood of

proving that claims 6 and 11 are unpatentable under § 103(a) as obvious over Stone and the Guidance.

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

Claims 2–5, 12, and 14–17 depend directly or indirectly from claim 1. Ex. 1001, 14:28–38, 15:32–35, 16:1–15. Claims 7–10, 18, and 20–23 depend directly or indirectly from claim 6. *Id.* at 14:62–15:5, 16:16–19, 16:24–38.

For claims 2–5, 7–10, 12, 14–18, and 20–23, Petitioner provides an analysis supported by Dr. Jones’s testimony about how the combined disclosures in Stone and the Guidance teach the claimed subject matter. *See* Pet. 81–86; Ex. 1003 ¶¶ 147–154, 241–252, 260–263, 271–286.

At this stage of the proceeding, Patent Owner makes no arguments specific to any of claims 2–5, 7–10, 12, 14–18, and 20–23. *See, e.g.*, Prelim. Resp. 46–54; Prelim. Sur-reply 1–3.

Based on the current record and for (1) the reasons stated by Petitioner and supported by Dr. Jones’s testimony and (2) the reasons discussed above for claims 1 and 6, Petitioner establishes sufficiently that the combined disclosures in Stone and the Guidance teach the subject matter in claims 2–5, 7–10, 12, 14–18, and 20–23. *See* Pet. 81–86; Ex. 1003 ¶¶ 147–154, 241–252, 260–263, 271–286; *supra* §§ IV.F.2–IV.F.3. Hence, Petitioner demonstrates a reasonable likelihood of proving that claims 2–5, 7–10, 12, 14–18, and 20–23 are unpatentable under § 103(a) as obvious over Stone and the Guidance.

*G. Alleged Obviousness over Stone, the Guidance,
and Campbell: Claims 15–17 and 21–23*

Petitioner contends that claims 15–17 and 21–23 are unpatentable under § 103(a) as obvious over Stone, the Guidance, and Campbell. *See* Pet. 6, 87–91; Prelim. Reply 3–5. Patent Owner disputes Petitioner’s contentions. *See* Prelim. Resp. 46–54; Prelim. Sur-reply 1–3.

Specifically, Petitioner asserts that Campbell teaches the limitations in claims 15–17 and 21–23 for the reasons discussed above for the Stone-Hoyos-Varghese-Campbell challenge. Pet. 88–91; *see supra* § IV.E.2. Additionally, Petitioner asserts that an ordinarily skilled artisan would have been motivated to combine Campbell’s teachings with the teachings Stone and the Guidance for reasons the skilled artisan would have been motivated to combine Campbell’s teachings with the teachings of Stone, Hoyos, and Varghese, e.g., to “achieve better performance for reducing fraudulent transactions.” Pet. 87–88.

Dr. Jones’s testimony supports Petitioner’s positions. *See* Ex. 1003 ¶¶ 287–306.

At this stage of the proceeding, Patent Owner makes no arguments specific to any of claims 15–17 and 21–23 and no arguments against combining Campbell’s teachings with the teachings of Stone and the Guidance. *See, e.g.*, Prelim. Resp. 29–54; Prelim. Sur-reply 1–3.

Based on the current record and for the reasons stated by Petitioner and supported by Dr. Jones’s testimony, Petitioner establishes sufficiently that Campbell teaches the limitations in claims 15–17 and 21–23. *See* Pet. 88–91; Ex. 1003 ¶¶ 293–306. Further, based on the current record, Petitioner establishes sufficiently that an ordinarily skilled artisan would

have had a reason to combine Campbell’s teachings with the teachings of Stone and the Guidance, e.g., to “achieve better performance for reducing fraudulent transactions.” *See* Pet. 87–88; Ex. 1003 ¶¶ 288, 290–292. Hence, Petitioner demonstrates a reasonable likelihood of proving that claims 15–17 and 21–23 are unpatentable under § 103(a) as obvious over Stone, the Guidance, and Campbell.

V. CONCLUSION

Based on the arguments and evidence presented by the parties, we determine that there is a reasonable likelihood Petitioner would prevail with respect to at least one claim challenged in the Petition. Hence, we institute an *inter partes* review of all challenged claims on all challenges included in the Petition. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1355 (2018) (noting that the language of 35 U.S.C. § 314(b) “indicates a binary choice—either institute review or don’t”); *PGS Geophysical AS v. Iancu*, 891 F.3d 1354, 1360 (Fed. Cir. 2018) (interpreting the statute as requiring “a simple yes-or-no institution choice respecting a petition, embracing all challenges included in the petition”); 37 C.F.R. § 42.108(a). Additionally, we decline to exercise our discretion under § 314(a) to deny institution.

At this preliminary stage, we have not made a final determination about the patentability of any challenged claim, the construction of any claim term, phrase, or limitation, or any other legal or factual issue.

VI. ORDER

Accordingly, it is

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1–12, 14–18, and 20–23 in the ’886 patent is instituted on all challenges included in the Petition; and

IPR2024-00331
Patent 11,526,886 B1

FURTHER ORDERED that, according to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial that commences on the entry date of this decision.

IPR2024-00331
Patent 11,526,886 B1

For PETITIONER:

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

For PATENT OWNER:

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