

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner.

IPR2024-00330
Patent 10,713,656 B1

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

PESLAK, *Administrative Patent Judge*.

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

I. INTRODUCTION

Apple Inc. (“Petitioner”) filed a Petition pursuant to 35 U.S.C. §§ 311–319 requesting an *inter partes* review of claims 1–19 (“the challenged claims”) of U.S. Patent No. 10,713,656 B1 (“the ’656 patent,” Ex. 1001). Paper 2. Petitioner filed a Declaration of Dr. Creed Jones in support of the Petition. Ex. 1003. Carbyne Biometrics, LLC (“Patent Owner”) filed a Preliminary Response. Paper 7 (“Prelim. Resp.”). With our authorization, Petitioner also filed a stipulation concerning parallel district court litigation on April 29, 2024. Ex. 1048. Petitioner filed an authorized Preliminary Reply. Paper 8 (“Prelim. Reply”). Patent Owner filed an authorized Preliminary Sur-reply. Paper 9 (“Prelim. Sur-reply”).

We have authority, acting on the designation of the Director, to determine whether to institute an *inter partes* review under 35 U.S.C. § 314(a). *See* 37 C.F.R. § 42.4(a) (2024) (“The Board institutes the trial on behalf of the Director.”). Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted unless the information presented in the Petition shows “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.”

Considering the Petition, the Preliminary Response, the Preliminary Reply, and the Preliminary Sur-reply as well as all supporting evidence, we conclude that the information presented in the Petition establishes a reasonable likelihood that Petitioner would prevail in its challenge of at least one claim of the ’656 patent as unpatentable. Pursuant to 35 U.S.C. § 314, we hereby institute an *inter partes* review of all challenged claims of the ’656 patent on all grounds stated in the Petition.

Our factual findings, claim construction, and legal conclusions at this stage of the proceeding are based on the evidentiary record developed thus far. This decision to institute trial is not a final decision as to the unpatentability of the claims for which *inter partes* review is instituted. Our final decision will be based on the full record developed during trial.

A. Related Matters

The parties identify the following proceeding as a related matter: *Carbyne Biometrics, LLC v. Apple Inc.*, 1:23-cv-00324 (W.D. Tex.) (“Parallel District Court Proceeding”). Pet. 1; Paper 4, 2.

B. Real Parties in Interest

Petitioner and Patent Owner each identifies itself and no others as a real party in interest. Pet. 1; Paper 3, 2.

C. The '656 Patent

The '656 patent is titled “Method, Medium, and System for Reducing Fraud.” Ex. 1001, code (54). The '656 patent issued on July 14, 2020, from Application No. 15/948,744, which was filed on April 9, 2018. *Id.* at codes (45), (21), (22). Application No. 15/948,744 claims priority through a continuation application to Application No. 13/099,981, filed May 3, 2011, and also claims priority to Provisional Application No. 61/332,140, filed May 6, 2010. *Id.* at codes (63), (60).

As background, the '656 patent notes that fraud can be “perpetrated in the context of electronic transactions” and explains that “[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.” Ex. 1001, 1:26–30. The '656 patent states that “[i]mproved

techniques to prevent fraud” and “to identify those who commit fraud would . . . be useful.” *Id.* at 1:30–32.

Figure 4 of the '656 patent is reproduced below.

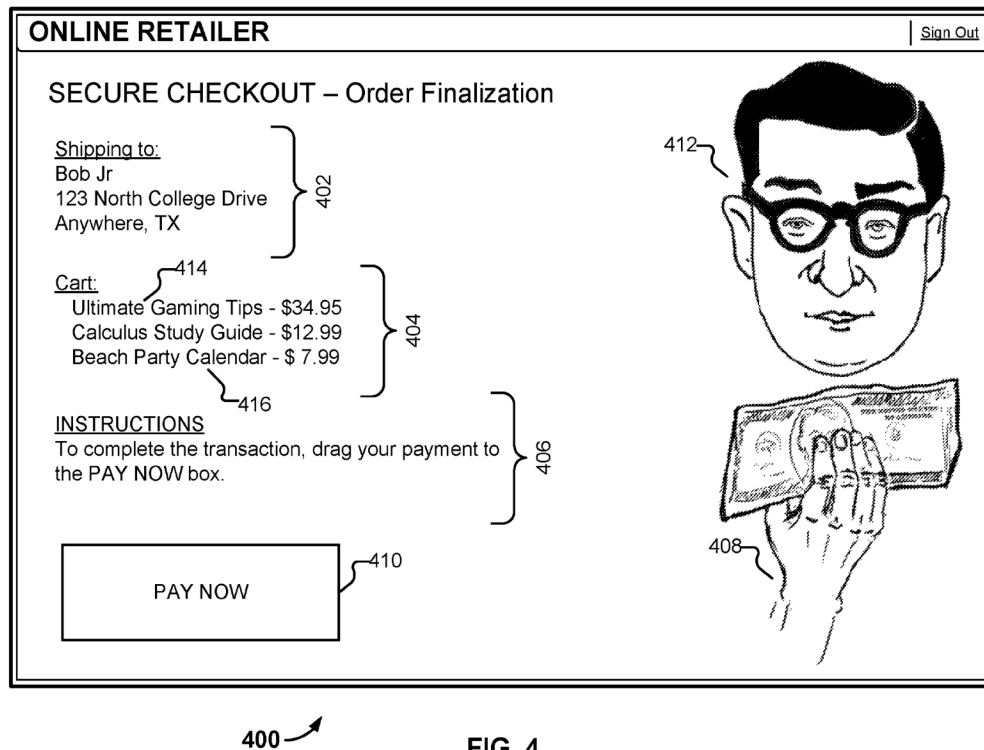


Figure 4 “illustrates an embodiment of an interface,” which is “rendered in a browser application of a personal computer, that would be shown to [a user] during a checkout process.” Ex. 1001, 6:24–27. According to the '656 patent, “in order to pay, [the user] must click on hand 408 and drag it to region 410 of the interface,” or take other actions, “such as by swiping hand 408 with a finger to drag it to region 410, or speaking ‘pay now’ or ‘I agree to pay’ into a microphone.” *Id.* at 6:35–41. The '656 patent explains that

if the user speaks “pay now,” the user’s voice can be recorded and used for audit purposes If the 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.

Id. at 6:42–49. “Also included in interface 400 is an image of [the account holder]’s face 412.” *Id.* at 6:52–53; *see also id.* at 5:27–56.

Figure 7 of the ’656 patent is reproduced below.

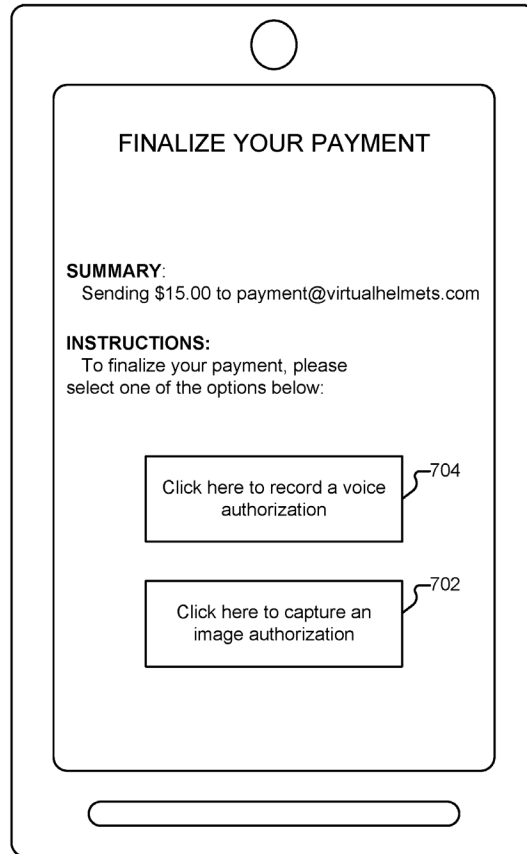


FIG. 7

Figure 7 “illustrates an embodiment of an interface.” Ex. 1001, 8:51. The ’656 patent describes that “to complete a transaction for digital goods (e.g., with social network game developer 120), the purchaser is given a choice of either providing an audio sample (by selecting box 704), or providing a photograph (by selecting box 702).” *Id.* at 8:53–57. “If the purchaser selects box 702, the purchaser will be asked to photograph himself or otherwise provide a form of photographic authorization.” *Id.* at 8:57–59. According to the ’656 patent, “[i]n some embodiments, an analysis of the

photograph is performed as part of the transaction” to confirm “that the object being photographed is alive,” or to require “that a face be detected in the captured image or that a certain amount of flesh tone be present in the picture.” *Id.* at 8:60–9:2.

D. Illustrative Claim

Claims 1, 10, and 19 are independent claims. Claim 1 is representative of the claimed subject matter and is reproduced below:

1. A system, comprising:

a processor configured to:

receive biometric information associated with an account holder;

store, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder;

render, in one or more interfaces, a virtual likeness of a face of a recipient of an electronic transaction;

render, in the one or more interfaces, a transaction icon associated with the electronic transaction;

receive an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the one or more interfaces;

subsequent to receiving the indication of the action taken by the user, capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information and location data associated with the user;

perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises:

performing a comparison based at least in part on the stored biometric information and the captured biometric information; and

determining, based at least in part on the captured biometric information, that the user is alive; and

based at least in part on both the user interaction with the transaction icon rendered in the interface and performing the fraud detection analysis, complete the electronic transaction; and

a memory coupled to the processor and configured to provide the processor with instructions.

Ex. 1001, 13:64–14:31.

E. Prior Art and Asserted Grounds

Petitioner asserts that claims 1–19 would have been unpatentable on the following grounds (Pet. 6):

Claim(s) Challenged	35 U.S.C. §	References/Basis
1, 4–10, and 13–19	103(a) ¹	Stone, ² Hoyos, ³ Varghese ⁴
1, 4–10, and 13–19	103(a)	Stone, FFIEC Guidance ⁵
2, 3, 11, and 12	103(a)	Stone, Hoyos, Varghese, Borovsky ⁶
2, 3, 11, and 12	103(a)	Stone, FFIEC Guidance, Borovsky

¹ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112–29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. § 103. Because the ’656 patent claims priority to an application filed before March 16, 2013 (the effective date of the amendments), the pre-AIA version of § 103 applies.

² U.S. Patent Application Publication No. US 2010/0042535 A1 (published February 18, 2010) (Ex. 1008, “Stone”).

³ U.S. Patent Application Publication No. US 2010/0014720 A1 (published January 21, 2010) (Ex. 1013, “Hoyos”).

⁴ U.S. Patent Application Publication No. US 2006/0282660 A1 (published December 14, 2006) (Ex. 1010, “Varghese”).

⁵ Federal Financial Institutions Examination Council, *Authentication in an Internet Banking Environment*, https://www.ffiec.gov/pdf/authentication_guidance.pdf (released October 12, 2005) (Ex. 1037, “FFIEC Guidance” or “Guidance”; *see also* Ex. 1040).

⁶ U.S. Patent Application Publication No. US 2010/0317335 A1 (published December 16, 2010) (Ex. 1041, “Borovsky”).

II. ANALYSIS

A. Discretionary Denial of Institution Under 35 U.S.C. § 314(a)

Patent Owner contends that we should exercise our discretion to deny institution under 35 U.S.C. § 314(a) and *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential). Prelim. Resp. 17–28. Patent Owner analyzes the factors set forth in *Fintiv* in light of the Parallel District Court Proceeding. *Id.* at 20–28.

Petitioner contends that we should not exercise our discretion to deny institution under 35 U.S.C. § 314(a) and provides its analysis of the *Fintiv* factors. Pet. 82–84. In the Petition, Petitioner stipulates that if we institute trial, “it will not pursue the same grounds raised in this Petition in the Parallel District Court Litigation.” *Id.* at 83–84 (citing *Sand Revolution II, LLC v. Cont’l Intermodal Grp.–Trucking LLC*, IPR2019-01393, Paper 24 at 7 (PTAB June 16, 2020)). Subsequently, as noted above, we authorized Petitioner to file a stipulation. See Ex. 1048. Petitioner’s stipulation provides that if we institute trial in this case, Petitioner “(i) will not pursue the grounds [raised in this proceeding] in the Parallel District Court Litigation and (ii) will not pursue any other ground that reasonably could have been raised during the IPR (should it be instituted) in the Parallel District Court Litigation.” *Id.* at 1.

Patent Owner counters that “Petitioner is using its late ‘stipulation’ to game the *Fintiv* process and get two bites at the invalidity apple.” Prelim. Resp. 27. Patent Owner contends that “Petitioner’s stipulation does not in fact guarantee the reduction of *any* duplicate effort,” and asserts that “Petitioner has already positioned itself to combine the petitioned art with art that Petitioner will argue it ‘could **not** have reasonably been raised’ in the

IPR petitions, such as system art, in the district court in order to avoid the consequences of its stipulation.” *Id.* at 26.

Analysis

The Director of the USPTO has proscribed an interim procedure for discretionary denials in AIA post-grant proceedings with parallel district court litigation. *See* Ex. 1025, Memorandum to Members of the PTAB from Director Vidal, dated June 21, 2022 (“Memorandum”). In the Memorandum, the Director states that “[w]hen a petitioner stipulates not to pursue in a parallel district court proceeding the same grounds as in the petition or any grounds that could have reasonably been raised in the petition, it mitigates concerns of potentially conflicting decisions and duplicative efforts between district court and the PTAB.” *Id.* at 7. Further, when such a stipulation is provided, “the grounds the PTAB resolves will differ from those present in the parallel district court litigation” and “the PTAB will not discretionarily deny institution of an IPR.” *Id.*

In this case, Petitioner provides a stipulation that falls within the contours of the Memorandum. Ex. 1048, 1. Petitioner’s stipulation meets the requirements of a stipulation pursuant to *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 at 18–19 (PTAB Dec. 1, 2020) (precedential as to § II.A), and, therefore, the Director’s Memorandum governs our determination here.

For the foregoing reasons, in accordance with the Director’s Memorandum, we do not exercise our discretion to deny institution under 35 U.S.C. § 314(a) due to the parallel district court litigation.

B. Overview

A claim is unpatentable under § 103(a) if the differences between the claimed subject matter 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. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when in evidence, objective indicia of non-obviousness (i.e., secondary considerations).⁷ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

The Supreme Court explained in *KSR International Co. v. Teleflex Inc.* that

[o]ften, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.

550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)) (“[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” (alteration in original)).

⁷ No evidence of secondary considerations has been presented at this stage of the proceeding.

“Whether an ordinarily skilled artisan would have been motivated to modify the teachings of a reference is a question of fact.” *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1327 (Fed. Cir. 2016) (citations omitted).

“[W]here a party argues a skilled artisan would have been motivated to combine references, it must show the artisan ‘would have had a reasonable expectation of success from doing so.’” *Arctic Cat Inc. v. Bombardier Recreational Prods. Inc.*, 876 F.3d 1350, 1360–61 (Fed. Cir. 2017) (quoting *In re Cyclobenzaprine Hydrochloride Extended-Release Capsule Patent Litig.*, 676 F.3d 1063, 1068–69 (Fed. Cir. 2012)).

C. Level of Ordinary Skill in the Art

Petitioner contends that “a Person of Ordinary Skill in the Art (“POSITA”) at the time of the claimed 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 (citing Ex. 1003 ¶ 21). Petitioner further states 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 POSITA.” *Id.* at 4–5 (citing Ex. 1003 ¶ 21).

Patent Owner, at this stage of the proceeding, does not dispute Petitioner’s definition of the person of ordinary skill in the art. Prelim. Resp. 13–14.

For the purposes of this Decision, we apply Petitioner’s proffered level of skill in the art, with the exception of the phrase “at least” which

injects potential ambiguity into the level of skill, because its proffered level of skill appears consistent with the problems addressed in the '656 patent and the prior art.

D. Claim Construction

We apply the same claim construction standard used by Article III federal courts and the International Trade Commission, both of which follow *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc), and its progeny. 37 C.F.R. § 42.100(b). Accordingly, we construe each challenged claim of the '656 patent to generally be “the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” *Id.*

If the specification “reveal[s] a special definition given to a claim term by the patentee that differs from the meaning it would otherwise possess[,] . . . the inventor’s lexicography governs.” *Phillips*, 415 F.3d at 1316 (citing *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002)). Another exception to the general rule that claims are given their ordinary and customary meaning is “when the patentee disavows the full scope of a claim term either in the specification or during prosecution.” *Uship Intellectual Props., LLC v. United States*, 714 F.3d 1311, 1313 (Fed. Cir. 2013) (quoting *Thorner v. Sony Comput. Ent. Am., LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012)).

Petitioner asserts that “for the purposes of this proceeding and the analysis presented herein, no claim term requires express construction” and states that the petition “analyzes the claims consistent with ordinary and customary meaning as would be understood by POSITA in light of the specification.” Pet. 5 (citing *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*,

200 F.3d 795, 803 (Fed. Cir. 1999); *Phillips*, 415 F.3d at 1314–17; Ex. 1003 ¶¶ 35–36).

Patent Owner “accepts Petitioner’s position that none of the claim terms of the ’656 Patent requires construction,” while noting that “in the parallel district court case, Petitioner sought construction of multiple claim terms for the ’656 Patent.” Prelim. Resp. 13 (citing Pet. 5; Ex. 2010).

We determine that no express construction of any claim term is necessary for purposes of this Decision. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.’”) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

The parties are free to address claim construction in subsequent briefing during trial.

E. Ground 1: Alleged Obviousness of Claims 1, 4–10, and 13–19 over Stone, Hoyos, and Varghese

Petitioner contends claims 1, 4–10, and 13–19 would have been obvious over Stone, Hoyos, and Varghese. Pet. 13–61. Petitioner supports its contentions with the Declaration of Dr. Jones. Ex. 1003. Patent Owner disputes Petitioner’s contentions. Prelim. Resp. 28–50.

We begin with brief summaries of Stone, Hoyos, and Varghese, and then address the parties’ respective contentions.

1. Stone (Ex. 1008)

Stone is titled “Currency Display.” Ex. 1008, code (54). Stone relates to “electronic visual displays” that “show a visual representation of financial instruments.” *Id.* ¶ 2. Stone states that its disclosed embodiments “enable

users to see a selected actual currency representing the amount entered by the user into a device with a display screen.” *Id.* ¶ 16.

For example, 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. 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. According to Stone, “[w]hen the currency representation is shown, the user can send the entered amount to another user through the network.” *Id.* ¶ 17.

Figure 2 of Stone is reproduced below.

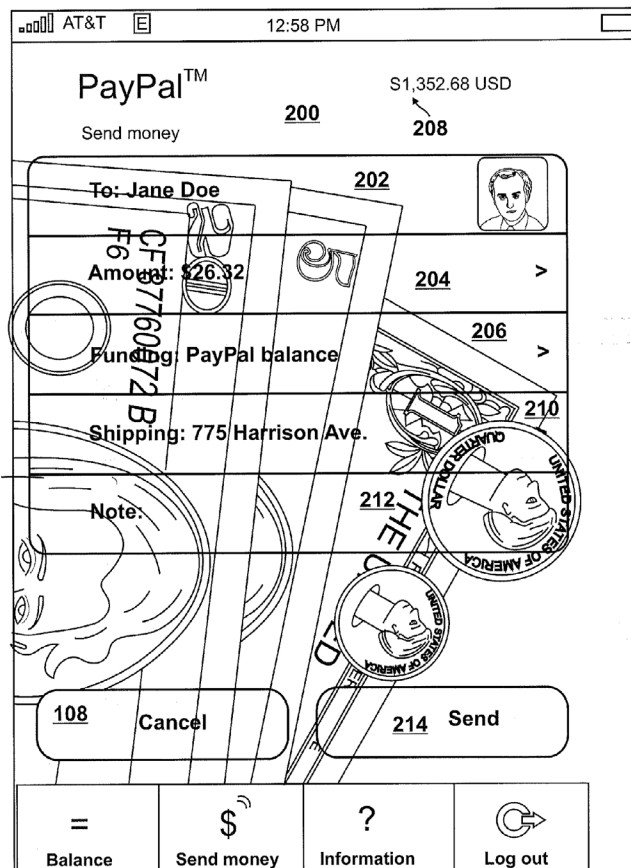


FIG. 2

Figure 2 “shows a currency display on a user device.” Ex. 1008 ¶ 11.

According to Stone,

display 200 has a name box 202 indicating the recipient of funds as well as a picture of the recipient, a funds box 204 indicating the amount of funds to be transferred, a note box 212 for the user to type in any notes to the recipient, cancel button 108, and a send button 214 to transfer the funds [as] in noted in box 204. Display 200 has additional information, such as a funding source box 206, indicating the source or account where the user’s funds will be transferred from, a balance area 208, indicating the current balance of the funding account, and an address box 210, indicating the address of the recipient.

Id. ¶ 24. Stone describes that “the actual currency representation is . . . present in the background.” *Id.*

2. Hoyos (Ex. 1013)

Hoyos is titled “Fraud Resistant Biometric Financial Transaction System and Method.” Ex. 1013, code (54). Hoyos states that “[o]ne problem faced by biometric recognition systems involves the possibility of spoofing,” such as “a life-sized, high-resolution photograph of a person . . . presented to an iris recognition system.” *Id.* ¶ 11. Hoyos is directed to a “method and system for authenticating financial transactions” wherein “biometric data is acquired from a person and the probability of liveness of the person and probability of a match between the person or token and known biometric or token information are calculated, preferably according to a formula $D=P(p)*(K+P(m))$, wherein K is a number between 0.1 and 100, and authenticating if the value of D exceeds a predetermined value.” *Id.* at code (57); *see also id.* ¶ 17.

Figure 1 of Hoyos is reproduced below.

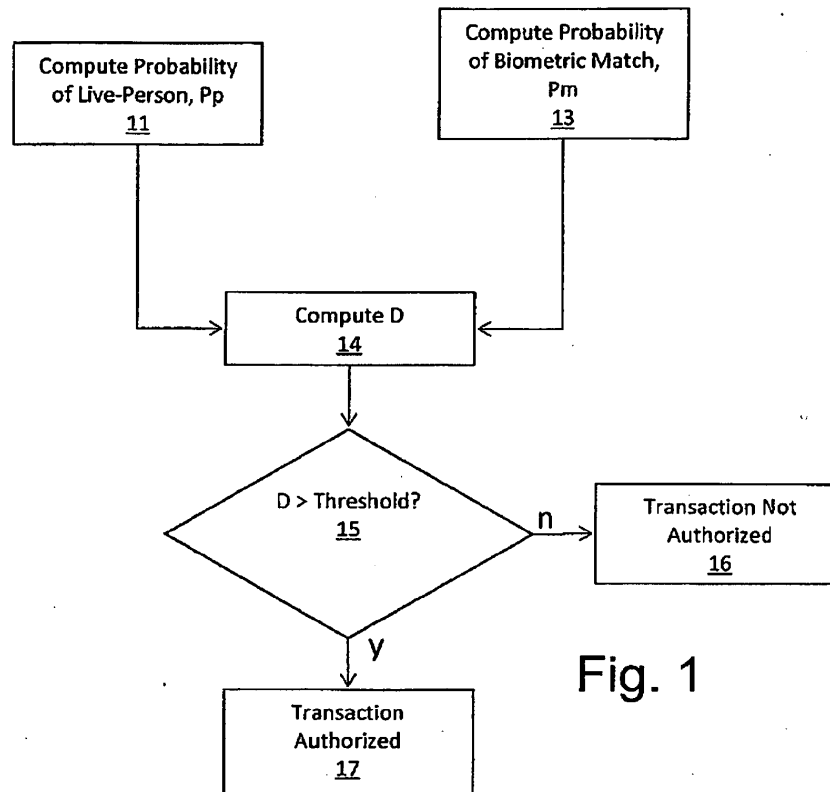


Fig. 1

Figure 1 is “a flow chart of an authentication system according to the invention.” Ex. 1013 ¶ 32. Hoyos explains:

the overall process is to compute 11 the probability, P_p , of a live person being presented, compute [at block] 13 the probability of a biometric match, P_m , computing [at block] 14 D according to the aforementioned formula, wherein at decision block 15 if D exceeds a preset threshold, the transaction is authorized [at block] 17 or, if D does not exceed the preset threshold, the transaction is not authorized, [at block] 16.

Id. ¶ 33. Hoyos also explains that since “[t]he invention authorizes transactions based on a combination of the two probabilities, 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.” *Id.* ¶ 27.

3. Varghese (Ex. 1010)

Varghese is titled “System and Method for Fraud Monitoring, Detection, and Tiered User Authentication.” Ex. 1010, code (54). Varghese is directed to “systems and methods for authenticating access requests from user devices by presenting one of a plurality of graphical user interfaces selected depending on a perceived risk of fraud associated with the devices.” *Id.* at code (57). Varghese states that “[t]he function of the present invention [is] configured to provide consistent methods of checking the authenticity and security of a user-initiated request made to a service-provider application, e.g., a[n] online store application, an online banking application, and the like.” *Id.* ¶ 88.

Figure 14 of Varghese is reproduced below:

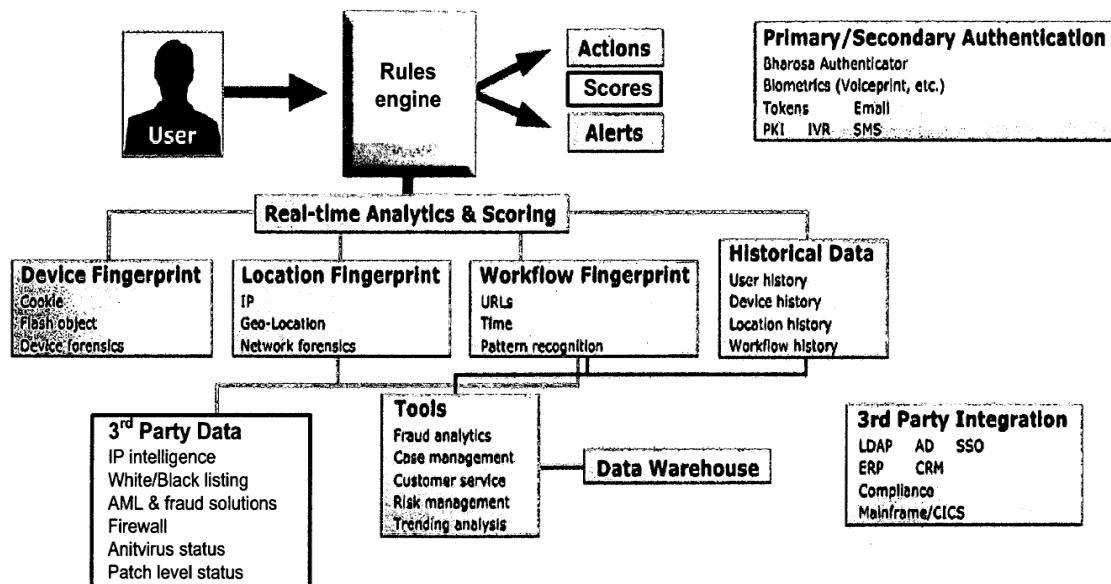


FIG. 14

Figure 14 “illustrates an exemplary functional configuration including the request attributes and criteria.” *Id.* ¶ 91. Varghese defines request attributes and criteria as follows:

Generally, the available, security-relevant information related to a user request (the “request attributes”) is broken into related

information groupings referred to as criteria so that each criteria preferably contains several pieces of data concerning a user request. Groups of rules, preferably criteria-specific, then evaluate the criteria, and the risk scores and actions that are output result from a combination and weighting of the results of the rule-based evaluation of each criteria.

Id. ¶ 89. According to Varghese, as shown in Figure 14,

The request attributes of the criteria are condensed into fingerprints: a location fingerprint, a device fingerprint, a workflow fingerprint, and an historical data fingerprint. The fingerprints are then processed to generate actions, alerts, and scores. Possible actions include primary authentication, which is the process by which the user is identified and authenticated. Primary authentication based primarily on location and device fingerprints and can include presentation of secure logon screens at the user device. Another action is secondary authentication, which can be invoked during a session if authentication confirmation or further authentication is needed. It can include use of, e.g., email, voiceprints, and the like.

Id. ¶ 91. Varghese also explains that “[l]ocation information and device information are important criteria, especially in the pre-authentication period” wherein “[l]ocation information characterizes the location of the device from which a request originates” and “[d]evice information characterizes the originating device itself, such as its hardware and software components.” *Id.* ¶ 93. According to Varghese, “the criteria data, packaged into fingerprints as already described, is processed and scored in real-time by fraud analytics driven by a rules engine.” *Id.* ¶ 97.

4. Claims 1, 10, and 19

Petitioner provides a limitation-by-limitation analysis of independent claims 1, 10, and 19,⁸ mapping the prior art to the claim limitations. Pet.

⁸ For ease of reference, in our analysis, we refer to Petitioner’s claim annotations.

26–52, 58–61. Petitioner also provides contentions concerning motivation to combine disclosures or embodiments of Stone (*id.* at 13–15); Stone and Hoyos (*id.* at 15–21); and Stone, Hoyos, and Varghese (*id.* at 21–26), and reasonable expectation of success in the combination.

Patent Owner does not dispute Petitioner’s mapping of the prior art to the claim limitations. *See generally* Prelim. Resp. Patent Owner contends that Dr. Jones’s testimony concerning motivation to combine and reasonable expectation of success should be given no weight (Prelim. Resp. 30–34); Petitioner’s explanation for motivation to combine Stone, Hoyos, and Varghese is insufficient (*id.* at 34–38); Stone is not analogous art (*id.* at 39–41); and Stone, Hoyos, and Varghese teach away from or conflict with each other (*id.* at 41–50).

With this background, we analyze the parties’ respective contentions.

[1.0]: A system, comprising:

Petitioner contends that “Stone discloses or renders obvious the preamble to the extent that it’s limiting.” Pet. 26 (citing Ex. 1003 ¶¶ 80–82).

Referring to Stone’s Figure 4, Petitioner specifically contends that “Stone describes ‘**a system 400** configured to utilize the currency display over a network 402.’” Pet. 26–27 (quoting Ex. 1008 ¶ 40 (emphasis by Petitioner)). According to Petitioner, Stone’s system 400 comprises user device 404, recipient devices 406, payment provider server 408 that communicates over network 402, and software stored on computer readable storage media. *Id.* (citing Ex. 1008 ¶¶ 40, 41, 44, 46, 54).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficiently discloses the subject matter of the preamble. Therefore, we need not address whether the preamble is limiting.

[1.1]: a processor configured to:

Petitioner contends that Stone alone or the combination of Stone, Hoyos, and Varghese teaches this limitation. Pet. 28 (citing Ex. 1003 ¶¶ 83–89).

Petitioner argues that the '656 patent states that “the term ‘processor’ refers to one of more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.” Pet. 28 (quoting Ex. 1001, 2:14–16).

Petitioner contends that Stone’s Figure 5 illustrates system 500 for implementing embodiments of its invention which “includes a processor (processing component 504).” Pet. 29 (citing Ex. 1008 ¶ 49, Fig. 5). Petitioner further contends that Stone’s system 400 includes “processor 504 in user device 404, alone or in combination with other processors including the processor 504 of other devices . . . configured to process data, such as computer program instructions, for perform[ing] processes for a transaction.” *Id.* at 29–30 (citing Ex. 1008, Fig. 4).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

[1.2]: receive biometric information associated with an account holder; store, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder;

Petitioner contends that Stone alone or the combination of Stone, Hoyos, and Varghese teaches this limitation. Pet. 31 (citing Ex. 1003 ¶¶ 90–95).

Petitioner provides the following annotated version of Stone’s Figure 4 (Pet. 32):

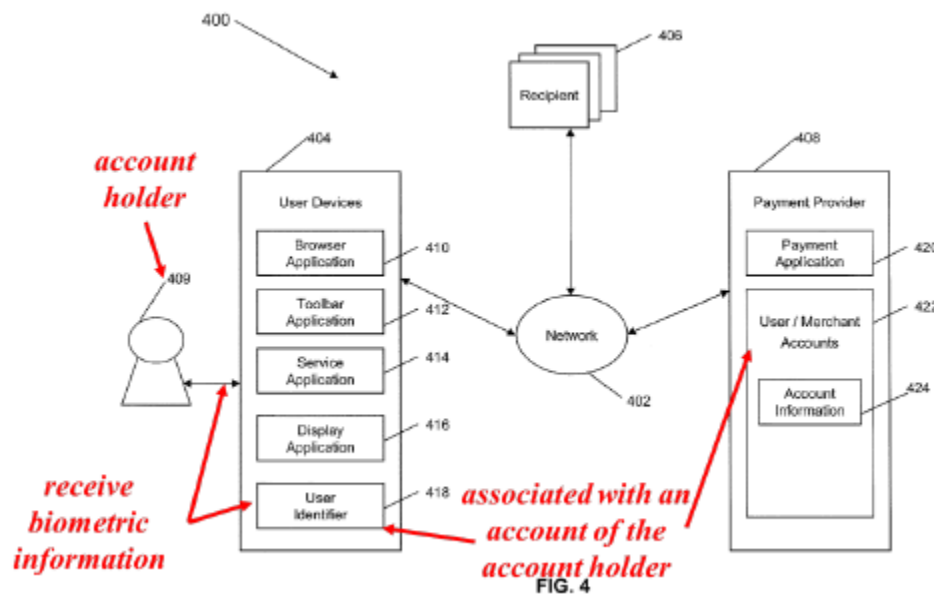


Figure 4 “is a block diagram of a system for using one embodiment” of Stone’s invention. Ex. 1008 ¶ 13. Petitioner annotates Figure 4 with red text stating “account holder” with a red arrow pointing to element 409, red text stating “receive biometric information” with two red arrows pointing to a line between element 409 and user device 404 and to element 418, and red text stating “associated with an account of the account holder” with two red arrows pointing to elements 418 and 422.

Petitioner contends that Stone’s Figure 4 illustrates “receiving from an account holder (user 409), biometric information (to be stored as ‘biometric id’) associated with the account holder (user 409); and storing the biometric information as ‘biometric id’ in a data store (storage component 508) of user device 404” and “the stored ‘biometric id’ is a user attribute of user identifier 418 associated with an account (account 422) of the account holder (user 409).” Pet. 31 (citing Ex. 1008 ¶ 45). According to Petitioner, an ordinarily skilled artisan “would have understood that ‘biometric id’ means

“biometric identification information.”” *Id.* at 32 (citing Ex. 1003 ¶ 91), *see also id.* (arguing “it is basic fundamental knowledge of biometric authentication that Stone’s biometric information/‘biometric id’ is typically received and stored on user device 404 during an enrollment/registration process.” (citing Ex. 1003 ¶ 92)), *id.* at 33 (“Hoyos expressly describes receiving and storing biometric information during enrollment, and the stored biometric information is used for comparison with subsequent captured biometric data during transaction authentication.” (citing Ex. 1003 ¶ 94)).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

[1.3]: render, in one or more interfaces, a virtual likeness of a face of a recipient of an electronic transaction;

Petitioner contends that Stone teaches this claim limitation. Pet. 34 (citing Ex. 1003 ¶¶ 96–99).

Petitioner provides the following annotated version of Stone’s Figure 2 (Pet. 35):

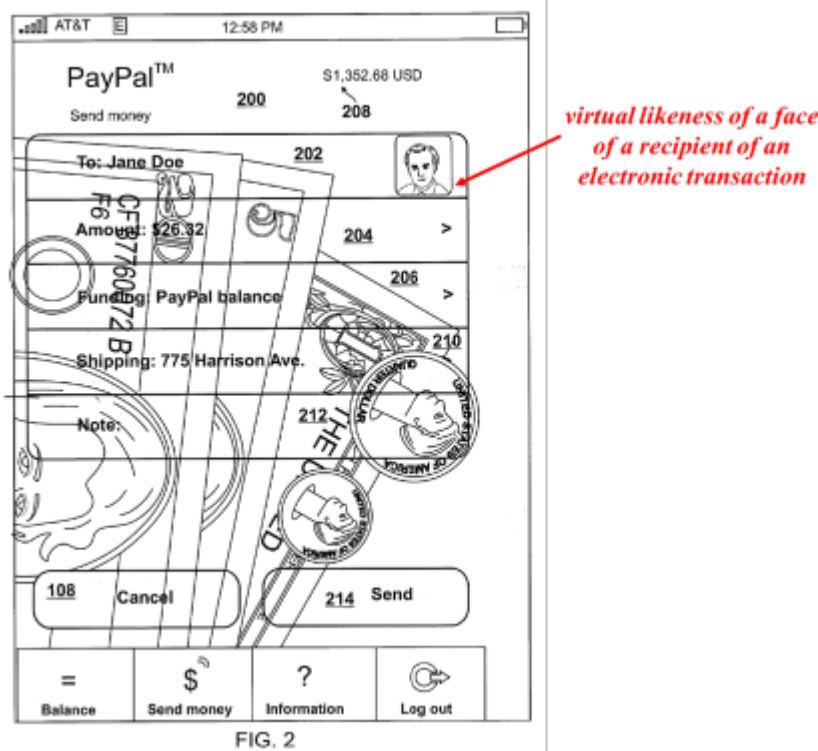


Figure 2 “shows a currency display on a user device.” Ex. 1008 ¶ 11. Petitioner adds red text stating “virtual likeness of a face of a recipient of an electronic transaction” with an arrow pointing to an image of a face shown in element 202. Pet. 35.

Petitioner contends that Stone discloses “the processor configured to *render in one or more interfaces* (e.g. interface 200 of FIG. 2), *a virtual likeness of a face* (e.g., recipient icon including ‘a picture of the recipient’) *of a recipient of an electronic transaction* (e.g., picture of recipient next to the name box 202 of FIG. 2).” Pet. 34 (citing Ex. 1003 ¶ 97; Ex. 1008 ¶¶ 20, 24, 36, Fig. 2). According to Petitioner, Stone’s recipient icon “teaches using a photograph of the recipient for display, because photographs for recipient icon are quick and easy for users to take and upload . . . and because photographs may increase[] transaction confidence.” *Id.* (citing Ex. 1003 ¶ 98).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

[1.4]: render, in the one or more interfaces, a transaction icon associated with the electronic transaction;

Petitioner contends that Stone teaches this limitation. Pet. 35 (citing Ex. 1003 ¶¶ 100–103).

Petitioner provides an annotated side-by-side reproduction of Stone’s Figures 2 and 3. Pet. 36. Petitioner contends that each of the following “control elements/blocks” shown therein, i.e., “\$Send money,” 202, 206, 214, personalized currency, 300, 302, 306, 312, 314, 316, correspond to the recited transaction icon “because it was well-known to implement each of these annotated items using a transaction icon in the interfaces to provide a visual indicator for various user interactions to initiate, continue, and/or confirm the transaction request associated with the electronic transaction.” *Id.* at 35–36 (citing Ex. 1003 ¶ 101). Petitioner alternately contends that even if any of those items are not transaction icons, an ordinarily skilled artisan “would have been motivated to implement the control items using a transaction icon, because icon and button are alternative design choices for control elements, and using transaction icons provides ‘a more visually rich interface.’” *Id.* at 36 (citing Ex. 1003 ¶ 102; Ex. 1008 ¶¶ 4, 16).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

[1.5]: receive an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the one or more interfaces;

Petitioner contends that Stone teaches this limitation. Pet. 37 (citing Ex. 1003 ¶¶ 104–109).

Referring to the elements Petitioner contends correspond to the recited transaction icons in limitation 1.4, Petitioner contends that Stone’s “processor is configured to receive an indication of an action taken by a user, the action comprising a user interaction with each of” the identified transaction icons. *Id.* (citing Ex. 1003 ¶ 106). Petitioner specifically contends that “in response to a user interaction with (e.g., clicking/tapping on) the ‘\$Send Money’ icon, the processor receives an indication of user action for initiating a send money transaction request, and in response, a corresponding interface 200 for a send money transaction is displayed.” *Id.* at 38 (citing Ex. 1003 ¶ 107).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

[1.6]: subsequent to receiving the indication of the action taken by the user, capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information and location data associated with the user;

Petitioner contends that the combination of Stone, Hoyos, and Varghese teaches this limitation. Pet. 39 (citing Ex. 1003 ¶¶ 111–122).

Petitioner provides the following annotated version of Varghese’s Figure 14 (Pet. 40):

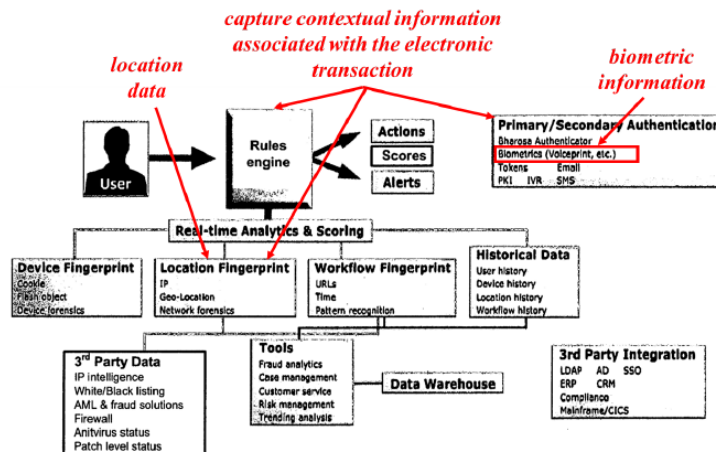


FIG. 14

Figure 14 is a block diagram illustrating “a preferred function configuration of [Varghese’s] invention.” Ex. 1010 ¶ 14. Petitioner annotates Figure 14 with red text stating “location data” and a red arrow pointing to the block titled “Location Fingerprint,” red text stating “capture contextual information associated with the electronic transaction” with three red arrows pointing to the blocks titled “Location Fingerprint,” “Rules Engine,” and “Primary/Secondary Authentication”, and red text stating “biometric information” with a red arrow pointing to text stating “Biometrics (Voiceprint, etc.)” inside the block titled “Primary/Secondary Authentication.” Pet. 40.

Referring to Varghese’s Figure 14, Petitioner contends that “Varghese describes real-time risk-based contextual authentication, including capturing real-time contextual information (e.g., ‘biometrics’ and ‘location data’ associated with the user), after the user submits its transaction request.” Pet. 39 (citing Ex. 1003 ¶ 112). Petitioner next contends that Varghese discloses capturing a user IP address “and determining the physical location using a ‘geolocation service’ based on the user IP address.” *Id.* at 39–40 (citing Ex. 1013 ¶ 140). Petitioner argues that an ordinarily skilled artisan would have used any suitable geolocation technique well-known in the art “to capture location data, e.g., capturing a GPS data.” *Id.* at 40 (citing Ex. 1008 ¶ 26; Ex. 1016 ¶ 14).

Petitioner next contends that Varghese teaches “‘post-authentication’ real-time risk-based contextual authentication, where real-time contextual information (e.g., ‘biometrics’ and ‘location’ data associated with the user) are captured after the user submits its transaction request and used for real-time risk analysis for risk-based authentication.” Pet. 40 (citing Ex. 1003

¶ 113; Ex. 1010, ¶¶ 97–99, 109, Fig. 14). According to Petitioner, the captured location data “is contextual information for the transaction” because it is “a user location from which the transaction request originates.” *Id.* at 41 (citing Ex. 1003 ¶ 115; Ex. 1010 ¶¶ 81, 140, 142, claim 31).

Petitioner next contends that Hoyos discloses “capturing biometric contextual information (e.g., ‘**acquiring biometric data from a person**’ including images, palm temperature, etc.) used for fraud detection based thereupon.” Pet. 41–42 (citing Ex. 1003 ¶ 116; Ex. 1013 ¶ 17, Fig. 1). Petitioner further contends that the biometric information captured in Hoyos includes “a set of user facial images . . . captured using a camera,” in addition to “finger or palm temperature,” “iris recognition,” and “fingerprint image recognition, finger vein image recognition, or palm vein recognition.” *Id.* at 42 (citing Ex. 1003 ¶ 117; Ex. 1013 ¶¶ 3, 12, 18–22, 40).

Petitioner contends that an ordinarily skilled artisan would have implemented a combination of Stone, Hoyos, and Varghese as shown in the following annotated side-by-side image of Stone’s Figures 2 and 3 (Pet. 44 (citing Ex. 1003 ¶ 119)):

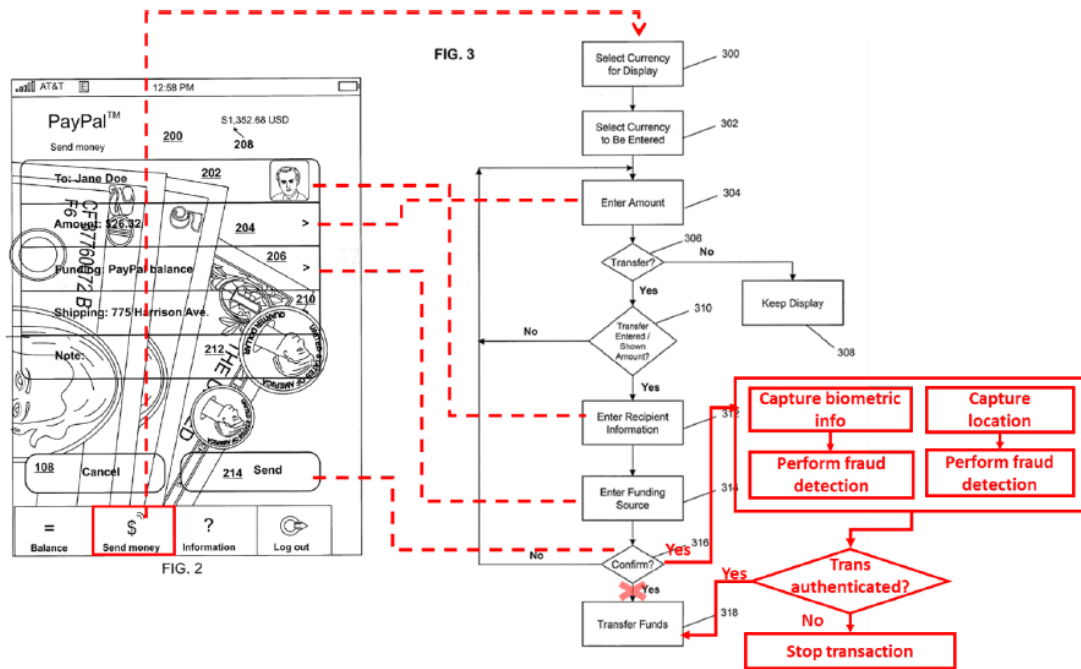


Figure 2, on the left, is “a currency display on a user device” of Stone and Figure 3, on the right, “is a flow chart.” Ex. 1008 ¶¶ 11, 12. Petitioner annotates the figures with broken red lines between the “\$Send Money” icon in Figure 2 and block 300 in Figure 3, between the image of the recipient in Figure 2 and block 312 in Figure 3, between element 204 in Figure 2 and block 304 in Figure 3, and between element 206 in Figure 2 and block 314 in Figure 3. Pet. 44. Petitioner also annotates in red proposed additional steps, based on Varghese’s disclosure of location analysis and Hoyos’s disclosure of biometric authentication analysis, to be performed between blocks 316 and 318 in Stone’s Figure 3. *Id.*

Referring to the annotated drawing, Petitioner contends that an ordinarily skilled artisan “would have been motivated to apply multifactor real-time contextual based authentication including location authentication taught by Varghese and biometric authentication taught by Hoyos in . . . Stone for fraud detection which is performed **subsequent to** user transaction

confirmation . . . for improved security.” Pet. 43–44, 45 (arguing that performing multifactor authentication at the point shown in the annotated drawing provides “the benefits of risk-based contextual authentication adaptive for the specific transaction based on transaction information, more accurate real-time information for real time authentication, and performing fraud analysis based on locations captured before and after transaction request for improved security.” (citing Ex. 1003 ¶ 120; Ex. 1010, ¶¶ 91, 97–99, 148, Fig. 14, Table 10; Ex. 1013 ¶ 28; Ex. 1015, Fig. 4; Ex. 1016 ¶¶ 36, 43, 73, Fig. 3; Ex. 1035, 4:60–62, 4:66–67)).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

[1.7.1]: perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises:

Petitioner contends that the combination of Stone, Hoyos, and Varghese teaches this limitation. Pet. 45 (citing Ex. 1003 ¶¶ 123–125).

Referring to the annotated drawing reproduced above in our analysis of limitation 1.6, Petitioner contends that the “analysis based on the captured biometrics [taught by Hoyos] and location data [taught by Varghese] . . . is performed for fraud detection analysis, after the user confirms the transaction request at 214/316 and after contextual biometrics and location data associated with the transaction request and user are captured.” *Id.* at 45–46 (citing Ex. 1003 ¶¶ 124–125).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

[1.7.2]: performing a comparison based at least in part on the stored biometric information and the captured biometric information; and

Petitioner contends that the combination of Stone, Hoyos, and Varghese teaches this limitation. Pet. 46 (citing Ex. 1003 ¶¶ 126–131).

Petitioner first contends that “it was fundamental knowledge that biometric authentication,” such as in the proposed combination, “performs a comparison based at least in part on the stored biometric information (obtained and stored during its enrollment stage) and the captured biometric information . . . as discussed” in connection with limitation 1.2. Pet. 47 (citing Ex. 1003 ¶ 127; Ex. 1014 ¶ 9; Ex. 1021, Abst.; Ex. 1023, 8:3–9:39; Ex. 1013 ¶ 3; Ex. 1024, 3:6–11; Ex. 1033, Fig. 3; Ex. 1037, 9-10).

Petitioner next contends that “Hoyos’ biometric authentication, as applied in the combination performs a comparison (block 13 of FIG. 1) based at least in part on the stored biometric information and the captured biometric information.” Pet. 47 (citing Ex. 1003 ¶¶ 128–129). Petitioner additionally contends that in addition to Hoyos’s biometric authentication based on combining comparison and liveness analysis, for higher risk transactions, an ordinarily skilled artisan “would have been motivated to apply additional biometric authentication including voice authentication (e.g., for transaction requests requiring higher-level security) as taught by Varghese, which similarly teaches comparison of live capture with previously stored voice samples.” *Id.* at 48 (citing Ex. 1003 ¶ 130; Ex. 1033, 1438, Fig. 3).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

[1.7.3]: determining, based at least in part on the captured biometric information, that the user is alive; and

Petitioner contends that the combination of Stone, Hoyos, and Varghese teaches this limitation. Pet. 48 (citing Ex. 1003 ¶¶ 132–136).

Petitioner contends that Hoyos’s biometric authentication applied to the proposed combination “teaches determining, based at least in part on the captured biometric information, that the user is alive.” Pet. 48 (citing Ex. 1003 ¶ 133). Petitioner provides the following annotated version of Hoyos’s Figure 1 (*id.*):

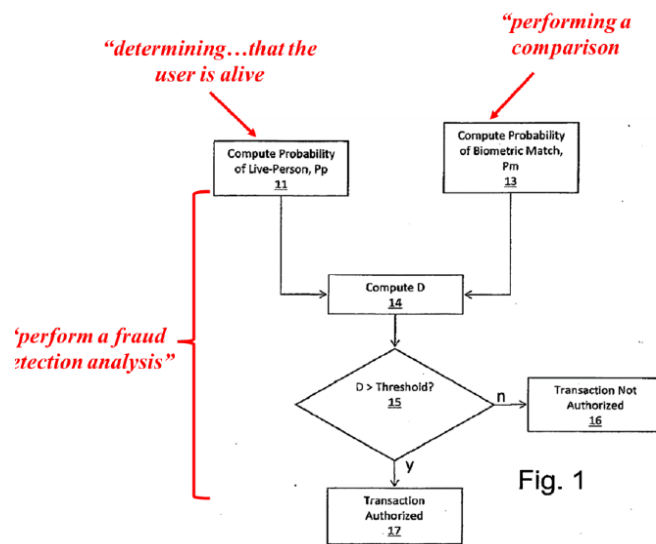


Figure 1 of Hoyos “is a flow chart of an authentication system.” Ex. 1013 ¶ 32. Petitioner adds red text “determining . . . that the user is alive” with a red arrow pointing to block 11 in Figure 1, “performing a comparison” with a red arrow pointing to block 12 in Figure 1, and “performing a fraud detection analysis” with a red line spanning the distance on the left side of Figure 1 from block 11 to block 17. Pet. 49.

Petitioner contends that Hoyos’s “authentication system includes blocks to ‘compute 11 the probability, P_p , of a live person being presented’ and ‘an authentication decision, D , is calculated as a function of the

probability of a match P_m and the probability of a live person, P_p .” Pet. 49 (citing Ex. 1003 ¶ 134; Ex. 1013 ¶ 17) (emphasis omitted). According to Petitioner, the liveness is used in Hoyos “for any step or steps taken to determine whether the biometric data is being acquired from a live human rather than a fake due to a spoof attempt.” *Id.* (citing Ex. 1003 ¶ 135; Ex. 1013 ¶ 12) (emphasis omitted).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

[1.8]: based at least in part on both the user interaction with the transaction icon rendered in the interface and performing the fraud detection analysis, complete the electronic transaction; and

Petitioner contends that the combination of Stone, Hoyos, and Varghese teaches this limitation. Pet. 50 (citing Ex. 1003 ¶¶ 137–140).

Petitioner contends that the electronic transaction is completed in the combination by “transferring funds at 318 of FIG. 3 of Stone . . . based at least in part on both the user interaction with the transaction icon (see [1.6]) and performing the fraud detection analysis (see [1.7.1]–[1.7.3]).” Pet. 50. According to Petitioner, “the user interaction is the user’s indication to continue/confirm the transaction request, and authorization of the transaction request is provided based on the fraud detection analysis, as taught by Hoyos and well-known in the art.” *Id.* (citing Ex. 1003 ¶¶ 138–139).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

[1.9]: a memory coupled to the processor and configured to provide the processor with instructions.

Petitioner contends that Stone alone or the combination of Stone, Hoyos, and Varghese teaches this limitation. Pet. 51 (citing Ex. 1003 ¶¶ 137–143).

Petitioner contends that Stone discloses memory component 506 “coupled to a processor 504 in each device of the system, and the memory is configured to provide the processor with instructions for various processes for an electronic transaction.” Pet. 51 (citing Ex. 1003 ¶ 138; Ex. 1008 ¶ 50, Fig. 5).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

a) Petitioner’s Motivation to Combine and Reasonable Expectation of Success Contentions

i. Embodiments of Stone

Petitioner contends that “[t]o the extent Patent Owner argues that FIG. 2 and 3 [of Stone] are separate embodiments” an ordinarily skilled artisan would have been motivated to combine the disclosures of Figures 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. 13 (citation omitted).

Petitioner contends that an ordinarily skilled artisan “would have understood that the display of FIG. 2 and modification thereof could be used to implement the method of FIG. 3, e.g., by adding removing, modifying components, or by using alternative design choices of buttons and icons.” Pet. 14 (citing Ex. 1003 ¶ 55; Ex. 1008 ¶¶ 55–56). Petitioner provides the following annotated side-by-side reproduction of Stone’s Figures 2 and 3 which it characterizes as “[a]n example implementation relationship with FIGS. 2 and 3” (*id.*):

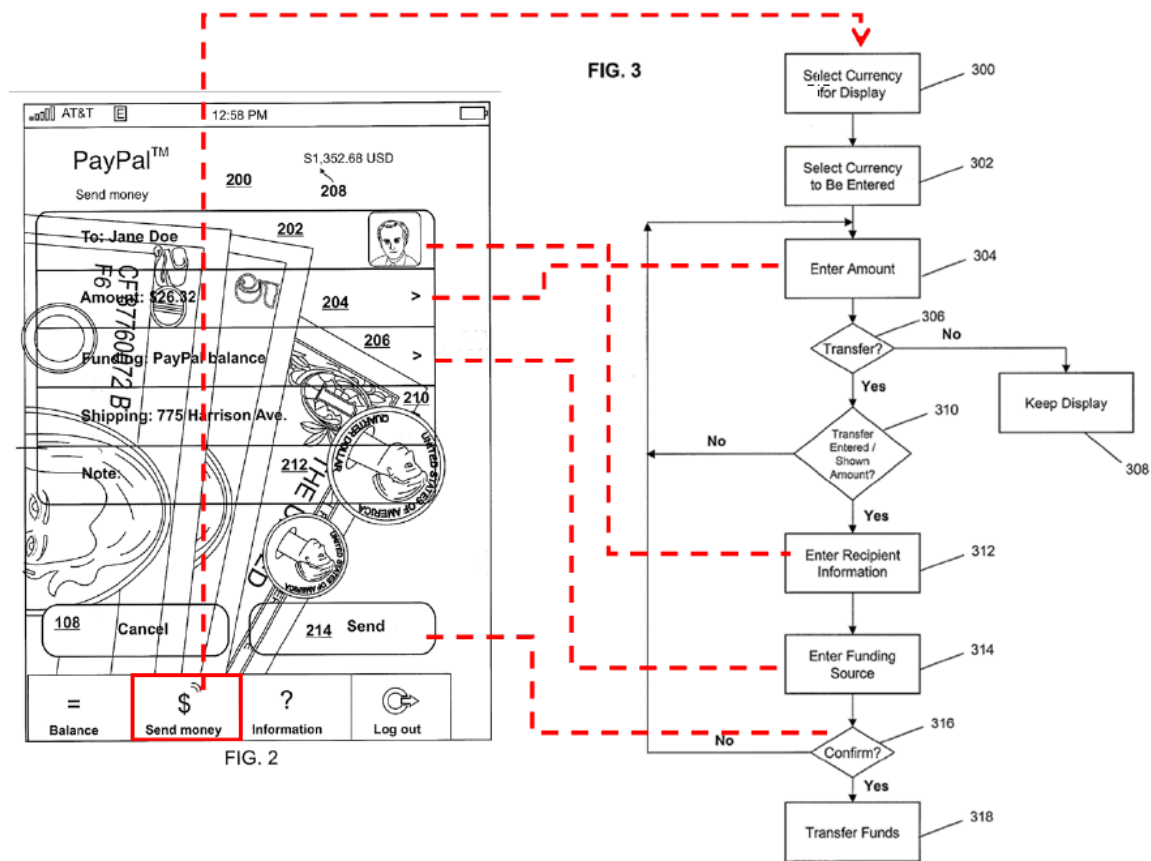


Figure 2, on the left, is “a currency display on a user device” of Stone and Figure 3, on the right, “is a flow chart” of a sample transaction. Ex. 1008 ¶¶ 11, 12, 29–35. Petitioner annotates the image with broken red lines between the “\$Send Money” icon in Figure 2 and block 300 in Figure 3, between the image of a user in Figure 2 and block 312 in Figure 3, between element 204 in Figure 2 and block 304 in Figure 3, and between element 206 in Figure 2 and block 314 in Figure 3. Pet. 14. Petitioner argues that this image shows 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 and any modification needed for combining FIGS. 2 and 3 . . . would have been within the skills of” an ordinarily skilled artisan. *Id.* at 15.

Patent Owner does not address Petitioner’s contentions. *See generally* Prelim. Resp.

We have reviewed Petitioner’s contentions and evidence and find it sufficient for institution.

ii. Stone and Hoyos

Petitioner contends that “Stone and Hoyos each are analogous art to the ’656 patent.” Pet. 15 (citing Ex. 1003 ¶ 60; Ex. 1010 ¶ 79; Ex. 1013, Title, Abstract, ¶ 2). Petitioner further contends that an ordinarily skilled artisan would have been motivated to combine “Hoyos’ teaching of fraud resistant biometric authentication in Stone’s financial transactions, for the benefits of improved fraud resistancy by addressing spoofing and achieving ‘improved deterrent against attempted fraudulent transactions and decreased rejection of valid customers’ as taught by Hoyos.” *Id.* (citing Ex. 1003 ¶¶ 59–68; Ex. 1013 ¶¶ 15, 17–22). According to Petitioner, “it was well-known that financial transactions of Stone had a need for authentication for fraud detection (e.g., with higher levels of security for higher-risk transactions).” *Id.* at 16 (citing Ex. 1003 ¶ 61; Ex. 1010 ¶ 148; Ex. 1013 ¶¶ 9, 11; Ex. 1016 ¶ 73, Fig. 3; Ex. 1022, 1; Ex. 1037, 1).

Petitioner provides the following annotated illustration of Figures 2 and 3 of Stone described above with additional annotations illustrating how it contends an ordinarily skilled artisan would have combined the teachings of Stone and Hoyos to “incorporate[e] Hoyos’ biometric authentication teachings in Stone.” Pet. 17 (citing Ex. 1003 ¶ 63; Ex. 1008, Figs. 2, 3; Ex. 1013 ¶ 17, Fig. 1).

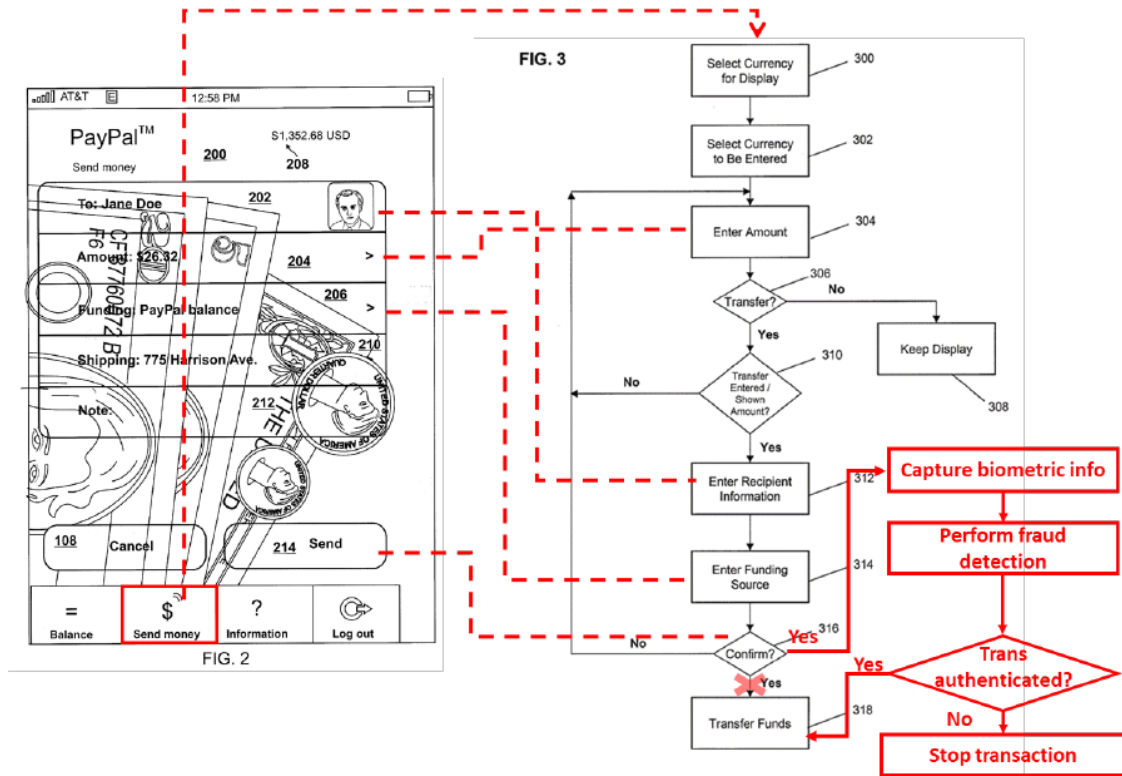


Figure 2, on the left, is “a currency display on a user device” of Stone and Figure 3, on the right, “is a flow chart.” Ex. 1008 ¶¶ 11, 12. Petitioner annotates the figures with broken red lines between the “\$Send Money” icon in Figure 2 and block 300 in Figure 3, between the image of the recipient in Figure 2 and block 312 in Figure 3, between element 204 in Figure 2 and block 304 in Figure 3, and between element 206 in Figure 2 and block 314 in Figure 3. *Id.* Petitioner also adds in red proposed additional steps, based on Hoyos’s disclosure of biometric authentication analysis, to be performed between blocks 316 and 318 in Figure 3 of Stone. *Id.* Petitioner annotates the additional steps in red as “Capture biometric info”, “Perform fraud detection”, “Trans Authenticated?”, and “Stop transaction”. *Id.*

Petitioner argues that an ordinarily skilled artisan would have implemented Hoyos’s biometric transaction authentication “after a user confirms a user transaction request, which is **at least after** a user interaction

with an icon . . . to initiate the transaction request, and **after user interactions** with icons to continue . . . and confirm . . . the transaction request.” Pet. 17–18 (citing Ex. 1003 ¶ 64). According to Petitioner, “performing real-time authentication using authentication data captured after and in response to user transaction request confirmation had various benefits with improved security.” *Id.* at 18, 19 (“by capturing real-time, more accurate data, improved fraud detection and security is achieved, e.g., by avoiding imposters from communicating based on stolen biometric data and reducing spoofing.” (citing Ex. 1003 ¶ 65)). Petitioner contends that in the combination of Stone and Hoyos, an ordinarily skilled artisan “would assess the risk of a transaction based on various transaction factors received through user interaction with icons in the user interface” such as “a large transaction amount would typically be considered higher risk than a small transaction amount.” *Id.* at 18–19,

Petitioner next contends 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 within the skill of” an ordinarily skilled artisan. Pet. 20 (citing Ex. 1003 ¶ 66; Ex. 1009, 15:22–23; Ex. 1013, Title, ¶¶ 7, 40, claims 13, 14). Petitioner further contends that an ordinarily skilled artisan “would have been motivated to implement the fraud detection analysis based on the biometric information **locally** on the user device of Stone.” *Id.* at 20–21. According to Petitioner, implementing the fraud detection locally on the user device provides “benefits including reduced latency . . . offline analysis capabilities . . . enhanced privacy . . . customization for device characteristics . . . improved security . . . and

reduced server load for cost savings and improved scalability.” *Id.* at 21 (citing Ex. 1003 ¶ 68).

We have reviewed Petitioner’s contentions and evidence and find it sufficient for institution. For the reasons discussed below, we find that Patent Owner’s arguments against the combination of Stone and Hoyos and whether Stone is analogous art do not undercut Petitioner’s showing based on the present record.

iii. Stone, Hoyos, and Varghese

Petitioner first contends that “Varghese is analogous art to the ’656 patent” and “provid[es] additional forms of authentication as needed e.g., where the service provider is a bank or other financial institution which seeks a higher security authentication.” Pet. 22 (citing Ex. 1003 ¶ 70; Ex. 1010 ¶ 45). In particular, Petitioner contends that an ordinarily skilled artisan would have “appl[ied] Varghese’s teaching of multifactor real-time authentication for user transaction requests, including authentication based on physical location associated with the user and voice authentication, in Stone-Hoyos for improved security for financial transactions.” *Id.* at 21–22 (citing Ex. 1003 ¶¶ 69–79). Petitioner argues the combination would “implement[] the multifactor authentication such that, together with the biometric authentication as taught by Hoyos . . . physical location authentication . . . as taught by Varghese is” used for “detecting and preventing access attempts from locations commonly associated with cyber threats, providing cross-checking with a user location for a transaction request, and providing additional security without significant additional inconvenience to the user.” *Id.* at 22–23 (citing Ex. 1003 ¶ 71; Ex. 1037, 7–12).

Petitioner provides the following annotated illustration of Figures 2 and 3 of Stone described above with annotations of how it contends an ordinarily skilled artisan would have combined the teachings of Stone, Hoyos, and Varghese (Pet. 23 (citing Ex. 1003 ¶ 73)):

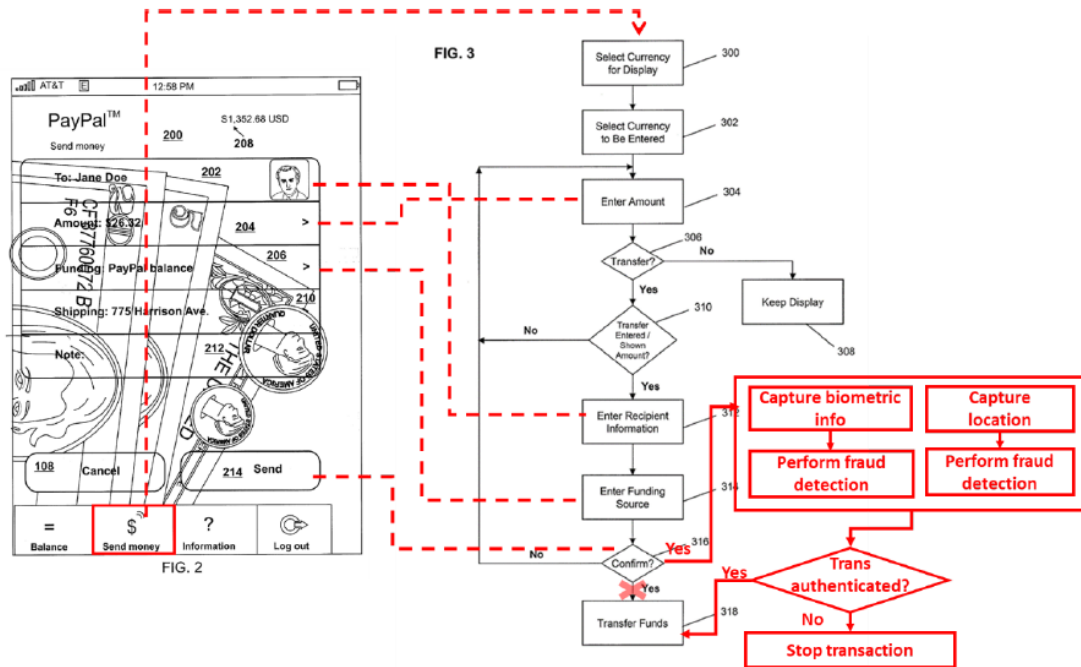


Figure 2, on the left, is “a currency display on a user device” of Stone and Figure 3, on the right, “is a flow chart.” Ex. 1008 ¶¶ 11, 12. Petitioner annotates the figures with broken red lines between the “\$Send Money” icon in Figure 2 and block 300 in Figure 3, between the image of the recipient in Figure 2 and block 312 in Figure 3, between element 204 in Figure 2 and block 304 in Figure 3, and between element 206 in Figure 2 and block 314 in Figure 3. *Id.* Petitioner also annotates in red proposed additional steps, based on Varghese’s disclosure of location analysis and Hoyos’s disclosure of biometric authentication analysis, to be performed between blocks 316 and 318 in Figure 3. *Id.*

Petitioner provides reasons why an ordinarily skilled artisan would have incorporated Varghese's multifactor real-time authentication after a user confirms a transaction request that are similar to the reasons provided for combining the teachings of Stone and Hoyos discussed above. Pet. 24. According to Petitioner, adding the teachings of Varghese to the Stone and Hoyos combination would provide the additional benefit of "perform[ing] fraud detection based on whether the two locations (captured before for currency display and after confirmation at 316) match for improved security." *Id.* (citing Ex. 1003 ¶ 76).

Petitioner next contends that an ordinarily skilled artisan would have a reasonable expectation of success "in configuring Stone-Hoyos-Varghese to leverage Varghese's multifactor real-time authentication functionality since its implementation would have required only routine knowledge well within the skill of a" person of ordinary skill in the art. Pet. 25 (citing Ex. 1033 ¶ 77). Petitioner further contends that "it would have been within the skills of a [person of ordinary skill in the art] to implement the teachings of Varghese, locally or remotely in the system of Stone." *Id.* According to Petitioner, implementing fraud detection analysis locally on Stone's user device would provide the benefits of "reduced latency," "offline analysis capabilities," "enhance privacy," "efficient resource utilization," "customization for device characteristics," "improved security," and "reduced server load for cost savings and improved scalability." *Id.* at 26 (citing Ex. 1003 ¶ 79).

We have reviewed Petitioner's contentions and evidence and find it sufficient for institution. For the reasons discussed below, we find that

Patent Owner's arguments against the combination of Stone, Hoyos, and Varghese do not undercut Petitioner's showing based on the present record.

b) Patent Owner's Contentions

i. Sufficiency of Dr. Jones's Declaration

Patent Owner contends that we should give no weight to the testimony of Dr. Jones in connection with Petitioner's motivation-to-combine and reasonable-expectation-of-success arguments. Prelim. Resp. 30. In support of this contention, Patent Owner provides a table reproducing side-by-side various statements from pages 21–26 of the Petition with paragraphs 69 and 79 (as allegedly representative of paragraphs 69–79) of Dr. Jones's declaration testimony. *Id.* at 37–41. Patent Owner argues that Dr. Jones's cited testimony "is virtually identical to the analysis in the Petition." *Id.* at 31. According to Patent Owner, the "Board has previously held that where, as here, an expert adds nothing beyond what is in the Petition, the expert's testimony should be given little or no weight." *Id.* at 34 (citing *Samsung Elecs. Co. v. RightQuestion, LLC*, IPR2022-0025, Paper 17 at 24 (PTAB June 9, 2022)).

For the following reasons, this contention is unavailing based on the present evidentiary record.

In *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 at 15–17 (PTAB Aug. 24, 2022) (precedential), the Board accorded "little weight" to declaration testimony that contains a *verbatim* restatement of a petition's arguments without additional supporting evidence or reasoning. In *Xerox*, the Board held that the critical inquiry is whether a declaration is conclusory and unsupported and whether it discloses underlying facts or data on which the opinion is based. *Xerox*, Paper 9 at 15 (quoting 37 C.F.R. § 42.65(a)

(“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.”)); *see also RightQuestion, LLC*, Paper 17 at 23 (“Petitioner’s declarant makes these same statements verbatim, without more, and with no additional citations to evidence.”).

Patent Owner ignores Dr. Jones’s testimony summarizing the relevant disclosures from Stone, Hoyos, and Varghese on which he relies to form his opinions. Ex. 1003 ¶¶ 37–46. Patent Owner also ignores Dr. Jones’s testimony of the specific basis for his opinion that a person of ordinary skill in the art would have been motivated to combine Stone, Hoyos, and Varghese with a reasonable expectation of success. Ex. 1003 ¶¶ 54–68. This testimony contains specific detailed citations to the references in support of Dr. Jones’s opinions.

We, thus, find that Dr. Jones’s testimony in support of the Petition, taken as a whole, is supported sufficiently with evidence and technical reasoning at this stage of the proceeding. Consequently, we do not give his testimony little to no weight because portions of it are repeated in the Petition.

ii. Petitioner’s Explanation for Combining Stone, Hoyos, and Varghese

Patent Owner contends that “Petitioner’s ‘explanations’ for why a [person of ordinary skill in the art] would have combined Stone, Hoyos, and Varghese offer no explanation at all.” Prelim. Resp. 34–35. Patent Owner makes substantially the same assertion with respect to Petitioner’s proposed combination of Stone and Hoyos. *Id.* at 35.

For the Stone and Hoyos combination, Patent Owner asserts that “Stone does not mention fraud, and certainly does not discuss any

techniques for preventing fraud, particularly biometric authentication techniques described in Hoyos.” Prelim. Resp. 35–36. Patent Owner next asserts that “Hoyos . . . has an extremely narrow focus—improving known biometric matching techniques by incorporating a method to determine the probability that the subject is alive.” *Id.* at 36 (citing Ex. 1013 ¶¶ 16–22). According to Patent Owner, “Hoyos is not concerned with improving an electronic display . . . or improving a user’s experience based on providing a richer interface (like Stone),” and according to Patent Owner “[n]othing in Hoyos would lead a [person of ordinary skill in the art] to combine its biometric authentication models with an interactive interface, particularly a currency display like the one Stone provides.” *Id.*; *see also id.* at 48 (arguing “there is nothing in the teachings of Hoyos to suggest it would be employed with a user interface.”).

For the following reasons, Patent Owner’s contentions do not undercut Petitioner’s showing based on the present evidentiary record at this stage of the proceeding.

Although Stone does not explicitly mention the word “fraud,” it discloses that user device 408 may include user identifiers 418 that “may include attributes related to the user such as . . . a user name, password, photograph image, biometric id.” Ex. 1008 ¶ 45. Dr. Jones testifies that “Stone’s biometric information/‘biometric id’ is typically received and stored on user device 404 during an enrollment/registration process” and “is used for subsequent comparison with the later captured data to provide an authentication decision for a transaction request.” Ex. 1003 ¶ 92 (citing Ex. 1014 ¶ 9; Ex. 1021, Abst.; Ex. 1023, 8:3–9:39). Patent Owner’s attorney argument that Stone does not mention fraud or biometric authentication

ignores the cited disclosure in Stone and Dr. Jones’s testimony which is sufficiently supported by the references he cites. Further, Patent Owner’s argument that Stone does not discuss techniques for preventing fraud is undercut by its acknowledgement that Stone discloses “authentication of the user[] by the payment server where the user’s account information is stored.” Prelim. Resp. 44 (citing Ex. 1008 ¶ 46).

Patent Owner’s argument that Hoyos is not concerned with improving an electronic display or a user’s experience (Prelim. Resp. 36) is unavailing because it fails to address Petitioner’s proposed combination. Petitioner does not rely on Hoyos to improve an electronic display or the user experience but proposes modifying Stone by “implement[ing] Hoyos’ spoofing resistant biometric authentication for fraud detection” with the resulting benefit of “improved deterrent against attempted fraudulent transactions and decreased rejection of valid customers.” Pet. 16 (citing Ex. 1003 ¶ 62).

With respect to adding Varghese to the combination of Stone and Hoyos, Patent Owner’s argument is that Petitioner “fails to explain why a [person of ordinary skill in the art] would have combined location authentication mentioned in Varghese with Hoyos’s biometric authentication techniques.” Prelim. Resp. 37. Patent Owner, however, does not address Petitioner’s assertions that a person of ordinary skill in the art would have implemented Varghese’s multifactor real-time authentication including location authentication “for improved security” and the other alleged benefits for doing so stated in the Petition. Pet. 22.

iii. Patent Owner's Assertion that Stone Is Not Analogous Art

Patent Owner asserts that Stone does not satisfy either prong of the analogous-art test. Prelim. Resp. 39.

Patent Owner first contends that “Stone is not in the same field of endeavor as the ’656 Patent.” Prelim. Resp. 39. Patent Owner argues that the background of the invention of the ’656 patent and claims are focused on detecting and preventing fraud in electronic transactions. *Id.* at 40. According to Patent Owner, Stone “relates to electronic visual displays . . . that show a visual representation of financial instruments,” “is not in the field of electronic fraud prevention,” and “never discusses fraud.” *Id.*

As to whether or not Stone is reasonably pertinent to the particular problem of “electronic payment fraud,” Patent Owner asserts that Stone is not analogous art because it “does not even recognize payment fraud as a problem needing to be solved.” Pet. 40–41.

Petitioner, in turn, argues that “Stone discloses secure transactions with multi-factor authentication.” Prelim. Reply 3.

For the following reasons, Patent Owner’s contention is unavailing based on the present record.

For a prior-art reference to qualify as analogous art, the reference must either be in the field of the applicant’s endeavor or reasonably pertinent to the problem with which the inventor was concerned. *In re Oetiker*, 977 F.2d 1443, 1447 (Fed. Cir. 1992). References are selected as being reasonably pertinent to the problem based on the judgment of a person having ordinary skill in the art. *Id.* (“[I]t is necessary to consider ‘the reality of the circumstances,’ --in other words, common sense--in deciding in which fields a person of ordinary skill would reasonably be expected to look for a

solution to the problem facing the inventor.” (quoting *In re Wood*, 599 F.2d 1032, 1036 (CCPA 1979))). Furthermore, the scope of analogous art is to be construed broadly. *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1238 (Fed. Cir. 2010) (“The Supreme Court’s decision in *KSR International Co. v. Teleflex, Inc.*, 550 U.S. 398 (2007), directs us to construe the scope of analogous art broadly, stating that ‘*familiar items may have obvious uses beyond their primary purposes*, and a person of ordinary skill often will be able to fit the teachings of multiple patents together like pieces of a puzzle.’ *Id.* at 402 (emphasis added).”).

The ’656 patent describes that “[a] \$20 bill when held in a person’s hand and presented to a merchant is a tangible item with a concrete value” but “[when] the same amount of money is involved in an electronic transaction . . . the amount of money involved may seem less concrete.” Ex. 1001, 5:2–7. The ’656 patent further describes a display that “mak[es] a given transaction more concrete and emphasizing the victim’s identity.” *Id.* at 5:23–35.

Stone discloses a user display used in electronic financial transactions. Ex. 1008, Figs. 1, 2. The display shows “the actual currency representing the” funds to be transferred and a face of the recipient. *Id.* ¶¶ 23, 24.

As discussed above, Stone discloses user device 408 includes personal information of a user including “a user name, password, photograph image, and biometric id.” Ex. 1008 ¶ 45. Further, as discussed above, Dr. Jones testifies that a person of ordinary skill in the art would understand that Stone’s biometric id is used for authentication. Ex. 1003 ¶ 92. The ’656 patent similarly discloses use of biometrics. *See e.g.*, Ex. 1001, 6:45–51.

Dr. Jones further testifies that Stone (as well as Hoyos and Varghese) is analogous art to the '656 patent as in the same field of endeavor and/or reasonably pertinent to a problem faced by the inventor of the '656 patent. Ex. 1003 ¶ 53. Dr. Jones provides citations to the '656 patent and to Stone in support of his testimony. *Id.*

For all the foregoing reasons and construing the scope of analogous art broadly, Patent Owner's attorney argument does not undercut Petitioner's showing at this stage of the proceeding that Stone is at least "reasonably pertinent" analogous art.

iv. Patent Owner's Assertion that the References Teach Away from or Conflict with Each Other
a. Stone and Hoyos

Patent Owner first contends that "Stone and Hoyos teach away from each other and are incompatible because their inventions are directed to different computing environments." Prelim. Resp. 41. In support of this contention, Patent Owner argues that Stone "is premised on a client-server structure for communication to populate the currency display and complete electronic transactions." *Id.* at 41–42 (citing Ex. 1008 ¶¶ 40–48, Fig. 4). Patent Owner attempts to draw a contrast with Stone by arguing that Hoyos "proposes user verification that occurs only on the client device" and "does not mention applying its authentication techniques to a client-server structure." *Id.* at 42 (citing Ex. 1013 ¶¶ 16–22).

Patent Owner next contends that "Hoyos is not compatible with [a client-server environment] because of *how* it employs its disclosed biometric identification techniques." Prelim Resp. 42. Patent Owner argues that Hoyos calculates a "match" probability between "collected biometric information" and "the user's known biometric information" in an

“eigenvector-based facial recognition system” disclosed in U.S. Patent 5,164, 992 (Ex. 2028, “Turk Patent”). *Id.* (citing Ex. 1013 ¶ 38; Ex. 2028, 3:17–25). According to Patent Owner, the “method described in the Turk Patent is computationally intensive and intended to handle a much smaller number of users, as the computational effort becomes more burdensome as the population of known users grows.” *Id.* (citing Ex. 2028, 8:16–24), 24 (“Turk also makes clear that it performs these identification tasks for limited groups of known users on the client, not a server environment that may consider thousands, if not millions, of potential users.” *Id.* at 43 (citing Ex. 2028, 8:16–24).

Patent Owner next contends that “[g]iven the computationally intensive nature of Turk’s identification method that Hoyos employs . . . and its intention to apply it to a small number of [users] identified in a known pool, a [person of ordinary skill in the art] would not have applied this method to the client-server structure that Stone envisions.” Prelim. Resp. 43. Patent Owner additionally argues that “[i]t also would not make sense to add the Hoyos client-only identification method as an extra step to Stone’s transaction process as Petitioner describes in the Petition. *Id.* (citing Pet. 21–26, 44–45 (“Inserting the Hoyos client-only authentication process as the final step before completing the transaction would require a second round of authentication, to be done locally on the device no less, followed by more communication with the payment server to complete the transaction.”), 45 (“These multiple rounds of authentication would be redundant and would slow down transaction time, which undermines a goal of Hoyos (transaction speed) to address a problem that Stone does not even identify as a concern (payment fraud).”).

Petitioner, in turn, argues that Patent Owner’s “teaching away (based on the incorrect bodily incorporation of an example from Turk), is also misplaced because it identifies nothing in prior art that criticized, discredits, or otherwise discourages the claimed invention.” Prelim. Reply 5.

For the following reasons, Patent Owner’s contention is unavailing based on the present record.

“A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1327 (Fed. Cir. 2009) (citation omitted). But even if a reference is not found to teach away, its statements regarding preferences are relevant to a finding regarding whether a skilled artisan would have been motivated to combine that reference with another reference. *See Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1051 n.15 (Fed. Cir. 2016) (en banc).

The crux of Patent Owner’s teaching-away contention is that an ordinarily skilled artisan would not have combined Hoyos with Stone because the required computations in Turk, referenced in paragraph 38 of Hoyos, are extensive and, according to Patent Owner, can only be applied to a small number of users not a large number of users such as in Stone’s client-server structure. Patent Owner relies on three portions of Turk to support this argument, i.e., col. 3, lines 17–25, col. 7, lines 7:41–47, and col. 8, lines 16–24. Prelim. Resp. 41–43. Those portions of Turk read as follows:

Referring to FIG. 1, in an audience monitoring system 2, a video camera 4, which is trained on an area where members of a viewing

audience generally sit to watch the TV, sends a sequence of video image frames to a motion detection module 6. Video camera 4, which may, for example, be installed in the home of a family that has volunteered to participate in a study of public viewing habits, generate images of TV viewing audience.
Ex. 2028, 3:1–17.

To summarize, the eigenfaces approach to face recognition involves the following steps:

1. Collect a set of characteristic face images of the known individuals. This set may include a number of images for each person, with some variation in expression and in lighting. (Say four images for ten people, so $M=40$).
Id. at 7:41–47.

Designing a practical system for face recognition within this framework requires assessing the tradeoffs between generality, required accuracy, and speed. If the face recognition task is restricted to a small set of people (such as the members of a family or small company), a small set of eigenfaces is adequate to span the faces of interest. If the system is to learn new faces or represent many people, a larger basis set of eigenfaces will likely be required.
Id. at 8:16–24 (emphasis added).

Based on our review of the cited portions of Turk, we find little, if any support, for Patent Owner’s contention that Hoyos (or Turk) teaches away from Stone because of Stone’s client-server structure. Rather than discouraging applying its technique to Stone, it appears that Turk explicitly contemplates applying its technique to groups of people larger than the example discussed in Turk, such as in the client-server structure of Stone, based on tradeoffs between generality, required accuracy, and speed. *See Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed Cir. 2006) (“a given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine.”).

Whether or not a person of ordinary skill in the art would be motivated to combine Stone and Hoyos is ultimately a question of fact. *WBIP*, 829 F.3d at 1327. Petitioner relies on Dr. Jones’s testimony to support its contention that a person of ordinary skill in the art would have combined Stone and Hoyos. Pet. 15 (citing Ex. 1003 ¶¶ 59–68). Dr. Jones provides detailed technical reasoning with reference to various portions of Stone and Hoyos in support of Petitioner’s contention. Ex. 1003 ¶¶ 59–68. Patent Owner’s contention is attorney argument that, based on the present record, does not appear to be supported by Turk.

b. Varghese and Hoyos

Patent Owner first contends that “Varghese amplifies the disconnect between Stone and Hoyos regarding the client and server distinction” and “Varghese like Stone, envisions a client-server structure.” Prelim. Resp. 46 (citing Ex. 1010 ¶¶ 5–6). Patent Owner relies on the same arguments as for the Stone and Hoyos combination just discussed. *Id.* This contention is, thus, unavailing for the same reasons discussed above for Stone and Hoyos.

Patent Owner next contends that an ordinarily skilled artisan would not have combined Varghese and Hoyos because one of Varghese’s goals “is to provide a ‘purely software based solution to identity theft that does not require hardware devices to be issued and maintained.” Prelim. Resp. 46 (citing Ex. 1010 ¶ 22). Patent Owner points out that Hoyos discloses “sensor-based biometrics, such as fingerprints and facial biometrics, both of which need hardware sensors to operate.” *Id.* (citing Ex. 1013 ¶¶ 18–19, 22, 34–36). According to Patent Owner, “[b]ecause the hardware-based biometrics collection and authentication techniques described in Hoyos conflict with Varghese’s stated goal of providing a ‘purely software based

solution to identify theft’ . . . a [person of ordinary skill in the art] would not have been motivated to combine these references.” *Id.* at 47.

Petitioner, in turn, argues that Patent Owner’s “reliance on Varghese’s solution that ‘***does not require hardware device to be issued and maintained***’ . . . is misplaced, because it refers to a solution that does not require physical tokens issued to users.” Prelim. Reply 3–4 (citing Ex. 1037, 8–9).

We acknowledge the portion of Varghese cited by Patent Owner describes “a purely software based solution that does not requires hardware devices to be issued and maintained.” Ex. 1010 ¶ 22. The import of this statement in the context of the entire disclosure of Varghese is unclear based on the present record. For example, Varghese, like Hoyos, discloses authentication using a fingerprint process which appears to undercut Patent Owner’s argument. *See* Ex. 1010, Fig. 13B, ¶ 73. Consequently, this issue is better resolved based on a complete record at trial.

For the foregoing reasons, Patent Owner does not undercut Petitioner’s reasoning why one with ordinary skill in the art would have been motivated to combine Varghese with Stone and Hoyos based on the present evidentiary record.

c. Stone, Hoyos, and Varghese

Patent Owner argues that an ordinarily skilled artisan would not have been motivated to combine Stone, Hoyos, and Varghese because “there is nothing in the teachings of Hoyos to suggest it would be employed with a user interface, or more specifically, that its biometric collection and authentication procedures would occur at the final stages of an electronic transaction.” Prelim. Resp. 48. Patent Owner next argues that an ordinarily

skilled artisan would not “have been motivated to add the location collection of Varghese to . . . Stone, particularly at the final confirmation stage.” *Id.* at 49. In support of this argument, Patent Owner submits that “Varghese discloses a multifactor authentication framework divided into pre-authentication and post-authentication stages” and “most critical, Varghese teaches that post-authentication is for completing monetary *electronic transactions*, which are authenticated using a user’s transaction history.” *Id.* at 49–50 (citing Ex. 1010 ¶¶ 65, 74, 90). According to Patent Owner, based on these teachings of Varghese, an ordinarily skilled artisan “would not have been motivated to collect location data (a pre-authentication technique for user login requests) to authenticate an *electronic transaction* [post-authentication request], particularly as the last step of the transaction.” *Id.* at 50.

Patent Owner’s contention is unavailing because it is attorney argument and appears to be arguing for a bodily incorporation of Varghese into the Stone/Hoyos combination. Further, Patent Owner does not address Petitioner’s stated reasons for the combination which are supported by the testimony of Dr. Jones and his detailed citations to the references. Pet. 21–24 (citing Ex. 1003 ¶¶ 69–79). Patent Owner’s attorney arguments do not undercut Petitioner’s showing at this stage of the proceeding based on the current record.

Independent Claims 10 and 19

For claims 10 and 19, Petitioner relies on its contentions for various limitations of claim 1. *See* Pet. 59–60, 61. With respect to the preamble of claim 10 ([10.0]: *A method, comprising:*) and the preamble of claim 19 ([19.0]: *A computer program product embodied in a non-transitory*

computer readable storage medium and comprising computer instructions for:), Petitioner argues that, to the extent they are limiting, Stone discloses them or renders them obvious. *Id.* at 58–59 (citing Ex. 1003 ¶¶ 168–170; Ex. 1008 ¶¶ 29–36, Fig. 3), 60–61 (citing Ex. 1003 ¶¶ 186–188; Ex. 1008 ¶ 54).

Patent Owner does not provide separate arguments for claims 10 and 19. *See generally* Prelim. Resp.

We reviewed Petitioner’s evidence and arguments for claims 10 and 19 and for the reasons discussed with respect to claim 1 determine that Petitioner has shown a reasonable likelihood that claims 10 and 19 would have been unpatentable over Stone, Hoyos, and Varghese.

Summary for Claims 1, 10, and 19

For all the foregoing reasons, we determine that Petitioner has shown a reasonable likelihood that claims 1, 10, and 19 would have been unpatentable over Stone, Hoyos, and Varghese.

5. Claims 4–9 and 13–18

These claims depend directly or indirectly from one of claims 1 and 10. Ex. 1001, 14:39–51, 15:23–36. Petitioner sets forth evidence and argument as to why Stone, Hoyos, and Varghese allegedly render claims 4–9 and 13–18 unpatentable. Pet. 52–58, 60.

Patent Owner does not provide separate arguments for these claims. *See generally* Prelim. Resp.

We reviewed Petitioner’s evidence and arguments and determine that Petitioner has shown a reasonable likelihood that these dependent claims would have been unpatentable over Stone, Hoyos, and Varghese.

F. Ground 2: Alleged Obviousness of Claims 1, 4–10, and 13–19 over Stone and FFIEC Guidance

Petitioner contends claims 1, 4–10, and 13–19 would have been obvious over Stone and FFIEC Guidance. Pet. 62–76. Petitioner supports its contentions with the Declaration of Dr. Jones. Ex. 1003. Patent Owner disputes Petitioner’s contentions. Prelim. Resp. 50–53.

We begin with a brief summary of FFIEC Guidance and then address the parties’ respective contentions.

1. FFIEC Guidance (Ex. 1037)

FFIEC Guidance is titled “Authentication in an Internet Banking Environment” and was issued by Federal Financial Institutions Examination Council. Ex. 1037, 1. FFIEC 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.” *Id.*

According to FFIEC Guidance, “[a]uthentication is typically dependent upon customers providing valid identification data followed by one or more authentication credentials (factors) to prove their identity. Ex. 1037, 7. Noting that “[a]ccount fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation,” FFIEC Guidance states that “[t]he agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties.” *Id.* at 1. “Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should

implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.” *Id.* at 1–2.

For example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN).

Id. at 3.

FFIEC Guidance describes “a variety of technologies and methodologies financial institutions can use to authenticate customers,” including “the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of ‘tokens’, transaction profile scripts, biometric identification, and others.” Ex. 1037, 2. For example, FFIEC Guidance describes authentication techniques using biometrics as follows:

Biometric technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic (something a person is). Physiological characteristics include fingerprints, iris configuration, and facial structure. Physical characteristics include, for example, the rate and flow of movements, such as the pattern of data entry on a computer keyboard. The process of introducing people into a biometrics-based system is called “enrollment.” In enrollment, samples of data are taken from one or more physiological or physical characteristics; the samples are converted into a mathematical model, or template; and the template is registered into a database on which a software application can perform analysis. Once enrolled, customers interact with the live-scan process of the biometrics technology. The live scan is used to identify and authenticate the customer. The results of a live scan, such as a fingerprint, are compared with the registered templates stored in the system. If there is a match, the customer is authenticated and granted access.

Id. at 9–10. FFIEC Guidance also describes other authentication techniques to filter and limit an online transaction, such as IPA location technology based on determination of “who is assigned to the requesting Internet Protocol Address,” or geo-location technology based on determination of where Internet users are. *Id.* at 12.

2. *Claims 1, 10, and 19*

Petitioner provides a limitation-by-limitation analysis of independent claims 1, 10, and 19, mapping the prior art to the claim limitations. Pet. 63–73, 74, 75–76. Petitioner also provides contentions concerning motivation to combine Stone and the Guidance, and reasonable expectation of success of the combination. *Id.* at 62–63.

Patent Owner does not dispute Petitioner’s mapping of the prior art to the claim limitations. *See generally* Prelim. Resp. Patent Owner contends that Petitioner’s expert’s declaration should be given no weight in the motivation-to-combine and reasonable-expectation-of-success analyses (Prelim. Resp. 50–51); Petitioner’s explanation for the motivation to combine Stone and the Guidance is insufficient (*id.* at 51–53); and Stone is not analogous art (*id.* at 53).

With this background, we analyze the parties’ respective contentions.

For the preamble and limitations 1.1–1.5, and 1.9, Petitioner relies on substantially the same disclosures from Stone which we found to be sufficient for ground 1. Pet. 62–65, 73.

We reviewed the evidence cited by Petitioner for these limitations which is not disputed by Patent Owner and find it sufficient for institution.

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

transaction, the captured contextual information comprising captured biometric information and location data associated with the user;

Petitioner contends that the combination of Stone and the Guidance teaches this limitation. Pet. 65 (citing Ex. 1003 ¶¶ 216–222).

Petitioner contends that the “Guidance describes multifactor real-time authentication for financial transactions, which uses a combination of authentication techniques of different factors including physical location authentication . . . along with biometric authentication including face recognition . . . with testing for liveness, based on the risk of the transaction.” Pet. 66 (citing Ex. 1003 ¶ 217; Ex. 1037, 3, 11–12). Petitioner further contends that, based on the Guidance, an ordinarily skilled artisan ‘would have been motivated to perform transaction authentication for a transaction request using a combination of physical location and biometrics authentication using facial recognition with liveness test.” *Id.* According to Petitioner, the benefits of using physical location authentication include “preventing access attempts from locations commonly associated with cyber threats, providing cross-checking with a user location for a transaction request, and providing additional security without significant additional inconvenience to the user.” *Id.* (citing Ex. 1003 ¶ 218). Petitioner further argues that biometric authentication using facial recognition provides “the benefits of contactless and hygienic authentication using easy to acquire . . . facial images and spoof-proofing.” *Id.* at 66–67 (citing Ex. 1003 ¶ 218).

Petitioner provides the following annotated illustration of Figures 2 and 3 of Stone described above with annotations of how it contends an ordinarily skilled artisan would have combined the teachings of Stone and the Guidance (Pet. 67–68 (citing Ex. 1003 ¶ 220)):

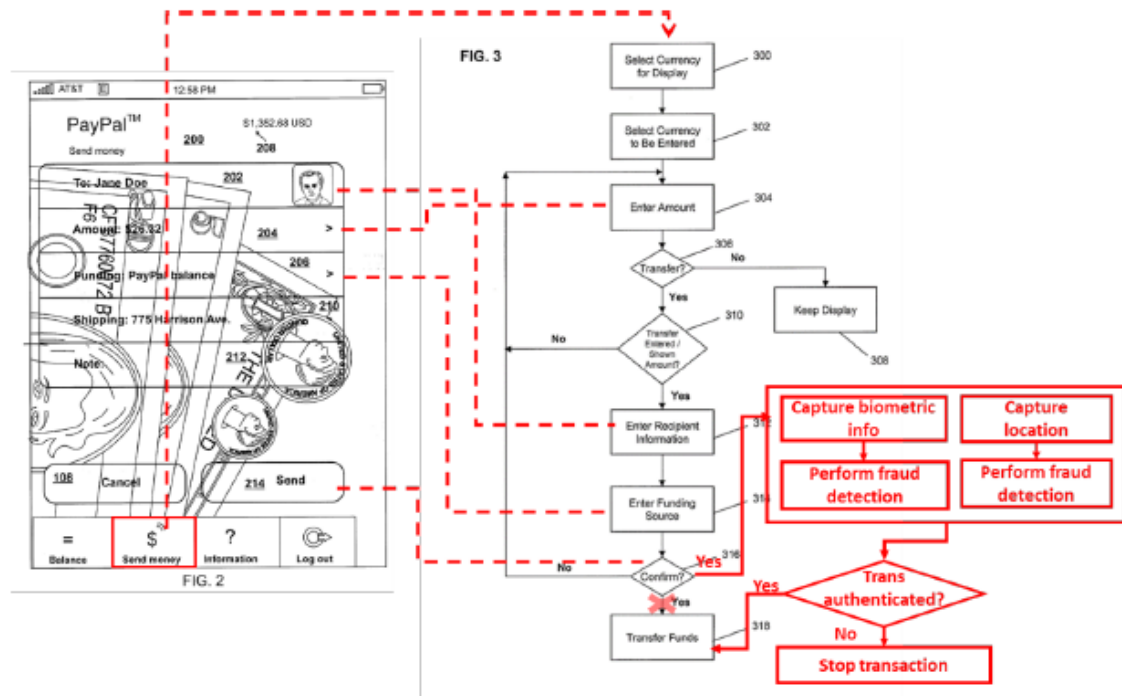


Figure 2, on the left, is “a currency display on a user device” of Stone and Figure 3, on the right, “is a flow chart.” Ex. 1008 ¶¶ 11, 12. Petitioner annotates the figures with broken red lines between the “\$Send Money” icon in Figure 2 and block 300 in Figure 3, between the image of the recipient in Figure 2 and block 312 in Figure 3, between element 204 in Figure 2 and block 304 in Figure 3, and between element 206 in Figure 2 and block 314 in Figure 3. *Id.* Petitioner also annotates in red proposed additional steps, based on the Guidance’s disclosure of location authentication analysis and biometric authentication analysis, to be performed between blocks 316 and 318 in Figure 3. *Id.*

Petitioner contends that an ordinarily skilled artisan would have been motivated to implement the Guidance’s multifactor real-time authentication in Stone “after user transaction request confirmation, which is at least after the user interaction with the icon . . . to initiate the transaction request, and

after user interactions with icons to continue . . . and confirm . . . the transaction request.” Pet. 68–69. Petitioner contends that the ordinarily skilled artisan would have done so “for the benefits of risk-based contextual authentication adaptive for the specific transaction based on transaction information, and more accurate real-time information for real-time authentication.” *Id.* at 69 (citing Ex. 1003 ¶ 221; Ex. 1010 ¶¶ 91, 97–99, 148, Fig. 14, Table 10; Ex. 1013 ¶ 28; Ex. 1015, Fig. 4; Ex. 1016 ¶¶ 36, 43, 73, Fig. 3; Ex. 1035, 4:60–62, 4:66–67).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

[1.7.1]: perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises:

Petitioner contends that the combination of Stone and the Guidance teaches this limitation. Pet. 69 (citing Ex. 1003 ¶¶ 223–225).

Petitioner specifically contends that the “Guidance describes performing a fraud detection analysis of the captured contextual information, describing various techniques for fraud detection analysis where ‘selection and use of any technique should be based upon the assessed risk.’” Pet. 69 (citing Ex. 1003 ¶ 224; Ex. 1037, 7, 9–10, 12).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

[1.7.2]: performing a comparison based at least in part on the stored biometric information and the captured biometric information; and

Petitioner contends that the combination of Stone and the Guidance teaches this limitation. Pet. 70 (citing Ex. 1003 ¶¶ 226–228).

Petitioner contends that the “Guidance describes, for biometric authentication as applied in Stone, the basic knowledge of performing a comparison based on the stored biometric information and the captured biometric information.” Pet. 70 (citing Ex. 1003 ¶ 227; Ex. 1037, 9–11)

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

[1.7.3]: determining, based at least in part on the captured biometric information, that the user is alive; and

Petitioner contends that the combination of Stone and the Guidance teaches this limitation. Pet. 71 (citing Ex. 1003 ¶ 229–232).

Petitioner contends that the “Guidance describes that biometric authentication as applied in Stone, includes face recognition that uses facial images from ‘video cameras’ with ‘tests for **liveness** such as blinking eyes.’” Pet. 71 (citing Ex. 1037, 11). Petitioner further contends that “[t]echniques for liveness tests based on facial images from video cameras were wellknown [sic].” *Id.* (citing Ex. 1003 ¶ 230).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

[1.8]: based at least in part on both the user interaction with the transaction icon rendered in the interface and performing the fraud detection analysis, complete the electronic transaction; and

Petitioner contends that the combination of Stone and the Guidance teaches this limitation. Pet. 71 (citing Ex. 1003 ¶¶ 233–236).

Petitioner contends that the combination of Stone and the Guidance completes the electronic transaction by transferring funds at block 318 in Figure 3 of Stone:

based at least in part on both the user interaction with the transaction icon (see [1.6] and performing the fraud detection analysis (see [1.7.1]-[1.7.3]) because the user interaction is the user's indication of continuing/confirming the transaction request, and the transaction request is authorized based on the fraud detection analysis, as well-known in the art.

Id. at 71–72 (citing Ex. 1003 ¶¶ 234–235).

We reviewed the evidence cited by Petitioner which is not disputed by Patent Owner and find it sufficient for institution.

3. *Petitioner's Motivation to Combine and Reasonable Expectation of Success Contentions*

Petitioner contends that the “Guidance is analogous art to the ’656 patent.” Pet. 62 (citing Ex. 1003 ¶ 200).

Petitioner contends that an ordinarily skilled artisan would have understood that the Guidance teaches “‘improved authentication technologies’ for reducing fraud and identity theft and improving customer protection, for service providers of financial transactions whether or not regulated by FFIEC.” Pet. 62 (citing Ex. 1003 ¶ 201; Ex. 1022, 1). Petitioner further contends that an ordinarily skilled artisan would have been motivated to apply the Guidance’s multi-factor, real-time, risk-based authentication teachings to Stone because “Stone had a need for authentication for fraud detection (e.g., with higher levels of security for higher-risk financial transactions), and because the Guidance was a recognized driver for implementing multi-factor authentication by a POSITA as shown in numerous articles and patent disclosures.” *Id.* at 62–63 (citing Ex. 1003 ¶¶ 50, 201).

Petitioner next contends that an ordinarily skilled artisan would have had a reasonable expectation of success in the combination because the implementation of the teachings of the Guidance “would have required only

routine knowledge well within the skill of” an ordinarily skilled artisan. Pet. 63 (citing Ex. 1003 ¶ 202).

We have reviewed Petitioner’s contentions and evidence and find it sufficient for institution. For the reasons discussed below, we find that Patent Owner’s arguments against the combination of Stone and the Guidance do not undercut Petitioner’s showing based on the present record.

Patent Owner’s Contentions

i. Sufficiency of Dr. Jones’s Testimony

Patent Owner contends that we should give no weight to Dr. Jones’s testimony in connection with Petitioner’s motivation-to-combine and reasonable-expectation-of-success arguments. Prelim. Resp. 50. Patent Owner’s arguments are substantially the same as the arguments made against Dr. Jones’s testimony in Ground 1. *Id.*

We reviewed Dr. Jones’s testimony in support of the Petition, and taken as a whole, it is supported sufficiently with evidence and technical reasoning at this stage of the proceeding. Consequently, we do not give his testimony little to no weight because portions of it are repeated in the Petition.

ii. Petitioner’s Explanation for Combining Stone and the Guidance

Patent Owner contends that “Petitioner’s assertions are conclusory and fail to explain *why* a POSITA would have combined Stone and the Guidance.” Prelim. Resp. 52. With respect to Stone, Patent Owner repeats its arguments from Ground 1 that “Stone is not concerned with security of transactions” but “[r]ather it is concerned with providing an improved display . . . that provides a currency display.” *Id.* Patent Owner also argues again that Stone “does not view fraud as a problem that needs to be

addressed with increased security, nor does it even mention electronic payment fraud.” *Id.*

For the Guidance, Patent Owner contends that it “is not concerned with conveying amounts of funds, providing visual representations of currency, or even providing a digital interface. It simply discusses biometrics and security in broad general terms.” *Id.*

Patent Owner next contends that “[t]here is no overlap in the teachings of these references” and characterizes Petitioner’s arguments for combining the teachings of the references as “mashing together two unrelated references that identify limitations of the ’656 Patent’s independent claims without giving anything more than perfunctory statement for *why* a POSITA would have combined them.” Prelim. Resp. 53.

For the following reasons, Patent Owner’s contentions are unavailing.

Regarding the reasons to combine the Guidance’s teachings with Stone’s teachings, as discussed above in connection with Ground 1, 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. 66–67, 71–74; Ex. 1008 ¶¶ 45, 48. Those advantages include “reducing fraud and identity theft and improving customer protection for service providers of financial transactions” resulting from “real-time risk-based authentication for fraud analysis.” Pet. 6, 67; *see* Ex. 1003 ¶¶ 197, 199, 212.

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). 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. 68–69, 71–72; *see* Ex. 1003 ¶¶ 197, 199, 212.

Hence, we disagree with Patent Owner that Petitioner’s motivation-to-combine assertions are “conclusory and fail to explain” why an ordinarily skilled artisan “would have combined Stone and the Guidance.” *See* Prelim. Resp. 52 (emphasis omitted).

iii. Patent Owner’s Assertion that Stone Is Not Analogous Art

Patent Owner relies on its arguments for Ground 1. As discussed above, those arguments are unavailing based on the present record.

Claims 10 and 19

For independent claims 10 and 19, Petitioner relies on its contentions for various limitations of claim 1. *See* Pet. 74, 75–76. With respect to the preamble of claim 10 ([10.0]: *A method, comprising:*), Petitioner argues that to the extent the preamble is limiting, Stone discloses or renders obvious the limitation. *Id.* at 74. With respect to the preamble of claim 19 ([19.0]: *A computer program product embodied in a non-transitory computer readable storage medium and comprising computer instructions for:*), Petitioner argues that to the extent the preamble is limiting, Stone alone or in combination with FFIEC Guidance renders obvious the limitation. *Id.* at 75.

Patent Owner does not provide separate arguments for claims 10 and 19. *See generally* Prelim. Resp.

We reviewed Petitioner’s evidence and arguments for claims 10 and 19 and for the reasons discussed with respect to claim 1 determine that Petitioner has shown a reasonable likelihood that claims 10 and 19 would have been unpatentable over Stone and FFIEC Guidance.

Summary for Claims 1, 10, and 19

For all the foregoing reasons, we determine that Petitioner has shown a reasonable likelihood that claims 1, 10, and 19 would have been unpatentable over Stone and FFIEC Guidance.

4. Claims 4–9 and 13–18

Petitioner sets forth evidence and argument as to why Stone and the Guidance allegedly render claims 4–9 and 13–18 unpatentable. Pet. 73, 74–75.

Patent Owner does not provide separate arguments for these claims. *See generally* Prelim. Resp.

We reviewed Petitioner’s evidence and arguments and determine that Petitioner has shown a reasonable likelihood that these dependent claims would have been unpatentable over Stone and FFIEC Guidance.

G. Grounds 3 and 4: Alleged Obviousness of Claims 2, 3, 11, and 12 over the Combination of Stone, Hoyos, Varghese, and Borovsky; and over the Combination of Stone, FFIEC Guidance, and Borovsky

Petitioner contends claims 2, 3, 11, and 12 would have been obvious over Stone, Hoyos, Varghese, and Borovsky (Ground 3); and over Stone, FFIEC Guidance, and Borovsky (Ground 4). Pet. 76–81. Petitioner supports its contentions with the Declaration of Dr. Jones. Ex. 1003.

Patent Owner does not address these claims in the Preliminary Response. *See generally* Prelim. Resp.

We begin with a brief summary of Borovsky and then address Petitioner’s contentions.

1. Borovsky (Ex. 1041)

Borovsky is titled “Systems and Methods for Remotely Configuring a Mobile Device.” Ex. 1041, code (54). Borovsky “relates generally to systems and methods for remotely configuring a mobile device such as, by way of example and not by way of limitation, a mobile phone.” *Id.* ¶ 13.

Borovsky’s Figure 1 is reproduced below.

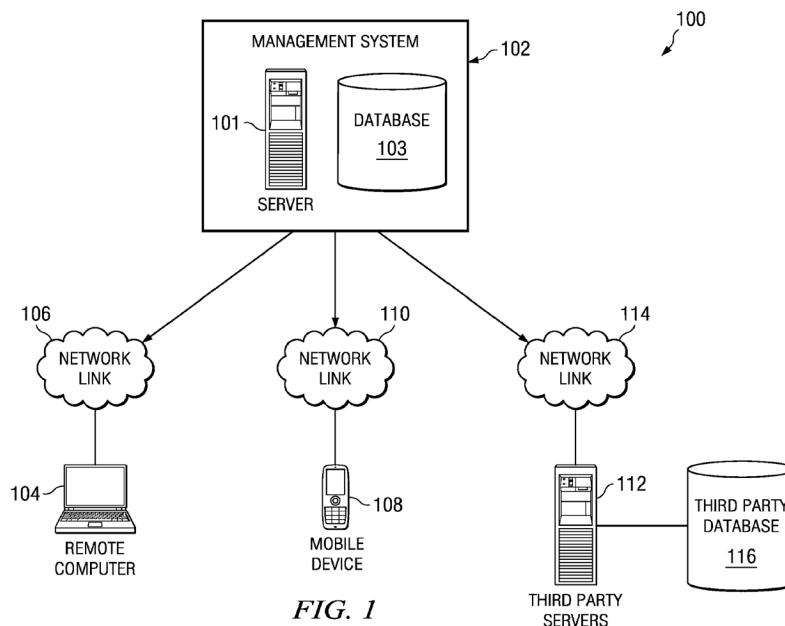


FIG. 1

Figure 1 “illustrates a block diagram of a computer network environment 100,” which “includes a management system 102, a remote computer system 104, a network link 106 by which management system 102 and remote computer system 104 are able to communicate, a mobile device 108, and a network link 110 by which management system 102 and mobile device 108 are able to communicate.” Ex. 1041 ¶ 14.

According to Borovsky, “management system 102 may be configured to present the user interface at remote computer 104 by transmitting, via network link 106, user interface data in the form of, for example, an HTML (Hyper Text Markup Language) document, to a client application (e.g., a web browser) hosted in remote computer 104.” Ex. 1041 ¶ 37. Borovsky describes that “a website affiliated with the management system 102 . . . provides the user interface via the display at remote computer 104 enabling the user to enter, select, update, and/or delete management information and/or configuration information . . . for configuring the mobile device 108.” *Id.* “Management system 102 is further configured to update configuration information for the mobile device 108 based on the management information,” and “send or transmit configuration information to mobile device 108.” *Id.* ¶¶ 37, 39.

Borovsky’s Figure 6 is reproduced below.

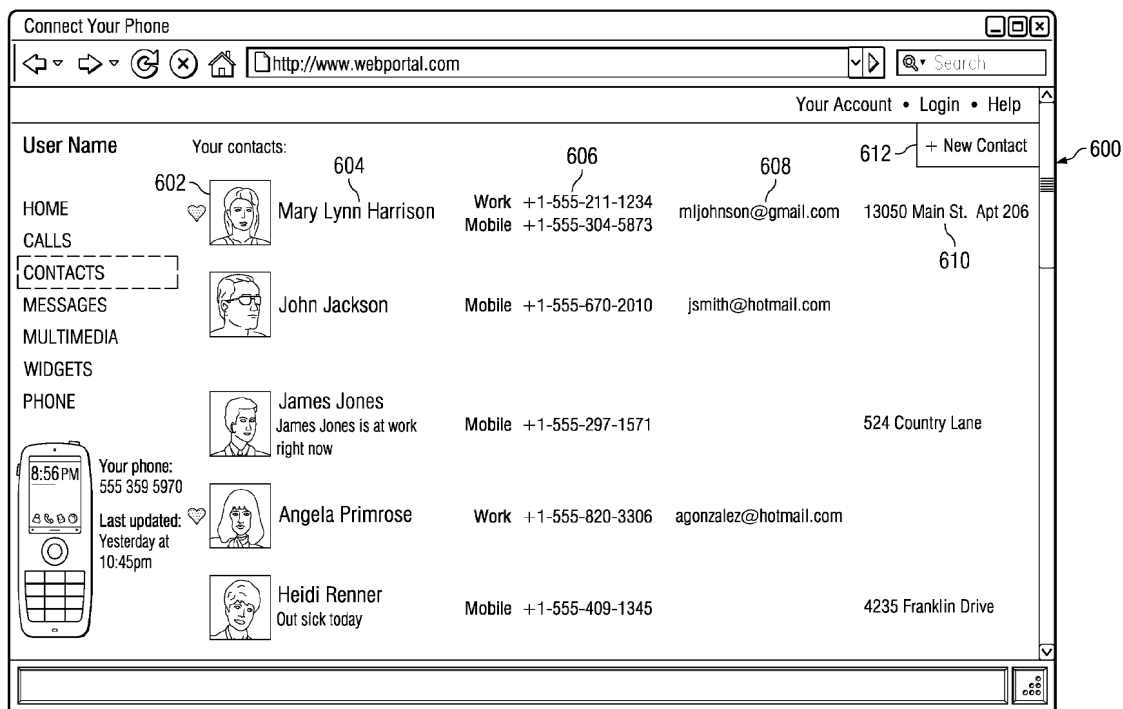


FIG. 6

Figure 6 “illustrates an example interface for viewing and/or editing contact information.” Ex. 1041 ¶ 8. According to Borovsky, the user may “view and manage the contact information updated and aggregated by management system 102 from third party servers 112 via user interface 600 displayable by management system 102 via remote computer 104,” and may also be enabled by user interface 600 “to update the aggregated contact information.” *Id.* ¶ 45. “By way of example, user interface 600 may include picture elements 602 for choosing a picture to be displayed with a particular contact.” *Id.* According to Borovsky, “any or all of elements or fields 602, 604, 606, 608, and 610 may be edited via user interface 600,” and “may also be edited at mobile device 108 whereby the updated data is subsequently pushed to management system 102 where it is then updated at database 103 for subsequent display via interface 600.” *Id.*

2. *Claims 2, 3, 11, and 12*

Petitioner provides a limitation-by-limitation analysis of claims 2, 3, 11, and 12, mapping the prior art to the claim elements. Pet. 79–81 (citing Ex. 1003 ¶¶ 280–287; Ex. 1041 ¶¶ 2, 31–33, 35, 39, 43, 45, 46, Figs. 5–6, claims 3–7). Petitioner also provides contentions concerning reasons to combine Stone and Borovsky and reasonable expectation of success in combination. *Id.* at 77–79.

Patent Owner does not address these claims in the Preliminary Response. *See generally* Prelim. Resp.

We reviewed Petitioner’s evidence and arguments and determine that Petitioner has shown a reasonable likelihood that these dependent claims would have been unpatentable over the combination of Stone, Hoyos,

Varghese, and Borovsky; or the combination of Stone, the Guidance, and Borovsky.

III. CONCLUSION

Based on the present record, we determine that Petitioner demonstrates a reasonable likelihood that it would prevail in establishing that at least one challenged claim of the '656 patent is unpatentable. We, thus, institute an *inter partes* review of all challenged claims of the '656 patent based on all grounds in the Petition. At this stage of the proceeding, we have not made a final determination under 35 U.S.C. § 318(a) with respect to the unpatentability of any challenged claim.⁹

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of the '656 patent is instituted with respect to all challenged claims and grounds set forth in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(a) and 37 C.F.R. § 42.4(b), *inter partes* review of the '656 patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

⁹ Patent Owner is cautioned that any arguments not raised in the Patent Owner Response may be deemed waived. *See In re NuVasive, Inc.*, 842 F.3d 1376, 1379–82 (Fed. Cir. 2016) (holding that a patent owner waived an argument addressed in a preliminary response by not raising the same argument in the patent owner response).

IPR2024-00330
Patent 10,713,656 B1

FOR PETITIONER:

David 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 Kamprath
George Fishback
McKOOL SMITH, P.C.
rkamprath@mckoolsmith.com
gfishback@mckoolsmith.com