Trials@uspto.gov
571-272-7822

Paper 29
Date: July 14, 2025

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*.

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

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 filed a Preliminary Reply ("Prelim. Reply") and Patent Owner filed a Preliminary Sur-reply ("Prelim. Sur-reply). Papers 8, 9. On August 1, 2024, we instituted this *inter partes* review as to all challenged claims and all grounds presented in the Petition. Paper 10 ("Dec.").

After institution, Patent Owner filed a Response to the Petition (Paper 17, "PO Resp.") supported by a Declaration of Dr. Michael T. Goodrich (Ex. 2032). Petitioner filed a Reply ("Pet. Reply"). Paper 19. Petitioner filed a Supplemental Declaration of Dr. Creed Jones with the Petitioner Reply. Ex. 1056. Patent Owner filed a Sur-reply ("Sur-reply"). Paper 20. An oral hearing was held on May 1, 2025, and the transcript is entered into the record. Paper 28 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6. This is a Final Written Decision under 35 U.S.C. § 318(a) as to the patentability of the Challenged Claims of the '656 patent. For the reasons discussed below, we determine Petitioner establishes by a preponderance of the evidence that all Challenged Claims are unpatentable.

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.). 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.

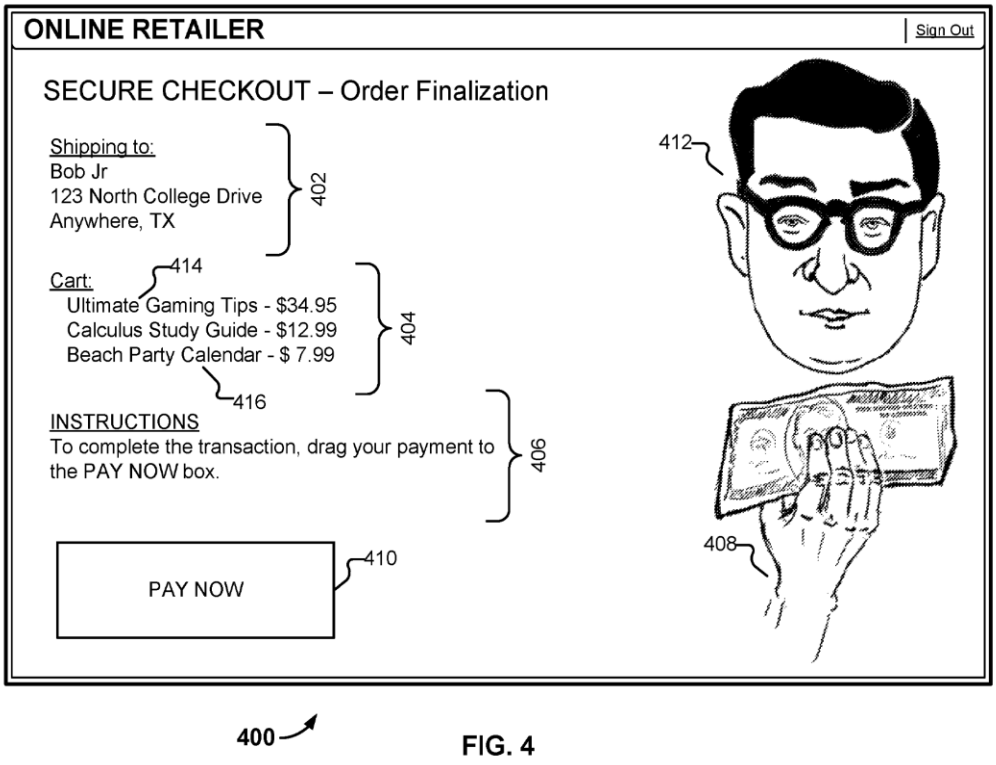

FIG. 4

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.

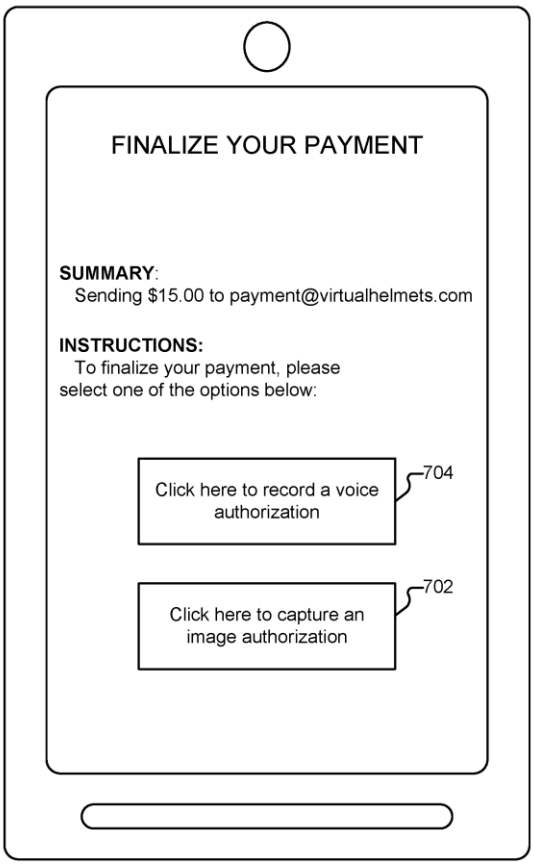

FIG. 7

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):

Ground No.	Claim(s) Challenged	35 U.S.C. §[1]	References/Basis
1	1, 4–10, and 13–19	103(a)	Stone,[2] Hoyos,[3] Varghese[4]
2	1, 4–10, and 13–19	103(a)	Stone, FFIEC Guidance[5]
3	2, 3, 11, and 12	103(a)	Stone, Hoyos, Varghese, Borovsky[6]
4	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. Overview

Petitioner bears the burden of establishing the unpatentability of the challenged claims by a preponderance of the evidence. 35 U.S.C. § 316(e) (2024); 37 C.F.R. § 42.1(d) (2024). This burden of persuasion never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

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.

[7] No evidence of secondary considerations has been presented.

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)).

"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)).

B. 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 has applied Petitioner's definition of the level of skill of a person of ordinary skill in the art. PO Resp. 14.

We apply Petitioner's undisputed level of skill in the art with the exception of the phrase "at least" which injects potential ambiguity into the level of skill, because Petitioner's proposed level of skill appears consistent with the problems addressed in the '656 patent and the prior art.

C. 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 Intell. 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." PO Resp. 14.

We determine that no 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.*, 200 F.3d at 803).

D. 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.

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.

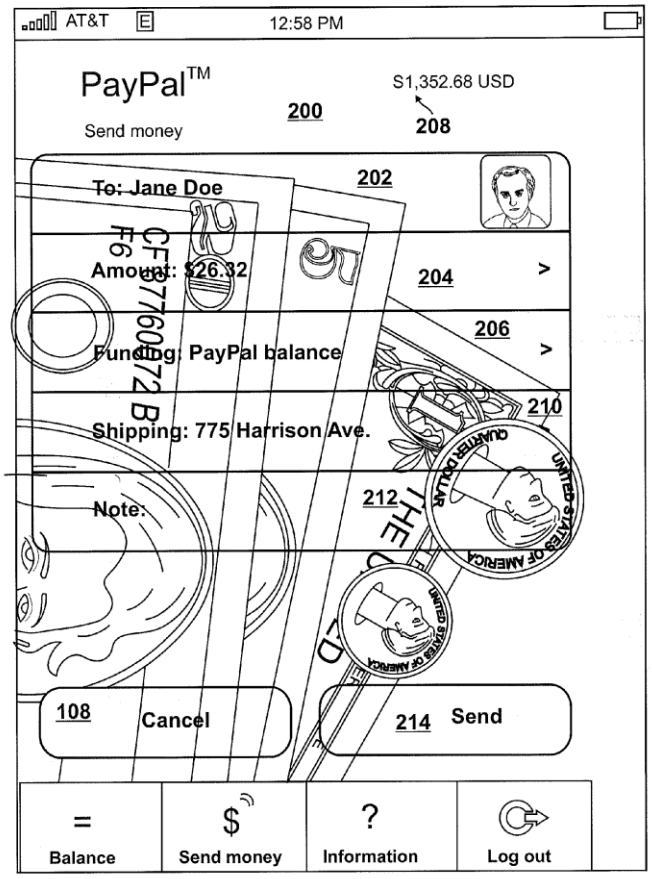

FIG. 2

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.

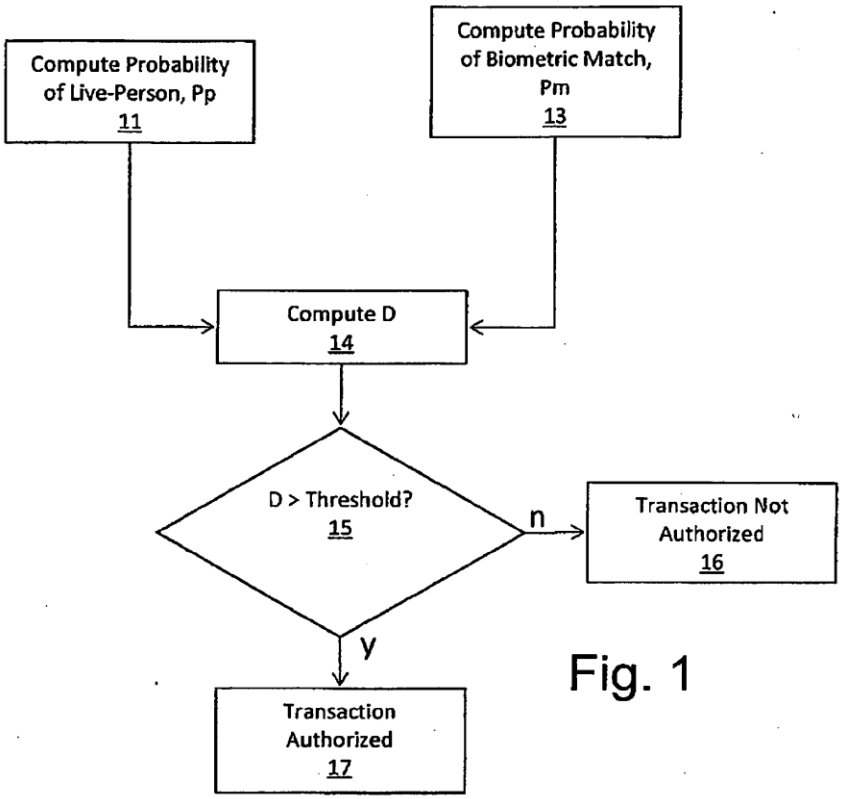

Fig. 1

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, Pp, of a live person being presented, compute [at block] 13 the probability of a biometric match, Pm, 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:

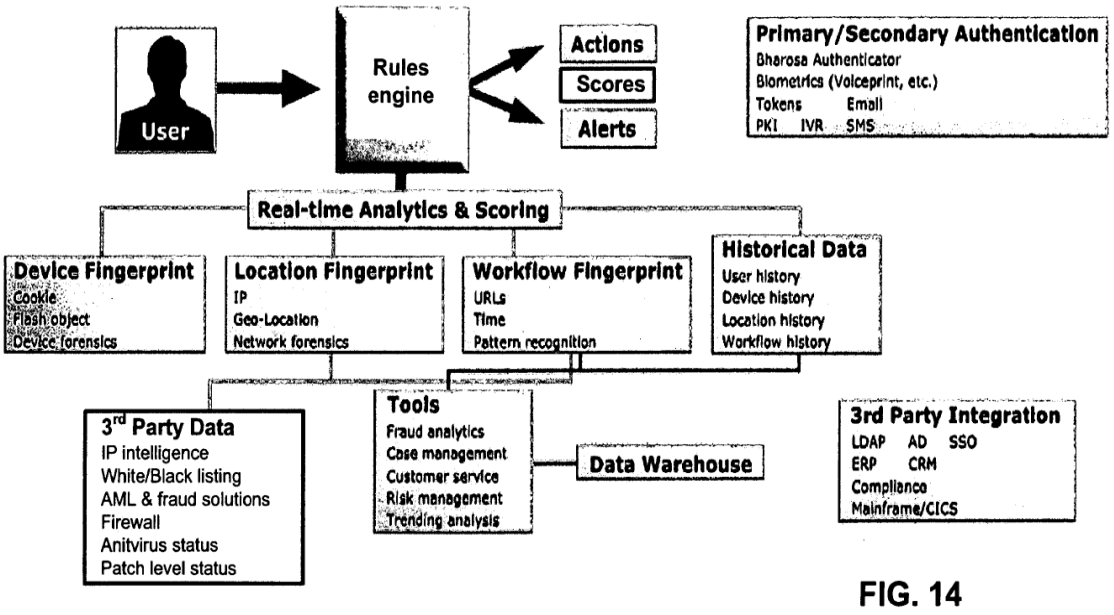

FIG. 14

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. 26–52, 58–61. Petitioner also provides contentions concerning motivation to combine disclosures or embodiments of Stone (*id*. at 13–15); motivation to combine Stone and Hoyos (*id*. at 15–21); motivation to combine Stone, Hoyos, and Varghese (*id*. at 21–26), and reasonable expectation of success (*id*. at 20, 25).

Patent Owner contends that the combination of Stone, Hoyos, and Varghese does not disclose limitations [1.2] and [1.9]. PO Resp. 32, 38. Patent Owner further contends that Petitioner's explanation for motivation to combine Stone, Hoyos, and Varghese is conclusory and insufficient (*id*. at 16); Stone is not analogous art (*id*. at 20); and Stone, Hoyos, and Varghese teach away from each other (*id*. at 23).

With this background, we analyze the parties' respective contentions. We start with Motivation to Combine because the resolution of Patent Owner's arguments concerning limitations [1.2] and [1.9] depend upon our disposition of Motivation to Combine.

Motivation to Combine and Reasonable Expectation of Success

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

[8] For ease of reference, in our analysis, we refer to Petitioner's claim limitation annotations.

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.*):

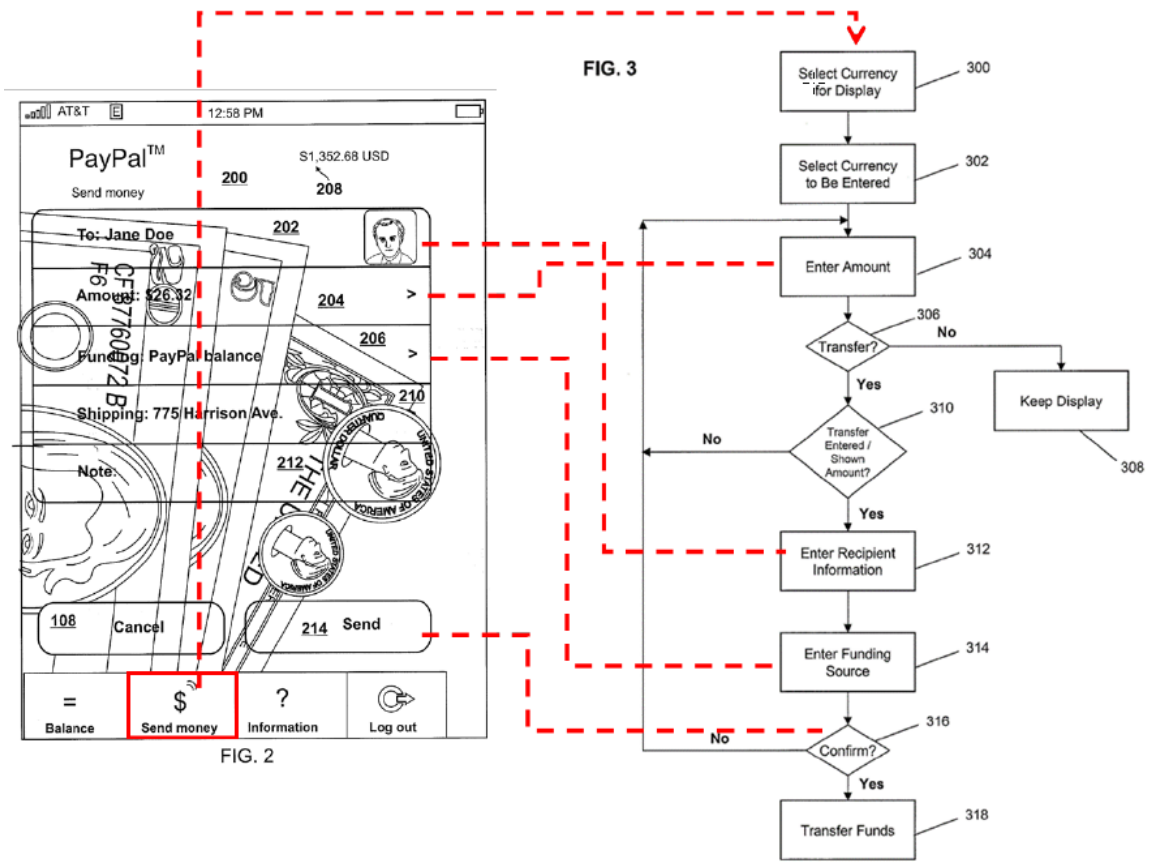

Figure 2, on the left, is "a currency display on a user device" of Stone and Figure 3, on the right, "is a flow chart" of a sample transaction. Ex. 1008

¶¶ 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 element 202 in Figure 2 and block 312 in Figure 3, between element 204 in Figure 2 and block 304 in Figure 3, between element 206 in Figure 2 and block 314 in Figure 3, and between element 214 in Figure 2 and block 316 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 (citing Ex. 1003 ¶¶ 57–58).

Patent Owner does not address Petitioner's contentions. *See generally* PO Resp. 16–31.

We have reviewed Petitioner's contentions and evidence and find that an ordinarily skilled artisan would have been motivated to combine the teachings of Figures 2 and 3 of Stone for the reasons stated by Petitioner. *See Bos. Sci. Scimed, Inc. v. Cordis Corp.*, 554 F.3d 982, 991 ("Combining two embodiments disclosed adjacent to each other in a prior art patent does not require a leap of inventiveness.").

ii. Whether Stone is Analogous Art

Petitioner contends that Stone is "(1) in the same field of endeavor (computer network applications for financial transactions); or (2) reasonably pertinent to a problem with which the inventor of the '656 patent was involved (e.g., fraud detection in electronic financial transactions)." Pet. 12–13 (citing Ex. 1001, code (54), 1:26–30); Ex. 1008, code (54), ¶¶ 1–4, 45).

Patent Owner asserts that Stone does not satisfy either prong of the analogous-art test. PO Resp. 21.

Patent Owner first contends that "Stone is not in the same field of endeavor as the '656 Patent." PO Resp. 21 (citing Ex. 2032 ¶ 64). 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.* According to Patent Owner, Stone "is not at all concerned with actually processing transactions, improving transaction processing, or user authentication" but "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.* at 7, 21 (citing Ex. 1008 ¶ 2; Ex. 2032 ¶¶ 64–65).

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." PO Resp. 23.

Petitioner, in turn, argues that "Stone is analogous art, because Stone explicitly describes its implementation in the context of PayPal[9], which is in the same field of endeavor as the ['656] Patent." Pet. Reply 5 (citing Ex. 1008, Fig. 2). Petitioner further argues Stone "is pertinent to the particular problem of making an electronic financial transaction seem 'more concrete' because 'physical cash is a concrete tangible item while a digital payment for a digital good is a more abstract concept.'" *Id.* (citing Ex. 1001,

[9] According to Petitioner, "PayPal was a widely used online payment platform allowing users to send and receive money and transfer funds between bank accounts and credit cards." Pet. Reply 5 (citing Ex. 1056 ¶ 10).

4:28–30, 4:62–67, 5:16–18; Ex. 1008, Figs. 1–2; Ex. 1056 ¶ 11); *see also* Prelim. Reply 3 ("Stone discloses secure transactions with multi-factor authentication (e.g., '***username, password,' 'biometric id,'*** and/or banking ***'user account numbers, security information'***) for fraud prevention.") (citing Ex. 1008 ¶¶ 45–46, Fig. 2).

Patent Owner responds that "Petitioner's proposed field of endeavor 'computer network applications for financial transaction' . . . is too broad, such that it would be beyond what a POSITA would reasonably be expected to look for to find a solution to the problem facing the inventor, i.e., fraud detection." Sur-Reply 4 (citing PO Resp. 20–21).

For the following reasons, we find that Stone is analogous art.

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 addresses the problem of making an electronic financial transaction seem "more concrete" by disclosing an electronic device with a display that shows the "actual currency" for an electronic financial transaction. Ex. 1008 ¶¶ 6, 8, 10–11, 16, 22–25, 31, 33, 39, code (57), Figs. 1–2; *see* Ex. 1003 ¶ 101; Ex. 1056 ¶ 11. Stone explains that "[t]his gives the user a visual representation of the amount, which reinforces the value of the amount." Ex. 1008 ¶ 16; *see* Ex. 1003 ¶ 38.

The '656 patent discloses use of biometrics to prevent fraud. *See e.g.*, Ex. 1001, 6:45–51. Claim 1 of the '656 patent recites "performing a comparison based at least in part on the stored biometric information and the captured biometric information." *Id.* at 14:21–23.

Stone discloses user device 408 stores personal information of a user including "a user name, password, photograph image, and biometric id." Ex. 1008 ¶ 45.

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. 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. Dr. Jones provides citations to the '656 patent and to Stone in support of his testimony. Ex. 1003 ¶ 53; Ex. 1056 ¶¶ 10–11. Based on our review of his testimony and the citations to the '656 patent and Stone, we find that his testimony is entitled to weight on the question of whether Stone is analogous art to the '656 patent.

Based on the evidence cited by Petitioner as well as Dr. Jones's testimony and for all the foregoing reasons, we find that a preponderance of the evidence establishes that Stone qualifies as analogous art to the '656 patent because it is at least "reasonably pertinent" to the problems of using biometric id to prevent fraud and making electronic transactions more concrete to a user.

iii. Combination of Stone and Hoyos

Petitioner 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." Pet. 15 (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 further contends that an ordinarily skilled artisan "would have been motivated to implement

Hoyos' spoofing-resistant biometric authentication for fraud detection in the system of Stone for 'improved deterrent against attempted fraudulent transactions, and decreased rejection of valid customers.'" *Id.* (citing Ex. 1003 ¶ 62).

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).

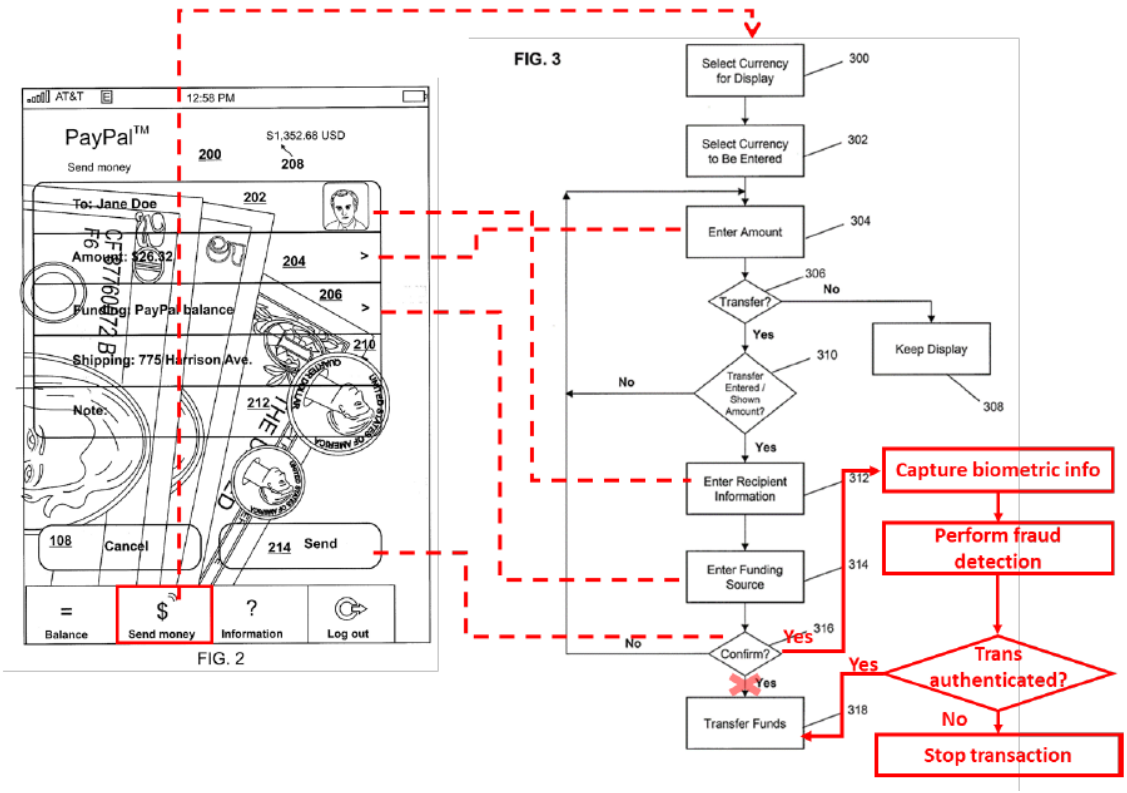

Figure 2, on the left, is "a currency display on a user device" of Stone and Figure 3, on the right, "is a flow chart." Ex. 1008 ¶¶ 11–12. Petitioner annotates the figures with broken red lines between the "$Send Money" icon in Figure 2 and block 300 in Figure 3, between element 202 in Figure 2 and

block 312 in Figure 3, between element 204 in Figure 2 and block 304 in Figure 3, between element 206 in Figure 2 and block 314 in Figure 3, and between element 214 in Figure 2 and block 316 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 asserts that Stone's system based on a client-server model and Hoyos's biometric authentication are complementary. Pet. Reply 6. Petitioner also asserts that an ordinarily skilled artisan would have adapted or applied Hoyos's biometric authentication to "function within Stone's system (either on the client or on a server), achieving secure authentication without undermining the system's architecture." *Id.* (citing Ex. 1003 ¶¶ 67–68; Ex. 1016 ¶¶ 40, 42; Ex. 1038, 64 Ex. 1056 ¶ 15; Pet. 20–21).

As support, Petitioner quotes the following statements in a 2005 paper titled "Secure Biometric Authentication for Weak Computational Devices" and co-authored by Dr. Goodrich: "[t]here are two broad approaches: The one where the comparison is done at the remote server, and the one where the comparison is done at the client end (the portable device where the biometric measurement is done). Most of the recent work has focused on the second category." Pet. Reply 7 (emphases omitted) (quoting Ex. 1055, 2); *see* Ex. 1055, 2; Ex. 1056 ¶ 15.

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).

Patent Owner contends that Petitioner's "assertions do not explain *why* a [person of ordinary skill in the art] would have combined the references." PO Resp. 17. According to Patent Owner, "Stone does not identify electronic payment fraud as a problem needing to be solved," "never mentions fraud," and "is not concerned with the actual processing of transactions." *Id.* (citing Ex. 1008 ¶ 23). Patent Owner further contends that because Stone "[does not] discuss any technique for preventing fraud, like those in Hoyos," an ordinarily skilled artisan "would not have been motivated to apply Hoyos's authentication techniques to Stone's teachings." *Id.* (citing Ex. 2032 ¶¶ 57–58).

Patent Owner concedes that Stone discloses the use of personal information including user name, password and biometric id but argues that it does not disclose that such information "is used for performing some form of authentication or fraud detection, specifically biometric based fraud detection." PO Resp. 17–18 (citing Ex. 2032 ¶¶ 58–60.)

Patent Owner next contends that "Hoyos is not concerned with improving a user display, specifically an electronic currency display (like that of Stone), or improving a user's experience based on providing a richer interface (like Stone)." PO Resp. 18–19. According to Patent Owner, "[n]othing in Hoyos would lead a [person of ordinary skill in the art] to combine its biometric authentication methods with an interactive interface, particularly a currency display like the one Stone provides." *Id.* at 19 (citing Ex. 2032 ¶¶ 57–61).

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

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). Dr. Goodrich does not dispute Dr. Jones's testimony on this point but parrots the argument in the Patent Owner Response that "Stone does not say that user identifier 418 is used to perform user authentication or fraud detection." Ex. 2032 ¶ 59. We credit the testimony of Dr. Jones in the absence of contrary evidence by Patent Owner. Consequently, Patent Owner's argument that Stone does not disclose using biometric id during the processing of transactions or as a technique for preventing fraud is unavailing.

Patent Owner's argument that Hoyos is not concerned with improving an electronic display or a user's experience (PO Resp. 18) is also unavailing. 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).

Patent Owner next contends that "Stone and Hoyos teach away from each other and are incompatible because [their inventions] are directed to different computing environments." PO Resp. 24.[10] In support of this contention, Patent Owner argues that Stone "requires a client-server structure." *Id.* (citing Ex. 1008 ¶¶ 40–48, Fig. 4); *id.* at 25 ("Stone provides no basis for applying Hoyos's authentication techniques locally because Stone discloses only a client-server structure for implementing its currency display." (citing Ex. 1008 ¶¶ 45–48, Fig. 4)). Patent Owner attempts to draw a contrast with Stone by arguing that "Hoyos's disclosed authentication methods are employed locally on the device with no mention of a server structure." *Id.* at 24 (citing Ex. 1013 ¶¶ 16–22, claim 4; Ex. 2032 ¶ 68).

Patent Owner next contends that "[e]mploying local biometric authentication within Stone's client-server structure also does not make sense to a [person of ordinary skill in the art]." PO Resp. 25 (citing Ex. 2032 ¶ 70). Patent Owner argues Stone displays the user account balance before the user completes the transaction which "would require some communication with the payment server where the user's account information must be stored . . . well before the end of the transaction where Petitioner inserts the Hoyos 'authentication process.'" *Id.* (citing Ex. 1008 ¶¶ 47–48, Fig. 4). According to Patent Owner, doing so "would then require the on-device authentication *after* the device already transferred information in communication with payment server 408, which is redundant." *Id.* at 25–26 (citing Ex. 2032 ¶¶ 70–71).

[10] Patent Owner relies on the same arguments discussed herein to support a teaching away argument and to more generally argue that a person of ordinary skill in the art would not have been motivated to combine Stone and Hoyos. PO Resp. 27 (citing Ex. 2032 ¶¶ 55–73).

Patent Owner next contends that implementing Hoyos's authentication techniques on "a client-server structure would . . . undermine Hoyos's stated goals of improving speed, accuracy, and security of biometric authentication." PO Resp. 26. Patent Owner points to Dr. Jones's testimony concerning the benefits of Hoyos's authentication techniques. *Id.* at 26–27 (citing Ex. 1003 ¶ 68). Patent Owner argues that "[l]atency is increased due to the time communicating with the server" and "[r]esources would not be efficiently used as processing power on the device would be sacrificed." *Id.* at 27 (citing Ex. 2032 ¶¶ 71–73).

Petitioner, in turn, argues that Patent Owner "fail[s] to identify anything in prior art that criticizes, discredits, or otherwise discourages the claimed invention." Pet. Reply 6 (citing Ex. 1056 ¶¶ 13–14). Petitioner further argues that "Stone's client-server model and Hoyos' authentication methods are complementary" and an ordinarily skilled artisan would have "adapt[ed] Hoyos' biometric methods to function within Stone's system (either on the client or on a server), achieving secure authentication without undermining the system's architecture." *Id.* (citing Pet. 20–21; Ex. 1003 ¶¶ 67–68; Ex. 1016 ¶¶ 40, 42, 76; Ex. 1038, 64; Ex. 1016 ¶ 15). Petitioner also argues that implementing "biometric authentication in a client-server architecture could be performed on a server or on a remote client, and that either approach has advantages and disadvantages in specific applications" and the combination of Stone and Hoyos would yield "the benefits of improved security and privacy, and '[s]uch an approach is convenient as it is relatively simple and cheap to build biometric authentication systems supporting biometric storage at the client end able to support local matching.'" *Id.* at 7 (citing Ex. 1038, 64; Ex. 1056 ¶ 16).

For the following reasons, we do not agree with Patent Owner that Stone and Hoyos teach away from each other or that an ordinarily skilled artisan would not have been motivated to combine Stone and Hoyos.

First, "[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). A reference does not teach away "if it merely expresses a general preference for an alternative invention but does not 'criticize, discredit, or otherwise discourage' investigation into the invention claimed." *Id.* (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).

Patent Owner's argument that the references teach away is unavailing because Patent Owner does not direct us to any disclosure in Hoyos that criticizes, discredits, or discourage implementing its biometric fraud prevention in a client-server architecture such as in Stone. PO Resp. 23–27; Sur-reply 4–7.

To the extent that Patent Owner argues that an ordinarily skilled artisan would not have been motivated to combine Stone and Hoyos due to "different computing environments" i.e., Stone's client-server and Hoyos local authentication methods, (PO Resp. 24), this argument is also unavailing. The Petition contemplates "implementing fraud detection

analysis locally using the user device or remotely." Pet. 20 (citing Ex. 1003 ¶ 67; Ex. 1016 ¶¶ 40, 42, 76); *see* Pet. Reply 6. Additionally, the argument is unavailing because it appears to be arguing that Petitioner has not shown that Stone can be bodily incorporated with Hoyos. *See In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012) ("It is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements.").

Patent Owner's argument that it would not make sense to an ordinarily skilled artisan to implement "local biometric authentication within Stone's client-server structure" (PO Resp. 25) ignores Petitioner's arguments and explanations for the combination. We agree with Petitioner that "Stone's client-server model and Hoyos' authentication methods are complementary" and that an ordinarily skilled artisan would have adapted or applied Hoyos's biometric authentication to "function within Stone's system (either on the client or on a server), achieving secure authentication without undermining the system's architecture." Pet. Reply 6 (citing Ex. 1003 ¶¶ 67–68; Ex. 1016 ¶¶ 40, 42; Ex. 1038, 64 Ex. 1056 ¶ 15; Pet. 20–21). We also agree with Petitioner that "'Biometric authentication can be implemented through systems performing the matching either on the server or on the client side,' [recognizing] 'security and privacy problems' and CPU-intensiveness of server side implementation, and 'relatively simple and cheap' with security and privacy benefits of client side implementation." *Id.* at 6–7 (quoting Ex. 1038, 64). Petitioner's arguments are supported by Dr. Jones's testimony, Exhibit 1016, Exhibit 1038, and Exhibit 1055, i.e., the 2005 paper titled "Secure Biometric Authentication for Weak Computational Devices" co-authored by Dr. Goodrich (discussed above).

Patent Owner's argument (PO Resp. 26) that implementing Hoyos's authentication techniques in Stone would allegedly undermine certain goals of Hoyos is also unavailing. We agree with Petitioner that "[d]epending on whether the matching of the biometric template is executed – at the server or at the client – different security problems arise" and that an ordinarily skilled artisan would have been motivated to implement Hoyos's biometric authentication techniques on the client side to "improve[] security and privacy" and because "it is relatively simple and cheap to build authentication systems supporting biometric storage at the client end able to support local matching." Pet. Reply 7 (citing Ex. 1038, 64; Ex. 1056 ¶ 16); Ex. 1003 ¶¶ 67–68. The fact that there may be disadvantages to the combination, as Patent Owner asserts, does not obviate Petitioner's stated reasons for the combination. *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.").

In summary, after reviewing the parties' competing contentions and all the evidence in the record, for the foregoing reasons, we find that a preponderance of the evidence supports Petitioner's position that an ordinarily skilled artisan would have been motivated to combine Stone and Hoyos. Ex. 1003 ¶¶ 59–69; Ex. 1056 ¶¶ 15–16.

iv. Combination of 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 an ordinarily skilled artisan

> would have implemented the multifactor authentication such that, together with the biometric authentication as taught by Hoyos ("Something a person is"/ "something you are") physical location authentication ("Something a person has"/"something you have") as taught by Varghese is used for benefits including 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. 1016 ¶ 43; 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)):

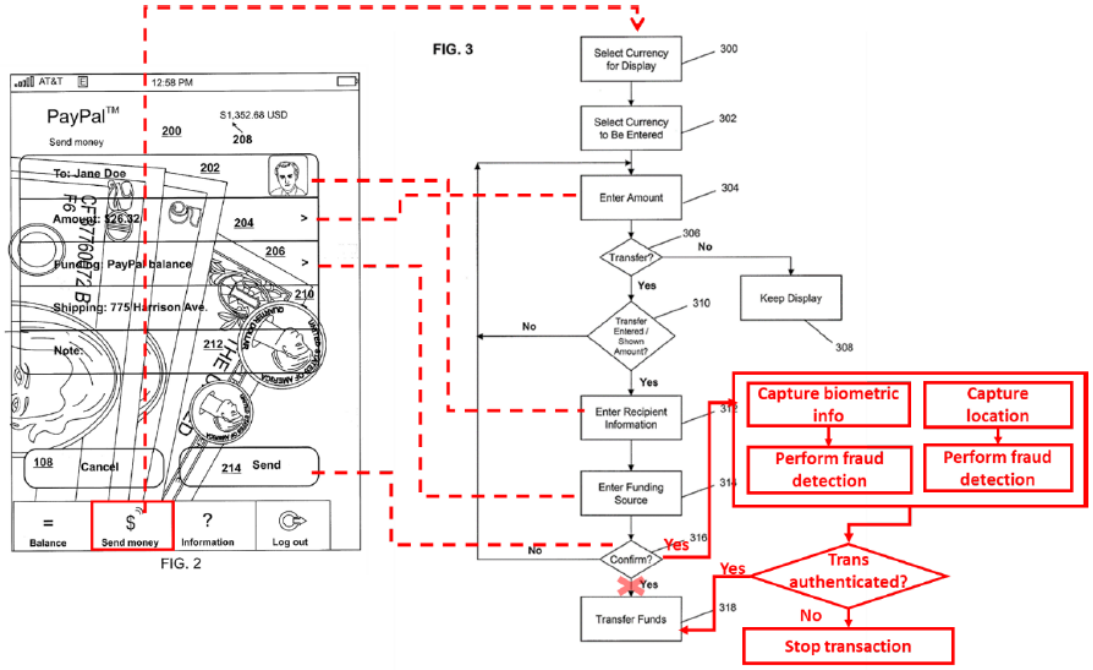

Figure 2, on the left, is "a currency display on a user device" of Stone and Figure 3, on the right, "is a flow chart." Ex. 1008 ¶¶ 11–12. Petitioner annotates the figures with broken red lines between the "$Send Money" icon in Figure 2 and block 300 in Figure 3, between element 202 in Figure 2 and block 312 in Figure 3, between element 204 in Figure 2 and block 304 in Figure 3, between element 206 in Figure 2 and block 314 in Figure 3, and between element 214 in Figure 2 and block 316 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, which **is at least after** the user interaction with the icon (e.g., user clicking the '$Send money' icon of

Fig. 2) to initiate the transaction request, and after user interaction with icons to continue . . . and confirm . . . the transaction request." Pet. 24 (citing Ex. 1003 ¶¶ 74–75; Ex. 1010 ¶¶ 91, 97–99, 148, Fig. 14, Table 10; Ex. 1015, Fig. 4; Ex. 1016 ¶¶ 36, 43, 73, Fig. 3; Ex. 1035, 4:60–62, 4:66–67). 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.* Petitioner next contends that an ordinarily skilled artisan would have "understood that the fraud detection analysis based on location data could be implemented with the alternative design choices of implementing fraud detection locally using the user device or remotely (e.g., by sending the location data to a payment provider device, or another remote device) in the system of Stone." *Id.* at 24–25 (citing Ex. 1003 ¶ 78; Ex. 1016 ¶¶ 40, 42, 76; Ex. 1038, 64). 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).

Patent Owner first contends that "Varghese amplifies the disconnect between Stone and Hoyos regarding the client and server distinction." PO Resp. 27. According to Patent Owner, "for the reasons explained above in the [ ] disparate structures of Stone and Hoyos, it would not make sense to combine techniques performed using a client-server structure (Varghese) with techniques performed only on a client device (Hoyos) to achieve the fraud analysis." *Id.* (citing Ex. 2032 ¶ 74)[11]; Sur-reply 7.

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." PO Resp. 28 (citing Ex. 1010 ¶ 22). Patent Owner further contends that "[t]he software-only goal of Varghese requires implementation through a client-server structure." *Id.* (citing Ex. 2032 ¶¶ 75–76). According to Patent Owner, "[t]he hardware-based biometrics collection and authentication techniques described in Hoyos conflict with Varghese's stated goal of providing a

[11] Patent Owner presents this argument under the heading of "Stone, Hoyos, and Varghese teach away from each other." PO Resp. 23. Patent Owner does not direct us to any disclosure in Varghese that allegedly criticizes, discredits, or discourages the claimed invention and, thus, any teaching away argument is unavailing. *See id.* at 27–31. Consequently, we consider whether Patent Owner's Varghese arguments support its contention that based on the teachings of Varghese, an ordinarily skilled artisan "would not have been motivated to collect location data . . . to authenticate an *electronic transaction* . . . particularly at the last step." *Id.* at 31.

'purely software based solution to identify theft' . . . a [person of ordinary skill in the art] would not have been motivated to look to Hoyos to improve or alter the system disclosed by Varghese, specifically to reach the claimed solution of the '656 Patent claims." *Id.* at 29 (citing Ex. 2032 ¶ 76).

Patent Owner next contends that Petitioner has not established that an ordinarily skilled artisan "would have been motivated to add Varghese's collection of location information to the transaction flow laid out in Stone, particularly at the final confirmation stage." PO Resp. 29 (citing Ex. 2032 ¶ 77). Patent Owner argues that during a pre-authentication phase, Varghese collects "information related to the user and the user's device to authenticate a user logging into a web application—focusing heavily on information collected from the user's device (e.g., device fingerprint [ ] collection of IP address information among other things)." *Id.* at 30 (citing Ex. 1010 ¶ 74). Patent Owner further argues that during a post-authentication phase, Varghese teaches "completing monetary *electronic transactions*, which are authenticated using a user's transaction history and historic workflow." *Id.* at 31 (citing Ex. 1010 ¶ 65; Ex. 2032 ¶ 78).

Patent Owner also contends that Varghese does not disclose collecting location data during post-authentication. *See* Tr. 104:3–5, 104:23–105:3. According to Patent Owner, location data used for post-authentication was already collected for pre-authentication, not newly collected for post-authentication. *See id.* According to Patent Owner, based on these teachings, 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 at the last step of the transaction as Petitioner claims." PO Resp. 31.

In the Petitioner's Reply, Petitioner responds to Patent Owner's "purely software-based solution" contention by arguing that "Varghese describes a 'purely software based solution to identify theft that ***does not require hardware devices to be issued and maintained***." Pet. Reply 8 (citing Ex. 1010 ¶ 22). Petitioner argues that the cited portion of "Varghese does not exclude sensors for capturing biometrics" but, according to Petitioner, "refers to tokens associated with the 'something the user has' factor (e.g., password-generating token)." *Id.* (citing Ex. 1037, 8–9). According to Petitioner, "Varghese explicitly describes use of sensor-based biometrics including 'obtaining biometric identification information (e.g., fingerprints, retinal scans, or the like)." *Id.* at 9 (citing Ex. 1010 ¶ 79). Further, Petitioner argues that "some biometric modalities can make use of sensors that are already part of the client system, such as webcams, microphones and fingerprint sensors for local login." *Id.* (citing Ex. 1056 ¶ 18).

Petitioner also argues that Patent Owner "mischaracterizes Varghese's collecting location data as **only** a pre-authorization technique for user login requests, and not a technique for the post-authentication for completing monetary electronic transactions." Pet. Reply 9 (citing PO Resp. 30; Ex. 1056 ¶ 19). According to Petitioner, "Varghese explicitly describes capturing real-time contextual information including capturing real-time physical location information in 'post-authentication.'" *Id.* (citing Ex. 1008 ¶ 19; Ex. 1056 ¶ 20).

Petitioner next contends the entry in Table 10 of Varghese labelled "Transaction from an un-registered device/location or frequently used fraud device/location" "illustrates business policies using real-time location data for the authentication for completing the electronic transaction." Pet. Reply 10 (citing Ex. 1008, Table 10; Ex. 1056 ¶¶ 21–22).

For the following reasons, we find that Petitioner establishes that an ordinarily skilled artisan would have been motivated to combine Stone, Hoyos, and Varghese with a reasonable expectation of success.

Petitioner identifies reasons that would have prompted an ordinarily skilled artisan to combine Varghese's "multifactor real-time authentication" including "location authentication for user transaction requests" with the Stone-Hoyos system in the way Petitioner proposes. *See* Pet. 21–24. Dr. Jones's testimony supports Petitioner's positions. *See* Ex. 1003 ¶¶ 69–79; Ex. 1056 ¶¶ 17–22.

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

(1) "detecting and preventing access attempts from locations commonly associated with cyber threats";

(2) "providing cross-checking with a user location for a transaction request"; and

(3) "providing additional security without significant additional inconvenience to the user."

See Ex. 1003 ¶ 71; Pet. 22–23.

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

(1) benefits similar to those produced by implementing Hoyos's biometric authentication after a user confirms a user transaction request, e.g., from performing "risk-based contextual authentication . . . based on the transaction and assessed risk for improved fraud detection"; and

(2) additional benefits, e.g., from performing "fraud detection based on whether the two locations (captured before . . . and after confirmation at block 316 [in Stone's Figure 3]) match, for improved security."

See Pet. 18, 24; Ex. 1003 ¶¶ 65, 76. Hence, we disagree with Patent Owner that an ordinarily skilled artisan "would not have been motivated to collect location data (a pre-authentication technique for user login requests) to authenticate an electronic transaction [post-authentication request]." *See* PO Resp. 31 (bracketed text added by Patent Owner) (emphasis omitted).

Additionally, we disagree with Patent Owner that when post-authentication according to Varghese uses location data, the location data was already collected for pre-authentication, not newly collected for post-authentication. *See* Tr. 104:3–5, 104:23–105:3. Varghese discloses "real-time risk scoring" for "each online login and transaction," i.e., "at login and in session," to "increase authentication security in real time." Ex. 1010 ¶¶ 38–39; *see* Ex. 1003 ¶ 186. Evaluating "in-session characteristics" (post-authentication) of each transaction "ensure[s] fraud detection and transactional integrity." Ex. 1010 ¶ 38. For example, post-authentication

may apply to "an existing user making a request that needs particular authentication," e.g., a request involving "high risk or potential fraud." *Id.* ¶¶ 38, 79.

Varghese explains that "real-time risk scoring" depends on, among other things, location data. Ex. 1010 ¶¶ 77, 88, 109, 140, 142, claim 31 (reciting an "access policy" based on "risks related to the current location of the user device" and "risk related to the current transaction"); *see* Ex. 1003 ¶¶ 46, 186. Varghese's analytics-and-scoring system may collect location data from "geolocation data services providing [the] likely geographical source of the current request" during "the course of a valid already-authenticated session." Ex. 1010 ¶¶ 77, 142, 148, claim 14 (reciting "a device geolocation data provider"). For instance, a user transaction request that involves "an amount of money over a certain threshold" or "large amounts of money" ("a high-value transaction") may "invoke a higher security authentication." Ex. 1010 ¶¶ 74–75, 142, 148. Moreover, one of Varghese's model rules focuses on location when a transaction actually occurs by specifying "Transaction from an un-registered device/location or frequently used fraud device/location." *Id.* ¶ 110; *see* Ex. 1003 ¶ 186.

Further, Varghese's Figure 14 depicts an "exemplary functional configuration" with "Real-time Analytics & Scoring" for authenticating a user transaction request based on fingerprints that are "processed and scored in real-time" by a rules engine. Ex. 1010 ¶¶ 91, 97, Fig. 14; *see* Ex. 1003 ¶ 46. The fingerprints include "a location fingerprint, a device fingerprint, a workflow fingerprint, and an historical data fingerprint." Ex. 1010 ¶ 91, Fig. 14; *see* Ex. 1003 ¶ 186. Figure 14 illustrates a "Location Fingerprint"

including "IP, Geo-Location, Network forensics." Ex. 1010, Fig. 14; *see* Ex. 1003 ¶ 186.

An ordinarily skilled artisan would have understood that real-time authentication according to Varghese includes "both real-time capture and real-time analysis of authentication data," including location data. Ex. 1003 ¶ 114; *see* Ex. 1010 ¶¶ 38–39, 74–75, 77, 79, 88, 91, 97, 109, 140, 142, 148, claim 14, Fig. 14; Ex. 1056 ¶¶ 19–20.

As for Varghese's disclosure about providing a "purely software based solution to identity theft that does not require hardware devices to be issued and maintained," we agree with Petitioner that the disclosure concerns "tokens associated with the 'something the user has' factor (e.g., password-generating token)." *See* Pet. Reply 8; Ex. 1056 ¶ 18. Varghese also discloses using hardware-based biometric sensors, e.g., for "obtaining biometric identification information (e.g., fingerprints, retinal scans, or the like), or obtaining voice prints, or the like." Ex. 1010 ¶ 79; *see* Ex. 1056 ¶ 44. Additionally, Varghese's Figure 14 depicts "Primary/Secondary Authentication" including "Biometrics (Voiceprint, etc.)." Ex. 1010, Fig. 14; *see* Ex. 1003 ¶ 186. Varghese's disclosure about using hardware-based biometric sensors demonstrates that Varghese's analytics-and-scoring system accommodates biometric sensors as disclosed in Hoyos. *See* Ex. 1010 ¶ 79; Ex. 1056 ¶ 18.

Patent Owner's assertion that an ordinarily skilled artisan "would not have been motivated to look to Hoyos to improve or alter the system disclosed by Varghese" to yield the claimed inventions mischaracterizes the proposed combination. *See* Pet. 21–24; PO Resp. 29. Petitioner does not propose modifying Varghese's analytics-and-scoring system based on

Hoyos's teachings. *See* Pet. 21–24. Rather, Petitioner proposes modifying Stone's system for financial transactions based on Hoyos's teachings and Varghese's teachings. *See id.*

Patent Owner's assertion about problems "using a client-server structure (Varghese) with techniques performed only on a client device (Hoyos) to achieve" the claimed fraud analysis lacks merit for the reasons discussed above for the Stone-Hoyos combination. *See* PO Resp. 28.

v. Reasonable Expectation of Success

For the reasons stated by Petitioner and supported by Dr. Jones's testimony, we agree with Petitioner that an ordinarily skilled artisan "would have reasonably expected to succeed in configuring Stone-Hoyos-Varghese to leverage Varghese's multifactor real-time authentication functionality since its implementation would have required only routine knowledge well within" the artisan's skill. *See* Pet. 25–26; Ex. 1003 ¶¶ 77–78.

vi. Summary of Motivation to Combine/Reasonable Expectation of Success

For all the foregoing reasons, we find that an ordinarily skilled artisan would have been motivated to combine the teachings of Stone, Hoyos, and Varghese with a reasonable expectation of success.

vii. Claim 1

[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 that Stone 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).

Petitioner next refers to its motivation to combine contentions discussed above and contends that an ordinarily skilled artisan "would have been motivated to implement various steps for an electronic transaction (e.g., steps of [1.2]–[1.8] discussed below) **locally** (e.g., on the user device of Stone) or remotely (e.g., on the service provider of Stone)." Pet. 30.

Petitioner further contends that an ordinarily skilled artisan "would have been motivated to implement the authentication steps (including capturing data and fraud detection analysis based thereupon) locally for the benefits including reduced latency, offline analysis capabilities, enhanced privacy, efficient resource utilization, customization for device characteristics, improved security." *Id.* at 30–31 (citing Ex. 1003 ¶ 88; Ex. 1015, 4:4–10, Fig. 3; Ex. 1016 ¶¶ 40, 42, 76).

Patent Owner does not dispute Petitioner's contentions for this limitation. PO Resp. 15–40.

We have reviewed Petitioner's evidence and explanations and find that the combination of Stone and Hoyos teaches this limitation.

[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):

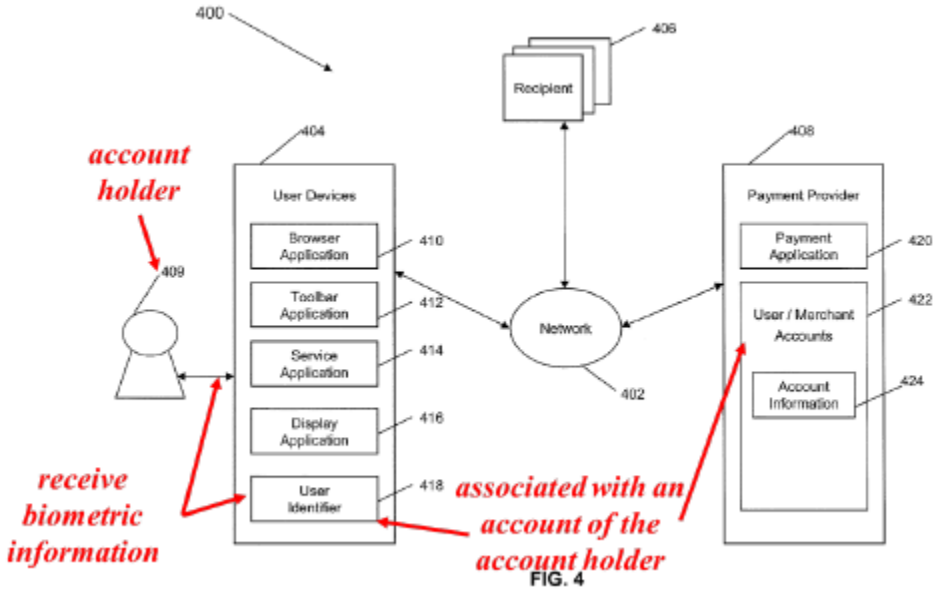

FIG. 4

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 user 409, red text stating "receive biometric information" with two red arrows pointing to a line between user 409 and user device 404 and to user identifier 418 in user device 404, and red text stating "associated with an account of the account holder" with two red arrows pointing to user identifier 418 in user device 404 and account information 422 in payment provider server 408.

> 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, where the stored "biometric id" is a user attribute of user identifier 418 associated with an account (account 422) of the account holder (user 409).

Pet. 31 (citing Ex. 1008 ¶ 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)).

Petitioner alternately argues that to the extent Stone does not describe biometric id, "Hoyos expressly describes receiving and storing biometric information during enrollment, and the stored biometric information is used for comparison with subsequent captured biometric data during transaction authentication." Pet. 33 (citing Ex. 1003 ¶ 94).

Patent Owner contends that "Petitioner fails to show that Stone discloses biometric information that is associated with an account of the account holder." PO Resp. 32 (citing Ex. 2032 ¶¶ 79–85); Sur-reply 11–12. In particular, Patent Owner contends that "[a]ny association that may occur of a user identifier with a user account occurs on the payment server 408, *not a data store on the user device*." PO Resp. 33 (citing Ex. 2032 ¶¶ 81–85) (emphasis added). According to Patent Owner, if Petitioner suggests that the association occurs in payment server 408, then limitations [1.6], [1.7.1], [1.7.2], [1.7.3], and [1.8] are not met because the requirement to capture biometric information and location data and perform fraud detection analysis "must occur *after* the account holder's biometric information is stored and associated with the account of the account holder in limitation [1.2] . . . Otherwise, there is no stored biometric information to be used for comparison." *Id.* at 35–36 (citing Ex. 2032 ¶ 84).

In connection with Petitioner's alternate reliance on Hoyos, Patent Owner argues that "Hoyos does not disclose receiving, storing, and

associating with an account biometric information in a data store in the exact manner claimed by the '656 Patent's limitation [1.2]." PO Resp. 37 (citing Ex. 2032 ¶ 85). Patent Owner further argues that "[t]he portion of Hoyos that Petitioner cites as disclosing limitation [1.2] is a generic description of the biometric matching technology known in the prior art at the time the Hoyos application was filed" and "[n]ot only is this not a disclosure of limitation [1.2], but a POSITA would not have been motivated to combine Hoyos's local authentication with Stone's client-server structure, particularly in terms of the 'association' step that occurs on the payment server 408 in Stone." *Id.* at 37–38 (citing Ex. 1013 ¶ 3; Ex. 2032 ¶¶ 79–85).

Petitioner, in turn, contends that in the combination of Stone, Hoyos, and Varghese, "the reference biometric information received during enrollment is associated with the user account in the biometric storage, which supports subsequent local matching during the live-scan process of the biometric authentication." Pet. Reply 12 (citing Ex. 1037, 9–10). According to Petitioner, in the proposed combination, "the biometric authentication is . . . stored **locally** and is associated with a user account for comparison later on, which provides enhanced privacy and improved security." *Id.* at 14 (citing Pet. 20–21; Ex. 1003 ¶ 68; Ex. 1038, 64; Ex. 1056 ¶ 27). Petitioner further contends that "where the biometric authentication is performed locally on the user device, user device 404 receives the user account through network 402 from the payment provider 408, and associates the received reference biometric information with the user account in its storage component, e.g., for performing a client-side biometric authentication process." *Id.* at 15 (citing Ex. 1055, 2; Ex. 1056 ¶ 28).

In connection with Patent Owner's argument concerning limitations [1.6]–[1.8], Petitioner contends the argument fails because it is "premised on a mischaracterization of Stone as '**only** disclos[ing] . . . associating the biometric id with a user's account [in the context of] a user money transfer request to the payment provider server.'" Pet. Reply 16 (citing PO Resp. 36; Ex. 1056 ¶ 29).

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

Patent Owner's argument is premised on Stone's disclosure of the payment provider server 408 using "user identifier 418" to "associate user 409 with a particular user account maintained by payment provider server 408." Ex. 1008 ¶ 45. This disclosure in Stone explicitly describes a process of "associating" identifier 418 with a particular user account maintained by the payment provider.

Limitation 1.2 recites that biometric information is received and stored in a data store and "wherein the biometric information is *associated* with an account of an account holder." Ex. 1001, 14:2–3 (emphasis added). The use of the past tense in limitation 1.2 indicates that the biometric information in a data store has been "associated" with an account of the account holder.[12] The plain and ordinary meaning of this clause is that the biometric information is "related" or "connected" to the user account information. Limitation 1.2 does not require that the process of associating the biometric information with an account of an account holder occurs in the recited data store, as Patent Owner asserts.

[12] A plain and ordinary meaning of "associated" is "related, connected, or combined together." Ex. 3001 (ASSOCIATED Definition & Meaning - Merriam-Webster).

Stone discloses that:

> User device 408 may include one or more user identifiers 418 which may be implemented, for example, as operating system registry entries, cookies associated with browser application 410, identifiers associated with hardware of user device 404, or various other appropriate identifiers. User identifier 418 may include attributes related to the user, such as personal information (e.g., a user name, password, photograph image, biometric id, address, phone number, etc.) and banking information (e.g., banking institution, credit card issuer, user account numbers, security information, etc.).

Ex. 1008 ¶ 45.

Dr. Jones testifies that

> 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, and is also referred to as "enrollment data." It is used for subsequent comparison with the later captured data to provide an authentication decision for a transaction request. APPL-0014 ¶ 9; (Heusch) Appl-1021, Abstract; (Draper) Appl-1023, 8:3–9:39.

Ex. 1003 ¶ 92.

> Stone describes that the received biometric information is associated with an account holder (use 409), and the biometric information ("biometric id") of user identifier 418 stored in user device 404 is associated with a user account 422 of the account holder 409 (account of the account holder) where user identifier 418 is used for identifying the account 422. (Stone) Appl-1018 ¶ 45 (describing that biometric id of user identifier 418 is one of the "attributes related to the user," and "user identifier 418 may be used by payment provider server 408 to associate user 409 with a particular user account maintained by payment provide server 408."), [0048].

Id. ¶ 93 (emphasis omitted).

Dr. Goodrich refers to the same disclosure in Stone as Dr. Jones and testifies that "Stone does not disclose any association of a user identifier 418 with a user's account 422 that occurs on the user's device 404. Any association that may occur of a user identifier with a user account occurs on

the payment server 408, not a data store on the user device." Ex. 2032 ¶ 81. Dr. Goodrich is relying on Stone's explicit disclosure of an association process on payment server 408, but, does not explain why a person of ordinary skill in the art would not understand that the biometric id in user identifier 418 is not "associated" (i.e., "related" or "connected") with the user account in the "banking information" portion of user identifier 418. *See id.* Consequently, we credit Dr. Jones's testimony on this point as it is consistent with the plain and ordinary meaning of "associated" as well as the disclosure of Stone. Dr. Goodrich's testimony on this point is entitled to little, if any, weight because of his lack of explanation or analysis as to why Stone's disclosure concerning user identifier 418 does not meet the requirement that "the biometric information is associated with an account of the account holder."

Based on the cited disclosure in Stone and Dr. Jones's testimony, we agree with Petitioner that "Stone describes that the received biometric information is associated with an account holder (user 409), and the biometric information ('biometric id') of user identifier 418 stored in user device 404 is associated with a user account 422 of the account holder 409." Pet. 32.

Patent Owner's argument that "[a]ny association that may occur of a user identifier with a user account occurs on the payment server 408, not a data store on the user device" is unavailing. PO Resp. 32; *see also* Sur-reply 13 ("Petitioner is also incorrect to say for local authentication in a system employing Stone-Hoyos-Varghese that the *association* is not required to occur on the payment server." (emphasis added)). As discussed above, the plain and ordinary meaning of limitation 1.2 does not require that the

process of association occur on the data store. Neither Patent Owner nor Dr. Goodrich offer a claim construction for limitation 1.2 that would require the "association" process to occur on a data store of the user device. *See* PO Resp. 14–15 ("Patent Owner and its expert have therefore given all claim terms their plain and ordinary meaning."); Ex. 2032 ¶ 82. The fact that Stone explicitly describes that the payment provider server 408 performs an association process is of little import in light of Stone's disclosure of biometric id associated with an account of the account holder as shown in user identifier 418. We, thus, agree with Petitioner that Patent Owner mischaracterizes Stone as disclosing that association only occurs on the payment provider server 408. Pet. Reply 16; Ex. 1056 ¶ 29.

Petitioner alternately relies on Hoyos to satisfy this limitation. Pet. 33. Hoyos discloses that:

> Biometric identification and authentication systems are known in the art, for example systems to compare facial features, iris imagery, fingerprints, finger vein images, and palm vein images have been used. *Such systems are known to be useful for either comparing biometric data acquired from an individual to stored sets of biometric data of known "enrolled" individuals or to compare biometric data acquired from an individual to a proposed template.*

Ex. 1013 ¶ 3 (emphasis added).

Dr. Jones testifies that

> Hoyos expressly describes receiving and storing biometric information during enrollment, and the stored biometric information is used for comparison with subsequent captured biometric data. (Hoyos) APPL-1013, [0003] . . . As discussed at VII.B.2, a [person of ordinary skill in the art] would have been motivated to apply Hoyos' fraud-resistant biometric authentication system in Stone, including implementing Hoyos' teaching of capture and store enrollment biometric data during enrollment for subsequent comparison.

Ex. 1003 ¶ 94.

Patent Owner's argument that "Hoyos does not disclose receiving, storing, and associating with an account biometric information in a data store in the exact manner claimed" is unavailing for several reasons. First, this is not an anticipation ground. Second, this argument, like Patent Owner's Stone argument, is improperly based on Patent Owner's argument that "associating" must occur in the data store. Further, Patent Owner's argument that an ordinarily skilled artisan would not have been motivated to combine "Hoyos's local authentication with Stone's client-server structure" is unavailing for the same reasons discussed above in our motivation to combine analysis. We, thus, find that Hoyos also discloses that biometric information in a local data store "is associated with an account of the account holder."

Patent Owner's argument that Petitioner's contentions for limitations 1.6, 1.7.1, 1.7.2, 1.7.3, and 1.8 fail because "there is no stored biometric information for [ ] comparison" and "Stone only discloses possibly associating the biometric id with a user's account 'with a user money transfer request to the payment provider server'" is also unavailing. PO Resp. 36 (citing Ex. 1008 ¶ 45). This argument is unavailing because, as discussed above, Stone discloses that "biometric information associated with an account of the account holder" is stored on the user device as does Hoyos.

For all foregoing reasons and after review of Petitioner's evidence in light of Patent Owner's contentions, we find that the combination of Stone, Hoyos, and Varghese teaches limitation 1.2.

[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):

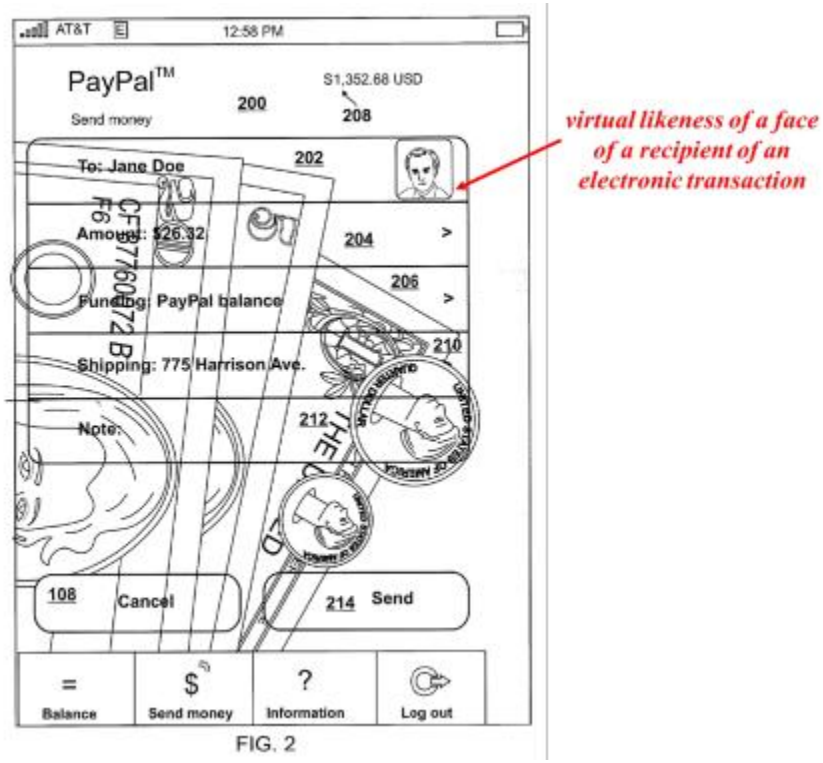

Figure 2 "shows a currency display on a user device." Ex. 1008 ¶ 11. Petitioner adds red text stating "virtual likeness of a face of a recipient of an electronic transaction" with an arrow pointing to an image of a face shown in element 202. Pet. 35.

Petitioner contends that Stone discloses "the processor is 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).

Patent Owner does not dispute Petitioner's contentions for this limitation. PO Resp. 15–40.

We reviewed the evidence cited by Petitioner and find that Stone teaches this limitation.

[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).

Patent Owner does not dispute Petitioner's contentions for this limitation. PO Resp. 15–40.

We reviewed the evidence cited by Petitioner and find that Stone teaches this limitation.

[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).

Patent Owner does not dispute Petitioner's contentions for this limitation. PO Resp. 15–40.

We reviewed the evidence cited by Petitioner and find that Stone teaches this limitation.

[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):

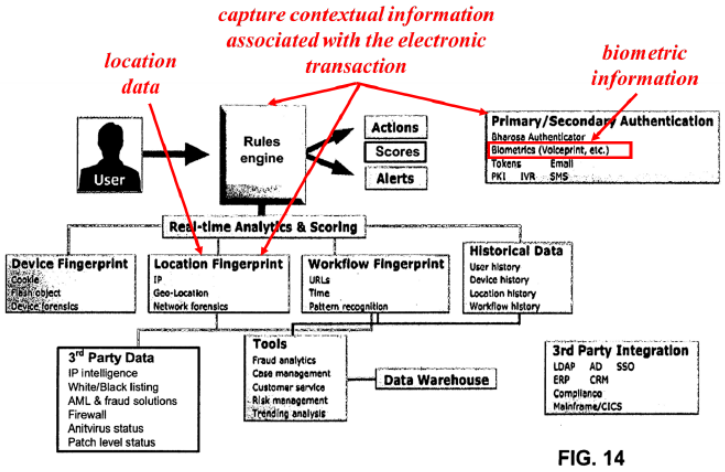

Figure 14 is a block diagram illustrating "a preferred function configuration of [Varghese's] invention." Ex. 1010 ¶ 14. Petitioner annotates Figure 14 with red text stating "location data" and a red arrow pointing to the block titled "Location Fingerprint," red text stating "capture contextual information 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)):

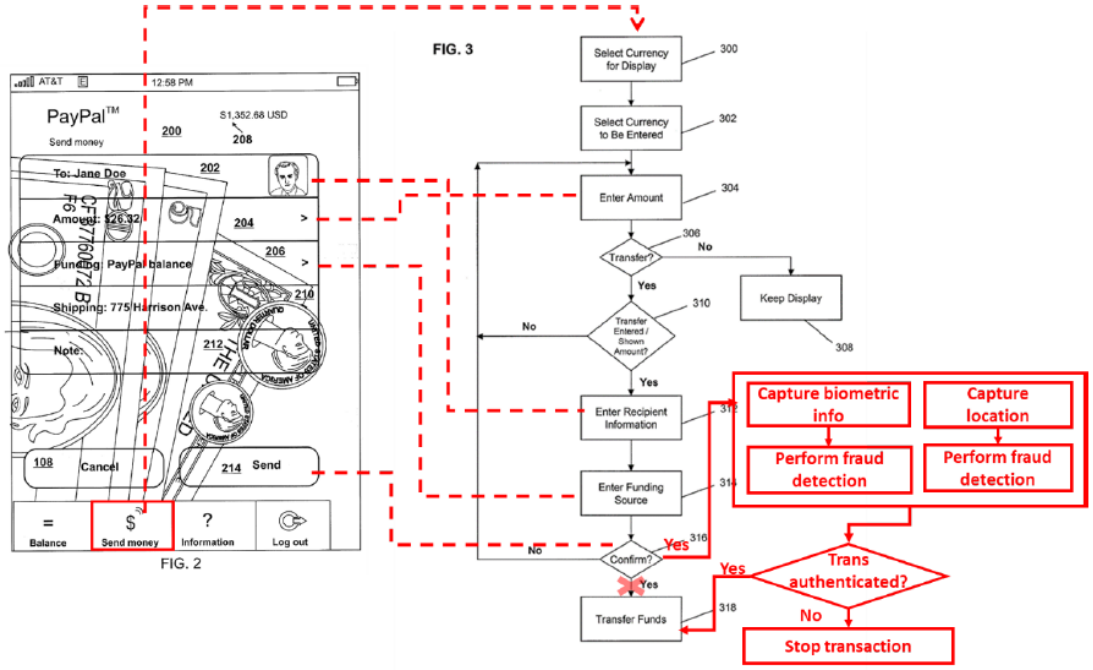

Figure 2, on the left, is "a currency display on a user device" of Stone and Figure 3, on the right, "is a flow chart." Ex. 1008 ¶¶ 11–12. Petitioner annotates the figures with broken red lines between the "$Send Money" icon in Figure 2 and block 300 in Figure 3, between element 202 in Figure 2 and block 312 in Figure 3, between element 204 in Figure 2 and block 304 in Figure 3, between element 206 in Figure 2 and block 314 in Figure 3, and between element 214 in Figure 2 and block 316 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)).

Patent Owner does not dispute Petitioner's contentions for this limitation. PO Resp. 15–40.

We reviewed the evidence cited by Petitioner and find that the combination of Stone, Hoyos, and Varghese teaches this limitation.

[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).

Patent Owner does not dispute Petitioner's contentions for this limitation. PO Resp. 15–40.

We reviewed the evidence cited by Petitioner and find that the combination of Stone, Hoyos, and Varghese teaches this limitation.

[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 liveliness 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).

Patent Owner does not dispute Petitioner's contentions for this limitation. PO Resp. 15–40.

We reviewed the evidence cited by Petitioner and find that the combination of Stone, Hoyos, and Varghese teaches this limitation.

[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.*):

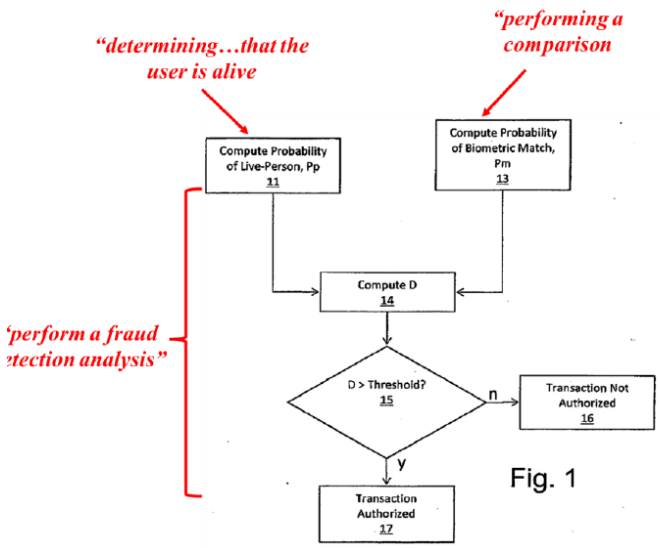

Figure 1 of Hoyos "is a flow chart of an authentication system." Ex. 1013 ¶ 32. Petitioner adds red text "determining . . . that the user is alive" with a red arrow pointing to block 11 in Figure 1, "performing a comparison" with a red arrow pointing to block 12 in Figure 1, and "performing a fraud

detection analysis" with a red line spanning the distance on the left side of Figure 1 from block 11 to block 17. Pet. 50.

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 Pm 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).

Patent Owner does not dispute Petitioner's contentions for this limitation. PO Resp. 15–40.

We reviewed the evidence cited by Petitioner and find that the combination of Stone, Hoyos, and Varghese teaches this limitation.

[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).

Patent Owner does not dispute Petitioner's contentions for this limitation. PO Resp. 15–40.

We reviewed the evidence cited by Petitioner and find that the combination of Stone, Hoyos, and Varghese teaches this limitation.

[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).

Patent Owner argues that for limitation 1.1, Petitioner relies on Stone's "processor 504 in user device 404, alone, or in combination with other processors including the processor 504 of other devices." PO Resp. 40 (citing Pet. 29–30; Ex. 2032 ¶ 87). Patent Owner then repackages its contentions for limitation 1.2 and argues that "[f]or the storing and association of biometric information with the account of the account holder required by limitation [1.2], this is done by the payment server 408." *Id.* According to Patent Owner, for this limitation, "under Petitioner's theory, the 'memory' must be at least coupled to the payment server 408 since the server must perform the association step." *Id.* (citing Ex. 2032 ¶ 87). As discussed above for limitation 1.2, we determine that Patent Owner's

arguments for limitation 1.2 are unavailing and, thus, Patent Owner's arguments for this limitation are also unavailing.

We reviewed the evidence cited by Petitioner and find that the combination of Stone, Hoyos, and Varghese teaches this limitation.

Summary of Claim 1

For all the foregoing reasons, Petitioner establishes by a preponderance of the evidence that claim 1 is obvious over the combination of Stone, Hoyos, and Varghese.

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* PO Resp. 15–40.

We reviewed Petitioner's evidence and arguments for claims 10 and 19 and for the reasons discussed with respect to claim 1, Petitioner establishes by a preponderance of the evidence that claims 10 and 19 are obvious over the combination of Stone, Hoyos, and Varghese.

5. Claims 4 and 13

Claims 4 depends from claim 1 and recites "wherein the virtual likeness of the face of the recipient was provided by the recipient." Ex. 1001, 14:39–30. Claim 13 depends from claim 10 and contains the same recitation. *Id.* at 15:23–24.

Petitioner contends that "Stone discloses or renders this element obvious. Pet. 52 (citing Ex. 1003 ¶¶ 144–148); *id.* at 60. Relying on its contentions for limitation 1.3, Petitioner contends that "Stone teaches rendering the virtual likeness of the face of the recipient in interface 200, e.g., using the photograph/icon information of user identifier 418 of recipient devices 406." *Id.* (citing Ex. 1008 ¶¶ 20, 36, 45–46). Petitioner next contends that "Stone's electronic transaction system provides a social networking aspect for connecting people, which was well known in the art." *Id.* (citing Ex. 1003 ¶ 146; Ex. 1008 ¶¶ 20, 36, Fig. 2). According to Petitioner, an ordinarily skilled artisan "would have been motivated to apply the well-known technique that an account holder (e.g., recipient) is provided the option to select the profile image for display (e.g., one sender's display in FIG. 2 of Stone), for benefits including online identity expression and 'increas[ing] a level of trust' between users." *Id.* (citing Ex. 1003 ¶ 147; Ex. 1009, 1:20–28, 15:15–27).

Patent Owner does not address Petitioner's contentions for claims 4 and 13 apart from its contentions for claim 1. PO Resp. 41–42.

We have reviewed Petitioner's evidence and arguments and determine that Petitioner establishes by a preponderance of the evidence that claims 4 and 13 are obvious over the combination of Stone, Hoyos, and Varghese.

6. Claims 5 and 14

Claim 5 depends from claim 1 and recites "wherein the transaction icon comprises a graphical representation of a payment form." Ex. 1001, 14:41–42. Claim 14 depends from claim 10 and contains the same recitation. *Id.* at 15:25–26.

Petitioner contends that "Stone discloses or renders obvious this element." Pet. 53 (citing Ex. 1003 ¶¶ 149–152), 60. Petitioner further contends that "Stone's funding source box 206 of FIG. 2 discloses a transaction icon for selecting a fund source." Pet. 53 (citing Ex. 1003 ¶ 150; Ex. 1008 ¶¶ 24, 34, Fig. 2). Petitioner alternatively argues that an ordinarily skilled artisan "would have been motivated to implement the funding source selection using a form of payment icon (e.g., 'the specific card, such as a Pay Pal card, Visa, MC, AMEX') for improved visual presentation, 'as contrasted to a generic representation of a card or no visual at all.'" *Id.* at 53–54 (citing Ex. 1003 ¶ 151; Ex. 1008 ¶¶ 4, 38).

Patent Owner contends that "[n]either Stone nor Hoyos discloses that a transaction icon can be a payment form." PO Resp. 41. Patent Owner further contends that "Petitioner provides no explanation why" an ordinarily skilled artisan "would have been motivated to implement the funding source selection using a form of payment icon . . . without working backward from claim [5] of the '656 Patent using hindsight." *Id.*; Sur-reply 17.

Petitioner, in turn, replies that Patent Owner "does not dispute that Stone teaches a *transaction icon* associated with a funding source ('funding source box 206' on FIG. 2 to implement the step 314 'Enter Funding Source')." Pet. Reply 22 (citing Ex. 1056 ¶ 39). Petitioner argues that Patent Owner "does not dispute that Stone teaches a *graphical*

representation of payment form of funding sources (display of 'specific card, such as a PayPal card, Visa, MC, AMEX, etc.')." *Id.* at 23 (citing Ex. 1008 ¶ 38). Petitioner further argues that Patent Owner "fails to rebut that a [person of ordinary skill in the art] would have been motivated to implement *a graphical representation* related to a specific user transaction for a user interface item (*transaction icon*) related to that specific user transaction" or would have been motivated "to use payment icons (e.g., type of currency) associated with blocks 300 and 302 for selecting types of currency." *Id.* at 22–23 (citing Ex. 1056 ¶¶ 40–41).

For the following reasons, Patent Owner's arguments are unavailing.

Figure 2 of Stone is reproduced below:

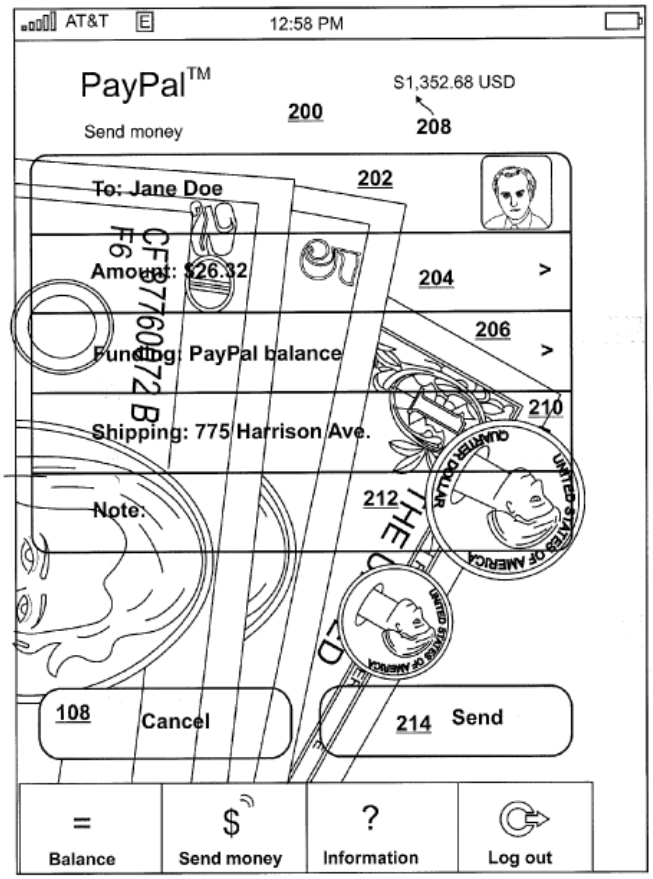

FIG. 2

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

As discussed above, Patent Owner does not dispute Petitioner's contentions for limitation 1.3. For limitation 1.3, Petitioner contends that numerous elements shown in Figure 2 correspond to the recited "transaction icons" including element 206. Pet. 35; Ex. 1003 ¶ 50 (citing Ex. 1008 ¶ 24, Fig. 2). As can be seen from Figure 2, the rectangle around element 206 contains the text "Funding: PayPal balance" and portions of various currency images appear in that rectangle. Ex. 1008, Fig. 2. Stone discloses that "[d]isplay 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 that "the display on the device may show a financial instrument, such as a specific type of credit card, bank card, or debit card." *Id.* ¶¶ 24, 38. Consequently, a preponderance of the evidence supports a finding that the text and various currency images shown in box 206 ("transaction icon") in Stone's Figure 2 correspond to the recited "graphical representation of a payment form." Additionally, Stone discloses that the display on the device may show a credit card, bank card, or debit card if that payment form is chosen by the user. For these reasons, we disagree with Patent Owner's contention that "[n]either Stone nor Hoyos discloses that a transaction icon can be a payment form" (PO Resp. 41). *See* Ex. 1056 ¶¶ 39–40. Because we find that Stone discloses "the transaction icon comprises a graphical representation of a payment form," Patent Owner's hindsight contention is unavailing.

For all the forgoing reasons, Petitioner establishes by a preponderance of the evidence that claim 5 and claim 14 are obvious over the combination of Stone, Hoyos, and Varghese. Ex. 1003 ¶¶ 149–152.

7. Claims 6 and 15

Claim 6 depends from claim 5 and recites "wherein the transaction icon comprises a graphical representation of money." Ex. 1001, 14:43–44. Claim 15 depends from claim 14 and contains the same recitation. *Id.* at 15:27–28.

Petitioner contends that "Stone discloses or renders obvious this element." Pet. 54 (citing Ex. 1003 ¶¶ 153–156), 60. Petitioner further contends that in Figure 2 of Stone, "each of the transaction icons '$Send money,' 'Send' 214, and the virtual currency discloses the transaction icon." *Id.* Petitioner next contends that "each transaction icon [in Figure 2] discloses graphical representation of money, e.g., '$ Send money' includes '$;' the virtual currency icon include[s] a group of one, five, and 20 dollar bills and coins." *Id.* at 55 (citing Ex. 1003 ¶ 155). According to Petitioner, an ordinarily skilled artisan "would have been motivated to implement 'Send' 214 of FIG. 2 and other transaction icons (e.g., 'Send,' 'Confirm,' 'Proceed' as discussed at [1.5] for transferring funds with a graphical representation of money (e.g., '$') for richer visual representation." *Id.*

Patent Owner does not provide separate arguments for these claims apart from its arguments for claims 1, 5, and 14. *See* PO Resp. 41–42.

We have reviewed Petitioner's evidence and arguments and determine that Petitioner establishes by a preponderance of the evidence that claims 6 and 15 are obvious over the combination of Stone, Hoyos, and Varghese.

8. Claims 8 and 17

Claim 8 depends from claim 1 and recites "the virtual likeness of the face of the recipient comprises an avatar of the recipient." Ex. 1001, 14:48–

49. Claim 17 depends from claim 10 and contains the same recitation. *Id.* at 15:35–36.

Petitioner contends that "Stone renders obvious this element." Pet. 56 (citing Ex. 1003 ¶¶ 158–161), 60. Petitioner further contends that "Stone discloses 'a recipient icon on the display, such as a picture of the recipient.'" *Id.* (citing Ex. 1008 ¶ 36) (emphasis omitted). Petitioner next contends that "Stone combined with a POSITA's knowledge that avatar is a well-known alternative of a picture for a user icon renders this element obvious." *Id.* (citing Ex. 1003 ¶ 160). According to Petitioner, an ordinarily skilled artisan would have "provide[d] the option to use an avatar as a recipient icon, because avatar was a well-known alternative design choice of pictures for user icon" and "has the benefits of providing an online identity that balances personal expression and privacy, and user picture has the benefits of enhanced personal recognition and trust." *Id.* (citing Ex. 1003 ¶ 106; Ex. 1047, 801).

Patent Owner contends that "Stone-Hoyos-Varghese does not disclose the use of an avatar to represent an account holder." PO Resp. 42 (citing Ex. 2032 ¶ 90). Patent Owner argues that Petitioner "states that an 'avatar' is a well-known alternative of a picture for a user icon" but, because it "is well known does not render it obvious." *Id.* According to Patent Owner, "Petitioner provides no justification why it would be obvious to use an avatar for an electronic payment system to reach the invention of the '656 Patent's claims 8 and 17, other than hindsight bias." *Id.* (citing Ex. 2032 ¶ 90); Sur-reply 18 ("Petitioner provides no reason why a POSITA would have been motivated to replace any of the user images Petitioner relies on from Stone . . . with an avatar.").

Petitioner in the Reply argues that Patent Owner disregards the "Petition's explanation that an 'avatar selected by the account holder is a well-known alternative of a picture for a user icon' [and] is within a POSITA's knowledge." Pet. Reply 24 (citing Pet. 56–57). Petitioner further argues that Patent Owner disregards the "Petition's explanation of benefits of using an avatar, supported by multiple references." *Id.*

For the following reasons, Patent Owner's arguments are unavailing.

Petitioner starts with Stone's disclosure of "a recipient icon on the display, such as a picture of the recipient." Pet. 56 (citing Ex. 1008 ¶ 36). Patent Owner does not dispute that Stone discloses a picture of the recipient.

Petitioner relies on Dr. Jones's testimony that it would have been within the knowledge of an ordinarily skilled artisan "that an avatar is a well-known alternative of a picture for a user icon." Ex. 1003 ¶ 160. Dr. Jones supports this testimony that avatars were well-known alternatives to a profile picture with reference to Exhibits 1009 ("Chatterjee") and Ex. 1047 ("Vasalou"). *Id.* In particular, Chatterjee discloses that "a profile picture or avatar of Baker can be displayed on mobile device 104." Ex. 1009, 9:34–36. Dr. Jones also provides testimony of the respective benefits of an avatar and a profile picture, i.e., "an avatar . . . balances personal expression and privacy, and a user picture has the benefits of enhanced personal recognition and trust." Ex. 1003 ¶ 160 (citing Ex. 1009, 9:30–35; Ex. 1047, 801). Neither Patent Owner nor Dr. Goodrich dispute this testimony by Dr. Jones. PO Resp. 42; Ex. 2032 ¶ 90.

We find that Petitioner establishes that it would have been obvious based on the disclosure of Stone and the knowledge of a person of ordinary skill in the art to substitute an avatar of the recipient for the picture of the

recipient shown in Figure 2 of Stone. Petitioner, supported by the testimony of Dr. Jones, has shown that an ordinarily skilled artisan would have known that an avatar was a well-known alternative to a picture and the benefits of using an avatar in place of a picture of the recipient. Ex. 1003 ¶ 160; Ex. 1009, 9:34–36; Ex. 1047, 801. Consequently, Petitioner's challenge to claim 8 has a rational underpinning.

For all the foregoing reasons, Petitioner establishes by a preponderance of the evidence that claims 8 and 17 are obvious over the combination of Stone, Hoyos, and Varghese.

9. Claims 9 and 18

Claim 9 depends from claim 1 and recites "a password is not required to initiate the electronic transaction." Ex. 1001, 14:50–51. Claim 18 depends from claim 10 and contains the same recitation. *Id.* at 15:35–36.

Petitioner contends that "Stone or Stone-Hoyos-Varghese renders obvious this element." Pet. 57 (citing Ex. 1003 ¶¶ 162–167), 60. Petitioner further contends that "Stone describes initiating the electronic transaction, e.g., clicking on '$Send money' of FIG. 2 without requiring a password." Pet. (citing Ex. 1003 ¶ 163).

Patent Owner does not provide separate arguments for these claims apart from its arguments for claim 1. *See* PO Resp. 41–42.

We have reviewed Petitioner's evidence and arguments and determine that Petitioner establishes by a preponderance of the evidence that claims 9 and 18 are obvious over the combination of Stone, Hoyos, and Varghese.

E. Ground 3: Alleged Obviousness of Claims 2, 3, 11, and 12 over the Combination of Stone, Hoyos, Varghese, and Borovsky

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

Patent Owner contends that Petitioner's proposed combination of Borovsky with Stone, Hoyos, and Varghese is based on improper hindsight. PO Resp. 48–49.

We begin with a brief summary of Borovsky and then address the parties' respective 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.

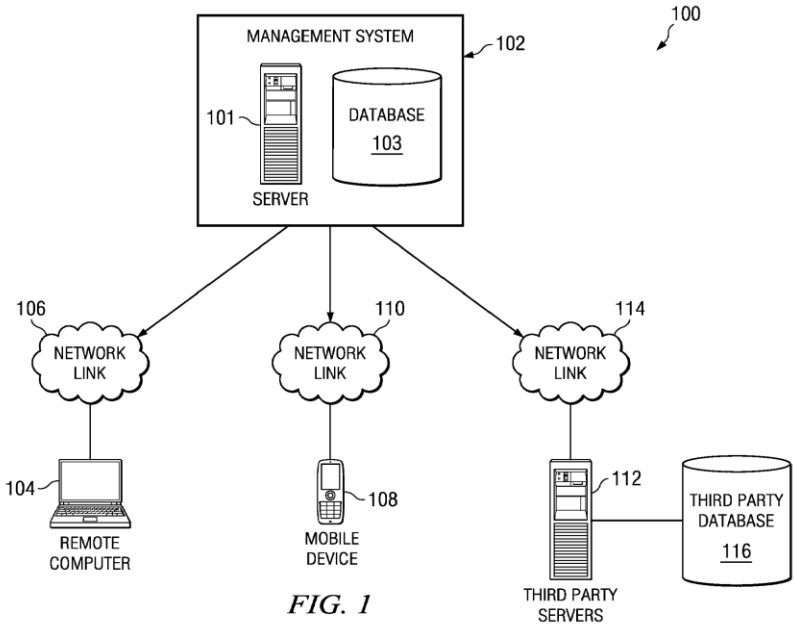

FIG. 1

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.

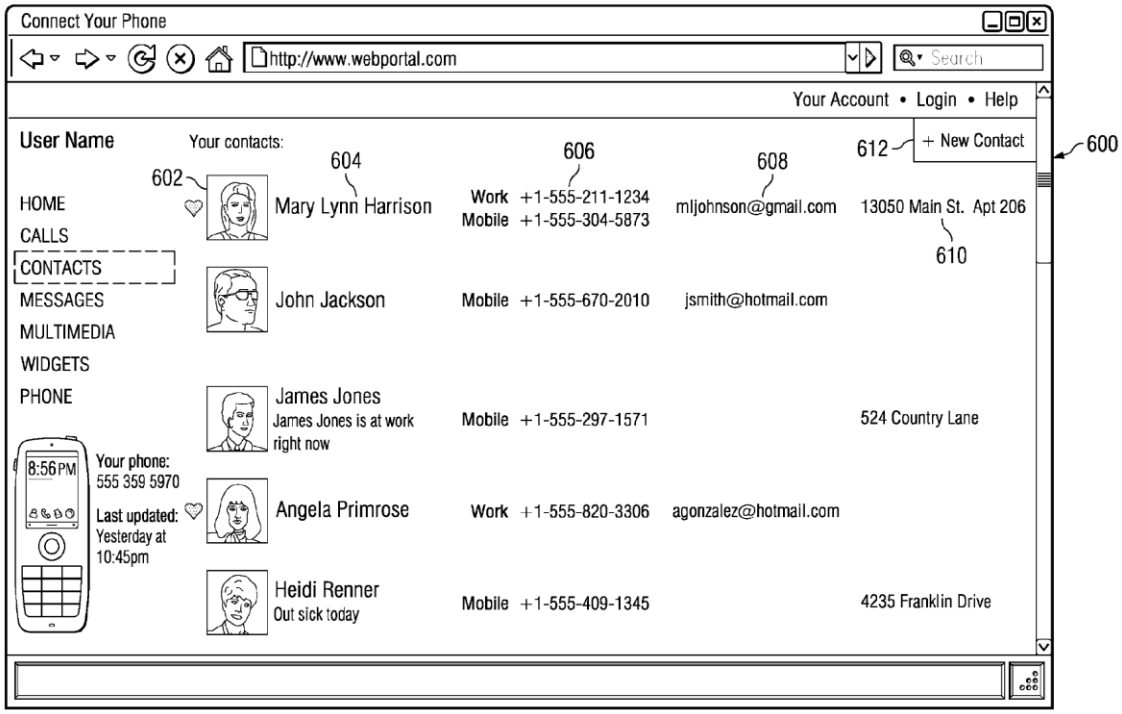

FIG. 6

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. Motivation to Combine/Reasonable Expectation of Success

Petitioner contends that Borovsky is analogous art to the '656 patent. Pet. 77–78. Petitioner argues that Borovsky is "in the same field of endeavor (computer network applications using a client-server system)" or alternatively "reasonably pertinent to a problem with which the inventor of the '656 patent was involved (e.g., improving display/identification of other users on a device)." *Id.* (citing Ex. 1003 ¶ 277; Ex. 1041, claims 1, 3, 6, 7). Patent Owner does not dispute that Borovsky is analogous art to the '656 patent. PO Resp. 48–49. For the reasons stated by Petitioner, we find that Borovsky is at least reasonably pertinent analogous art.

Petitioner first contends that Borovsky discloses "obtaining 'photos corresponding to the contact of the user' from 'social networking' sites . . . and sending these obtained photos together with other configuration information to a client device [to] 'be displayed with a particular contact.'" Pet. 76 (citing Ex. 1003 ¶ 275; Ex. 1041 ¶¶ 35, 39, 43, 45–46, Figs. 5–6, claims 3–7).

Petitioner next contends that "Stone has the need to obtain for display on the user device, pictures of other users connected to a network with the user." Pet. 78 (citing Ex. 1003 ¶ 278; Ex. 1008 ¶¶ 20, 36). Petitioner further contends that an ordinarily skilled artisan

> would have been motivated to apply Borovsky's teaching of providing contact photo obtained from social network sites for user device contact display as icons for network-connected users on user device, especially in the case that the other user did not profile a profile icon, for the benefits of enhanced user experience with helpful visuals, increased confidence and efficient identification.

Id. (citing Ex. 1003 ¶ 278).

Petitioner next contends that an ordinarily skilled artisan would have had a reasonable expectation of success because "Borovsky's teachings apply to various types of mobile devices including smartphones" and "Stone describes user devices implemented with any appropriate computing device . . . with wired and/or wireless communication over a network, and therefore, is not limited to any specific types of user devices." Pet. 79 (citing Ex. 1003 ¶ 279; Ex. 1008 ¶¶ 41–42; Ex. 1041 ¶ 13). According to Petitioner "configuring Stone to implement Borovsky's teaching . . . would have required only routine knowledge well within the skill of a POSITA." *Id.* (citing Ex. 1003 ¶ 279).

Patent Owner contends that "Petitioner does not state why a social networking site would be the obvious source for obtaining a user photo in Stone." PO Resp. 49 (citing Ex. 2032 ¶ 102); Sur-reply 20. Patent Owner further contends that "Stone does not discuss using social networks to populate any information for the disclosed interface," Stone's "information is all directly provided by the user . . . and/or banking or credit card information for the payment server 408," and "[n]othing in Stone suggests introducing another third-party server to Stone's existing client-server." *Id.* (citing Ex. 1008 ¶¶ 20, 36, 45–48). According to Patent Owner, "[t]he only motivation for doing [so] would be conceived in hindsight working backward from the '656 Patent's claims." *Id.*[13]

[13] Patent Owner does not address Petitioner's reasonable expectation of success contentions. PO Resp. 49.

Petitioner replies that Patent Owner's arguments disregard Petitioner's stated reasons for the combination. Pet. Reply 28 (citing Ex. 1056 ¶ 53). Petitioner contends that it "identifies Borovsky's known techniques used to improve a user interface by updating contact display on a user device with photos from social networks" and the "techniques would improve the user interface and user experience in Stone's system, in the same way when used according to Borovsky's teachings." *Id.* (citing Pet. 77–79; Ex. 1056 ¶ 54).

For the following reasons, Patent Owner's arguments are unavailing.

Stone discloses that "the user display may visually show other users." Ex. 1008 ¶ 24. Stone further discloses that when transferring funds, a user may "slide the visual currency to a recipient icon" and the "icon may appear on the screen, such as a picture of the person." *Id.* ¶ 36.

Petitioner provides the following annotated version of Figure 6 of Borovsky:

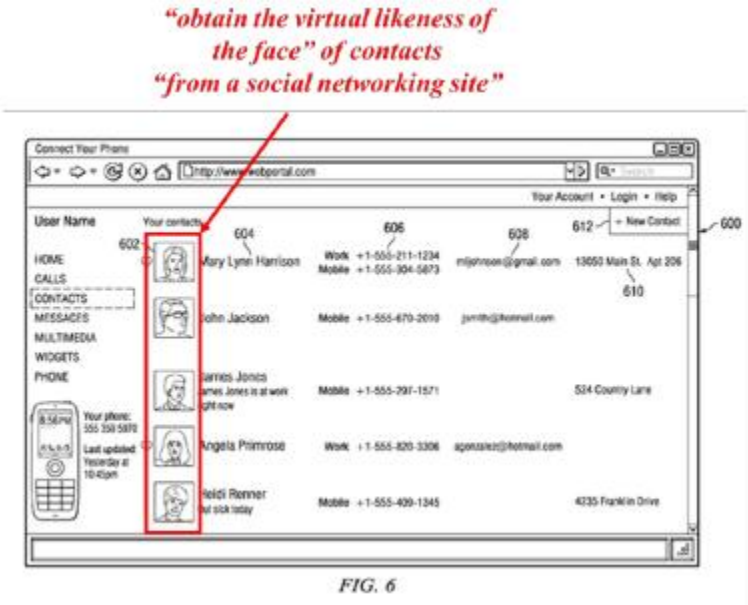

FIG. 6

Pet. 77. Figure 6 is "an example interface for viewing and/or editing contact information." Ex. 1041 ¶ 8. Petitioner annotates Figure 6 with a red rectangle around images of various contact persons, red text stating "'obtain the virtual likeness of the face' of contacts 'from a social networking site'" and a red arrow from the text pointing to the red rectangle. Pet. 77.

Dr. Jones explains Borovsky's use of a social networking site to obtain the virtual likeness of the face of a contact as follows:

> Borovsky describes obtaining "photos corresponding to contacts of the user" from "social networking" sites (e.g., "myspace™, facebook™, twitter™"), and sending these obtained photos, together with configuration information to a client device "for display." (Borovsky) APPL-1014, claims 3 ("pull third party information from the third party servers; aggregate and reconcile the pulled third party information with the configuration information"), claims 6 and 7 ("wherein the third party servers comprise . . . social network[] servers . . . and third party information comprises contact information including . . . photos corresponding to contacts of the user"); [0035], [0039] ("the updated configuration information sent to the mobile device 108 replaces configuration information already stored at the mobile device 108"), [0043] ("contact information may include . . . photos of the contacts"); [0045] ("By way of example, user interface 600 may include picture elements 602 for choosing a picture to be displayed with a particular contact (note that in some embodiments the picture may be automatically selected from one of a set of aggregated photos described below and displayed by management system 102 via interface 600) . . . This contact information may also be edited at mobile device 108" and updated at the management system), [0046] ("any and all of the afore mentioned aggregated contact information is pushed to the mobile device 108 for display and access via the mobile device 108"), FIGs 5, 6.

Ex. 1003 ¶ 275 (emphases omitted). Dr. Jones further testifies that the combination of Stone, Hoyos, and Varghese would benefit from

Borovsky's teachings in terms of "enhanced user experience with helpful visuals, increased transaction confidence (e.g., providing reassurance by seeing a recognizable photo), and efficient identification (e.g., easier identification of a recipient, esp. with common names)." *Id.* ¶ 276. Dr. Goodrich does not dispute Dr. Jones's testimony. Ex. 2032 ¶¶ 101–102. We credit Dr. Jones's testimony because it is consistent with the disclosure of Borovsky.

We disagree with Patent Owner's contention that Patent Owner's proposed combination is based on hindsight. As discussed above, Stone discloses using pictures of recipients on the user device. Ex. 1008 ¶¶ 20, 36; Ex. 1003 ¶ 278. As explained by Dr. Jones, Borovsky teaches obtaining contact photos for display on a user device from social networking sites and explains the benefits of Borovsky's teachings. Ex. 1003 ¶¶ 275–276. Given these disclosures in the cited references, Petitioner's combination is not based on hindsight but, rather, we agree with Petitioner that in the combination "Borovsky's known techniques [are] used to improve a user interface by updating contact display on a user device with a photo from social networks," and those "techniques would improve the user interface and user experience in Stone's system, in the same way when used according to Borovsky's teachings" (Pet. Reply 28). *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1380–81 (Fed. Cir. 2023) ("There is 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.'").

For all the foregoing reasons, Petitioner establishes that an ordinarily skilled artisan would have been motivated to combine Stone, Hoyos, Varghese, and Borovsky with a reasonable expectation of success. Ex. 1003 ¶¶ 275–279; Ex. 1056 ¶¶ 53–54.

3. Claims 2 and 11

Claim 2 depends from claim 1 and recites "the processor is further configured to obtain the virtual likeness of the face of the recipient from a social networking site." Ex. 1001, 14:32–34. Claim 11 depends from claim 10 and contains the same recitation. *Id.* at 15:16–18.

Petitioner contends that "Stone-Borovsky renders obvious this element." Pet. 79 (citing Ex. 1003 ¶¶ 280–283). Petitioner further contends that "Borovsky describes obtaining photos of contacts from a social networking site." *Id.* at 79–80 (citing Ex. 1003 ¶ 281; Ex. 1041 ¶¶ 35, 39, 42, 45–46, Figs. 5–6, claims 3–7). Petitioner further contends that Stone has the need to obtain photos of users for display on the user device and repeats its reasons, discussed above, for combining the teachings of Borovsky and Stone. *Id.* at 80 (citing Ex. 1003 ¶ 282).

Patent Owner first relies on its contentions for claim 1 discussed above in Ground 1. PO Resp. 48. As discussed above in connection with claim 1, those contentions are unavailing. Patent Owner's remaining contentions are directed to motivation to combine which, as discussed above, are also unavailing. *Id.* at 48–49.

We have reviewed Petitioner's evidence and determine that Petitioner establishes by a preponderance of the evidence that claims 2 and 11 are obvious over the combination of Stone, Hoyos, Varghese, and Borovsky.

4. Claims 3 and 12

Claim 3 depends from claim 2 and recites "obtaining the virtual likeness of the face of the recipient from the social networking site comprises scraping the social networking site for the virtual likeness of the face of the recipient." Ex. 1001, 14:35–39. Claim 12 depends from claim 11 and contains the same recitation. *Id.* at 15:19–22.

Petitioner contends that "Stone-Borovsky renders obvious this element." Pet. 81 (citing Ex. 1003 ¶¶ 294–287). According to Petitioner, "[i]t was well-known that scraping was a basic technique for collecting information including contact photos from social network sites, e.g., as an alternative when no API level access was available." *Id.* (citing Ex. 1003 ¶ 285; Ex. 1043, 4:42–49; Ex. 1045, 174; Ex. 1046 ¶¶ 26, 31–33). Petitioner contends that an ordinarily skilled artisan "would have been motivated to apply scraping the social network site to obtain the photo of the recipient in Stone-Borovsky." *Id.* (citing Ex. 1003 ¶ 286).

Patent Owner first relies on its contentions for claim 1 discussed above in Ground 1. PO Resp. 48. As discussed above in connection with claim 1, those contentions are unavailing. Patent Owner's remaining contentions are directed to motivation to combine which, as discussed above, are also unavailing. *Id.* at 48–49.

We have reviewed Petitioner's evidence and determine that Petitioner establishes by a preponderance of the evidence that claims 3 and 12 are obvious over the combination of Stone, Hoyos, Varghese, and Borovsky

F. Grounds 2 and 4

Petitioner submits these alternate challenges to the patentability of the Challenged Claims. Pet. 6. As discussed above, we have addressed all of the Challenged Claims based on Grounds 1 and 3, and as such, we need not and do not decide whether Petitioner has shown by a preponderance of the evidence that the Challenged Claims also would have been unpatentable over these alternate challenges. *See SAS Inst. Inc. v. Iancu*, 584 U.S. 357, 371 (2018) (holding that a petitioner "is entitled to a final written decision addressing all of the claims it has challenged"); *see also* 35 U.S.C. § 318(a); *cf. In re Gleave*, 560 F.3d 1331, 1338 (Fed. Cir. 2009) (not reaching other grounds of unpatentability after affirming the anticipation ground); *Beloit Corp. v. Valmet Oy*, 742 F.2d 1421, 1423 (Fed. Cir. 1984) (holding that once a dispositive issue is decided, there is no need to decide other issues).

III. CONCLUSION[14]

Weighing the competing evidence and testimony, we determine that Petitioner establishes by a preponderance of the evidence that the Challenged Claims of the '656 patent are unpatentable.

In summary:

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1, 4–10, 13–19	103(a)	Stone, Hoyos, Varghese	1, 4–10, 13–19	
1, 4–10, 13–19	103(a)	Stone, FFIEC Guidance[15]		
2, 3, 11, 12	103(a)	Stone, Hoyos, Varghese, Borovsky	2, 3, 11, 12	
2, 3, 11, 12	103(a)	Stone, FFIEC Guidance, Borovsky[16]		
Overall Outcome			1–19	

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

[15] We do not reach this ground because we determine that claims 1, 4–10, and 13–19 are unpatentable based on Petitioner's first ground.

[16] We do not reach this ground because we determine that claims 2, 3, 11, and 12 are unpatentable based on Petitioner's third ground.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–19 of the ’656 patent have been shown by a preponderance of the evidence to be unpatentable; and

FURTHER ORDERED that any party seeking judicial review must comply with the notice and service requirements of 37 C.F.R. § 90.2.

FOR PETITIONER:

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

FOR PATENT OWNER:

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