

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

CARBYNE BIOMETRICS, LLC,

Patent Owner

IPR2024-00329

U.S. Patent No. 9,972,010

**PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MANDATORY NOTICES	1
	A. Real Party-in-Interest	1
	B. Related Matters.....	1
	C. Lead and Back-up Counsel and Service Information	1
III.	GROUND FOR STANDING.....	2
IV.	THE '010 PATENT.....	2
	A. Summary of the '010 patent.....	2
	B. Prosecution History	3
V.	LEVEL OF ORDINARY SKILL IN THE ART.....	4
VI.	CLAIM CONSTRUCTION	5
VII.	REQUESTED RELIEF.....	5
VIII.	OVERVIEW OF CHALLENGES	6
	A. Challenged Claims	6
	B. Statutory Grounds for Challenges.....	6
IX.	IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE....	7
	A. Overview of Prior Art.....	7
	1. Stone.....	7
	2. Hoyos	8
	3. Varghese.....	10
	4. FFIEC Guidance	12
	5. Analogous Art.....	13
	B. Ground 1: Claims 1-2, 4-6, 9-10, 12-14, 17, 20-21, and 23 are Rendered Obvious under §103(a) over Stone in view of Hoyos.	14
	1. Combination of Disclosures/Embodiments of Stone.....	14
	2. Combination of Stone and Hoyos (“Stone-Hoyos”).....	17
	3. Claim 1	22

4.	Claim 2.....	47
5.	Claim 4.....	49
6.	Claim 5.....	51
7.	Claim 6.....	52
8.	Claim 9.....	53
9.	Claims 10, 12, 13, 14	55
10.	Claim 17.....	55
11.	Claim 20.....	56
12.	Claim 21	57
13.	Claim 23	57
C.	Ground 2: Claims 7, 15, and 22 are Rendered Obvious under §103(a) over Stone-Hoyos-Varghese.....	60
1.	Combination of Stone, Hoyos, and Varghese (“Stone-Hoyos-Varghese”).....	60
2.	Claims 7 and 15.....	64
3.	Claim 22	67
D.	Ground 3: Claims 1-2, 4-7, 9-10, 12-15, 17, 20-23 are Rendered Obvious under §103(a) over Stone in view of FFIEC Guidance.....	68
1.	Combination of Stone and FFIEC Guidance (“Stone-Guidance”)	68
2.	Claim 1	70
3.	Claims 2, 4, 5, 6	78
4.	Claim 7.....	79
5.	Claim 9.....	81
6.	Claims 10, 12, 13, 14	81
7.	Claim 15	81
8.	Claim 17.....	81
9.	Claim 20.....	82
10.	Claim 21	83

11. Claim 22	84
12. Claim 23	84
X. DISCRETIONARY DENIAL IS NOT WARRANTED	85
A. The <i>Fintiv</i> factors favor institution.	86
B. <i>Advanced Bionics</i> Test Favors Institution.....	88
XI. CONCLUSION.....	89
XII. CERTIFICATE OF WORD COUNT	90
CERTIFICATE OF SERVICE	91

PETITIONER’S EXHIBIT LIST

January 30, 2024

APPL-1001	U.S. Patent No. 9,972,010 to Jakobsson (“’010 patent”)
APPL-1002	Prosecution File History of U.S. App. No. 13/875,245 (“’245 App”)
APPL-1003	Declaration of Dr. Creed Jones (“Jones Decl.”)
APPL-1004	CV of Dr. Creed Jones
APPL-1005	Prosecution File History of U.S. Prov. App. 61/332,140 (“’140 App”)
APPL-1006	Prosecution File History of U.S. App. No. 13/099,981 (“’981 App”)
APPL-1007	RESERVED
APPL-1008	U.S. Pub. No. 2010/0042535 to Stone (“Stone”)
APPL-1009	U.S. Patent No. 8,386,620 to Chatterjee (“Chatterjee”)
APPL-1010	U.S. Pub. No. 2006/0282660 to Varghese et al. (“Varghese”)
APPL-1011	U.S. Pub. No. 2009/0135188 to Ding et al. (“Ding”)
APPL-1012	U.S. Patent No. 8,355,530 to Park et al. (“Park”)
APPL-1013	U.S. Pub. No. 2010/0014720 to Hoyos et al. (“Hoyos”)
APPL-1014	U.S. Pub. No. 2006/0158307 to Lee et al. (“Lee”)
APPL-1015	U.S. Patent No. 8,150,772 to Mardikar et al. (“Mardikar”)
APPL-1016	U.S. Pub. No. 2009/0157560 to Carter et al. (“Carter”)
APPL-1017	U.S. Patent No. 5,164,992 to Turk et al. (“Turk”)
APPL-1018	U.S. Patent No. 7,814,332 to Beenau et al. (“Beenau”)
APPL-1019	U.S. Patent No. 10,373,173 to Winner et al. (“Winner”)
APPL-1020	U.S. Patent No. 7,856,472 to Arav (“Arav”)
APPL-1021	Heusch, et al., “Local Binary Patterns as an Image Preprocessing for Face Authentication,” IDIAP Research Institute Report, November 2005 (“Heusch”)
APPL-1022	Oracle-Bharosa Acquisition Announcement, 2007,

	https://www.oracle.com/us/corporate/acquisitions/bharosa/oracle-bharosa-faq-072369.pdf (retrieved January 17, 2024) (“Oracle-Bharosa Acquisition Announcement”)
APPL-1023	U.S. Patent No. 7,779,268 to Draper et al. (“Draper”)
APPL-1024	U.S. Patent No. 5,930,804 to Yu et al. (“Yu”)
APPL-1025	Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (June 21, 2022) (“Director Memo”)
APPL-1026	Preliminary Constructions, <i>Carbyne Biometrics, LLC v. Apple Inc.</i> , WDTX-1:23-cv-00324 (December 11, 2023)
APPL-1027	United States District Courts—National Judicial Caseload Profile (September 30, 2023), https://www.uscourts.gov/statistics/table/na/federal-court-management-statistics/2023/09/30 (retrieved Dec. 14, 2023)
APPL-1028	Scheduling Order, <i>Carbyne Biometrics, LLC v. Apple Inc.</i> , WDTX-1:23-cv-00324 (July 14, 2023)
APPL-1029	Carbyne Preliminary Infringement Contentions, <i>Carbyne Biometrics, LLC v. Apple Inc.</i> , WDTX-1:23-cv-00324 (June 21, 2023)
APPL-1030 - APPL-1032	RESERVED
APPL-1033	J. P. Campbell, “Speaker Recognition: a Tutorial,” in Proceedings of the IEEE, vol. 85, no. 9, pp. 1437-1462, Sept. 1997 (“Campbell”)
APPL-1034	U.S. App. Pub. No. 2009/0288012A1 to Hertel et al. (“Hertel”)
APPL-1035	U.S. Patent No. 8,533,485 to Bansal et al. (“Bansal”)
APPL-1036	U.S. App. Pub. No. 2006/0271460A1 to Hanif (“Hanif”)
APPL-1037	Federal Financial Institutions Examination Council, FFIEC Press Release and FFIEC Guidance - Authentication in an Internet Banking Environment, Oct 12, 2005, https://www.ffiec.gov/pdf/authentication_guidance.pdf (retrieved January 17, 2024), accessible through hyperlinks in https://www.ffiec.gov/press/pr101205.htm (APPL-1040) and https://www.fdic.gov/news/inactive-financial-institution-

	letters/2005/fil10305.html (APPL-1039) (“Guidance”)
APPL-1038	Bhargav-Spantzel et al., “Privacy Preserving Multifactor Authentication with Biometrics,” DIM’06, November 3, 2006 (“Bhargav-Spantzel”)
APPL-1039	FDIC Financial Institution Letter, FFIEC Guidance Authentication in an Internet Banking Environment, FIL-103-2005, October 12, 2005, https://www.fdic.gov/news/inactive-financial-institution-letters/2005/fil10305.html (retrieved January 17, 2024), including hyperlink for APPL-1037 (“FIL-103-2005”)
APPL-1040	Federal Financial Institutions Examination Council, FFIEC Guidance Press Release, Oct 12, 2005, https://www.ffiec.gov/press/pr101205.htm (retrieved January 17, 2024), including hyperlink for APPL-1037 (“FFIEC Guidance Press Release”)
APPL-1041	U.S. App. Pub. No. 2010/0317335A1 to Borovsky (“Borovsky”)
APPL-1042	Ekler et al., “Similarity Management in Phonebook-Centric Social Networks,” 2009 Fourth International Conference on Internet and Web Applications and Services, Venice/Mestre, Italy, 2009, pp. 273-279, doi: 10.1109/ICIW.2009.46 (“Ekler”)
APPL-1043	U.S. Patent No. 8,954,500 to Marlow et al. (“Marlow”)
APPL-1044	Kollreider et al., “Verifying Liveness by Multiple Experts in Face Biometrics,” 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, Anchorage, AK, USA, 2008, pp. 1-6, doi: 10.1109/CVPRW.2008.4563115 (“Kollreider”)
APPL-1045	Narayanan et al., “De-anonymizing Social Networks,” 2009 30th IEEE Symposium on Security and Privacy, 2009 (“Narayanan”)
APPL-1046	U.S. App. Pub. No. US2008/0270038A1 to Partovi et al. (“Partovi”)
APPL-1047	Vasalou et al., “Avatars in Social Media: Balancing Accuracy, Playfulness and Embodied Messages,” International Journal of Human-Computer Studies Volume 66, Issue 11, November 2008, Pages 801-811 (“Vasalou”)

Listing of Challenged Claims

Claim 1	
[1.0]	A system, comprising:
[1.1]	one or more processors configured to:
[1.2]	receive a virtual likeness of a face of an account holder; associate, in a data store, the virtual likeness of the face of the account holder with an account of the account holder;
[1.3]	render, in an interface, the virtual likeness of the face of the account holder;
[1.4]	render a transaction icon associated with an electronic transaction, wherein the transaction icon is rendered in the interface with the virtual likeness of the face of the account holder;
[1.5]	receive an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the account holder;
[1.6]	capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information associated with a user;
[1.7]	perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises determining, based at least in part on the captured biometric information, that the user is alive; and
[1.8]	based at least in part on both the user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the account holder and performing the fraud detection analysis comprising determining that the user is alive

	based at least in part on the captured biometric information, complete the electronic transaction; and
[1.9]	a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.
Claim 2	
[2.0]	The system of claim 1 wherein the transaction icon includes a graphical representation of an amount of money.
Claim 4	
[4.0]	The system of claim 1 wherein the transaction icon includes a graphical representation of a payment form.
Claim 5	
[5.0]	The system of claim 1 wherein the virtual likeness comprises a photograph of the account holder.
Claim 6	
[6.0]	The system of claim 1 wherein the virtual likeness comprises an avatar selected by the account holder.
Claim 7	
[7.0]	The system of claim 1 wherein the captured contextual information further comprises at least one of physical location information and information spoken by the user.
Claim 9	
[9.0]	A method, comprising:
[9.1]	receiving a virtual likeness of a face of an account holder; associating, in a data store, the virtual likeness of the face of the account holder with an account of the account holder;

[9.2]	rendering, in an interface, the virtual likeness of the face of the account holder;
[9.3]	rendering a transaction icon associated with an electronic transaction, wherein the transaction icon is rendered in the interface with the virtual likeness of the face of the account holder;
[9.4]	receiving an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the account holder;
[9.5]	capturing contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information associated with a user;
[9.6]	performing a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises determining, based at least in part on the captured biometric information, that the user is alive; and
[9.7]	based at least in part on both the user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the account holder and performing the fraud detection analysis comprising determining that the user is alive based at least in part on the captured biometric information, completing the electronic transaction.
Claim 10	
[10.0]	The method of claim 9 wherein the transaction icon includes a graphical representation of an amount of money.
Claim 12	
[12.0]	The method of claim 9 wherein the transaction icon includes a graphical representation of a payment form.

Claim 13	
[13.0]	The method of claim 9 wherein the virtual likeness comprises a photograph of the account holder.
Claim 14	
[14.0]	The method of claim 9 wherein the virtual likeness comprises an avatar selected by the account holder.
Claim 15	
[15.0]	The method of claim 9 wherein the captured contextual information further comprises at least one of physical location information and information spoken by the user.
Claim 17	
[17.0]	A computer program product embodied in a non-transitory computer readable storage medium and comprising computer instructions for:
[17.1]	receiving a virtual likeness of a face of an account holder; associating, in a data store, the virtual likeness of the face of the account holder with an account of the account holder;
[17.2]	rendering, in an interface, the virtual likeness of the face of the account holder;
[17.3]	rendering a transaction icon associated with an electronic transaction, wherein the transaction icon is rendered in the interface with the virtual likeness of the face of the account holder;
[17.4]	receiving an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the account holder;
[17.5]	capturing contextual information associated with the electronic

	transaction, the captured contextual information comprising captured biometric information associated with a user;
[17.6]	performing a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises determining, based at least in part on the captured biometric information, that the user is alive; and
[17.7]	based at least in part on both the user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the account holder and performing the fraud detection analysis comprising determining that the user is alive based at least in part on the captured biometric information, completing the electronic transaction.
Claim 20	
[5.0]	20. The system of claim 1 wherein the captured biometric information associated with the user includes a fingerprint.
Claim 21	
[5.0]	21. The system of claim 1 wherein the captured biometric information comprises a plurality of photographs, and wherein the fraud detection analysis comprises an analysis of the plurality of photographs to determine that the user is alive.
Claim 22	
[22.0]	The system of claim 1 wherein the captured contextual information further comprises captured physical location information associated with the user, and wherein performing the fraud detection analysis further comprises determining a physical location of the user based at least in part on the captured physical location information.
Claim 23	

[23.0]	The system of claim 1 wherein the account holder comprises a first account holder, wherein the account comprises a first account, and wherein the one or more processors are further configured to:
[23.1]	receive a virtual likeness of a face of a second account holder; associate, in the data store, the virtual likeness of the face of the second account holder with a second account of the second account holder; and
[23.2]	render a destination image comprising the virtual likeness of the face of the second account holder; and
[23.3]	wherein completing the electronic transaction based at least in part on both the user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the first account holder and performing the fraud detection analysis comprising determining that the user is alive based at least in part on the captured biometric information comprises transferring funds between the first account of the first account holder and the second account of the second account holder for which the destination image comprising the virtual likeness of the face of the second account holder was rendered.

I. INTRODUCTION

U.S. Patent No. 9,972,010 (the “’010 patent”) relates to “Method, Medium, and System for Reducing Fraud.” APPL-1001, Title, Abstract. Apple Inc. (“Petitioner” or “Apple”) respectfully requests that the Board review and cancel as unpatentable under (pre-AIA) 35 U.S.C. §103(a) claims 1-2, 4-7, 9-10, 12-15, 17, 20-23 (“Challenged Claims”) of the ’010 patent.

II. MANDATORY NOTICES

A. Real Party-in-Interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that the real party-in-interest is Apple Inc.

B. Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), the ’010 patent is or was involved in the following cases, which may affect, or be affected by, this proceeding:

- *Carbyne Biometrics, LLC v. Apple Inc.*, 1:23-cv-00324 (WDTX), filed March 24, 2023 (Pending) (“Parallel District Court Proceeding”)

Apple is not aware of any disclaimers, reexamination certificates, or IPR petitions addressing the ’010 patent.

C. Lead and Back-up Counsel and Service Information

Lead Counsel

David W. O’Brien
HAYNES AND BOONE, LLP
2801 N. Harwood St., Suite 2300
Dallas, TX 75201

Phone: (512) 867-8457
Fax: (214) 200-0853
david.obrien.ipr@haynesboone.com
USPTO Reg. No. 40,107

Back-up Counsel

Hong Shi
HAYNES AND BOONE, LLP
2801 N. Harwood St., Suite 2300
Dallas, TX 75201

Phone: (512) 867-8440
Fax: (214) 200-0853
hong.shi.ipr@haynesboone.com
USPTO Reg. No. 69,009

Kelly Lyle
HAYNES AND BOONE, LLP
2801 N. Harwood St., Suite 2300
Dallas, TX 75201

Phone: (512) 867-8528
Fax: (214) 200-0853
kelly.lyle.ipr@haynesboone.com
USPTO Reg. No. 62,332

Please address all correspondence to lead and back-up counsel. Petitioner consents to electronic service and asks Patent Owner to do the same.

III. GROUNDS FOR STANDING

Petitioner certifies that the '010 patent is eligible for IPR and that Petitioner is not barred or estopped from requesting IPR challenging the patent claims. 37 C.F.R. §42.104(a).

IV. THE '010 PATENT

A. Summary of the '010 patent

The '010 patent is directed at electronic transactions, and specifically financial transaction systems. APPL-1001, Abstract. As shown in FIG. 7 below, the '010 patent describes that its improved techniques to prevent fraud include using an audio sample (by selecting box 704) or one or more photographs (by selecting box 702) for authentication. APPL-1003, ¶¶28-31.

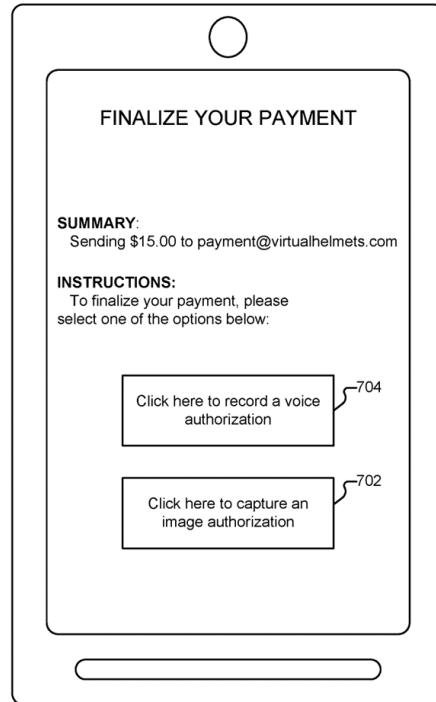


FIG. 7

APPL-1001, FIG. 7

Specifically, '010 patent describes techniques “for confirming that the object being photographed is alive (e.g., by taking multiple photographs in rapid succession) can be employed to help make sure that the fraudster isn’t using camera 112 to photograph a printed picture of the legitimate user.” APPL-1001, 8:54-60.

However, as discussed below, these supposedly improved techniques for fraud detection in electronic transactions were well-known at the time of the claimed invention.

B. Prosecution History

The prosecution history includes double patenting rejection and multiple

rejections under 101 and 103, RCES, and responses by Applicant with amendments amending the claims. APPL-1003, ¶¶32-35. Applicant filed terminal disclaimer over U.S. Patent No. 8,458,041 to overcome the double patenting rejection. APPL-1002, '245 App, 126.

On March 27, 2018, Notice of Allowance issued, with Examiner Amendment including “wherein performing the fraud detection analysis comprises determining, based at least in part on the captured biometric information, that the user is alive.” APPL-1002, 441-442.

V. LEVEL OF ORDINARY SKILL IN THE ART

The level of ordinary skill in the art may be reflected by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). Here, 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. APPL-1003, ¶20. Furthermore, 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.* However, Petitioner does not imply that a person having an extraordinary level of skill should be regarded as POSITA.

VI. CLAIM CONSTRUCTION

During IPR, claims are construed according to the standard as set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). 37 C.F.R. §42.100(b) (Nov. 13, 2018). Petitioner believes that, for the purposes of this proceeding and the analysis presented herein, no claim term requires express construction. *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (“only those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy”). Accordingly, this Petition analyzes the claims consistent with ordinary and customary meaning as would be understood by POSITA in light of the specification.¹ *Phillips*, 415 F.3d at 1314-17; APPL-1003, ¶¶36-37.

VII. REQUESTED RELIEF

Petitioner asks the Board to institute trial and cancel the Challenged Claims.

¹ The District Court, at Markman hearing on December 11, 2023, indicated its intention to adopt its preliminary constructions (APPL-1026), which apply plain and ordinary meaning for terms in dispute.

VIII. OVERVIEW OF CHALLENGES

A. Challenged Claims

Claims 1-2, 4-7, 9-10, 12-15, 17, and 20-23 (“Challenged Claims”) of the ’010 patent are challenged.

B. Statutory Grounds² for Challenges

Ground	Claims	Basis
#1	1-2, 4-6, 9-10, 12-14, 17, 20-21, and 23	§103(a) over Stone in view of Hoyos
#2	7, 15, and 22	§103(a) over Stone-Hoyos-Varghese
#3	1-2, 4-7, 9-10, 12-15, 17, and 20-23	§103(a) over Stone in view of FFIEC Guidance

Stone was filed Aug. 15, 2008 and published Feb. 18, 2010. Hoyos was filed Oct. 2, 2007 and published Jan. 21, 2010. Stone and Hoyos each are prior art under at least §§102(a) and 102(e).

Varghese was filed Apr. 28, 2006 and published Dec. 14, 2006. Varghese is prior art under at least § 102(b).

FFIEC Guidance (also referred to as “Guidance”) was published October 12, 2005, and was prior art under at least §102(b). Dr. Jones testifies that the Guidance was publicly accessible to a POSITA, and was widely referenced by numerous articles and patent disclosures before 2010 as an important driver for implementing

² Pre-AIA §§102 and 103(a) apply.

multifactor authentication for electronic transaction including financial transactions. APPL-1003, ¶¶47-50 (citing APPL-1039, APPL-1040, archive.org links, Google Scholar cites, patent disclosures).

IX. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE

A. Overview of Prior Art

1. Stone

Stone is titled “Currency Display,” and assigned to eBay on its face. Stone is analogous art to the ’010 patent, because it is directed to financial transaction applications. APPL-1008, [0001]-[0005]; APPL-1003, ¶¶38-39.

As shown in FIG. 2 of Stone below, Stone describes a system for electronic payment with improved electronic visual displays to provide the user with “a more visually rich interface,” e.g., by providing visual representations of financial instruments and the amount, and a visual representation when the monetary amount is transferred. APPL-1008, [0016], FIGS. 1 and 3. Stone describes that its system implementing user devices of different types (“mobile phone, laptop computer, PDA, or personal computer,” or “other suitable device”) and various communication connections (“the Internet and/or one or more intranets, landline networks, wireless networks, and/or other appropriate types of communication networks”). APPL-1008, [0022], [0024], [0041], [0044], [0046].

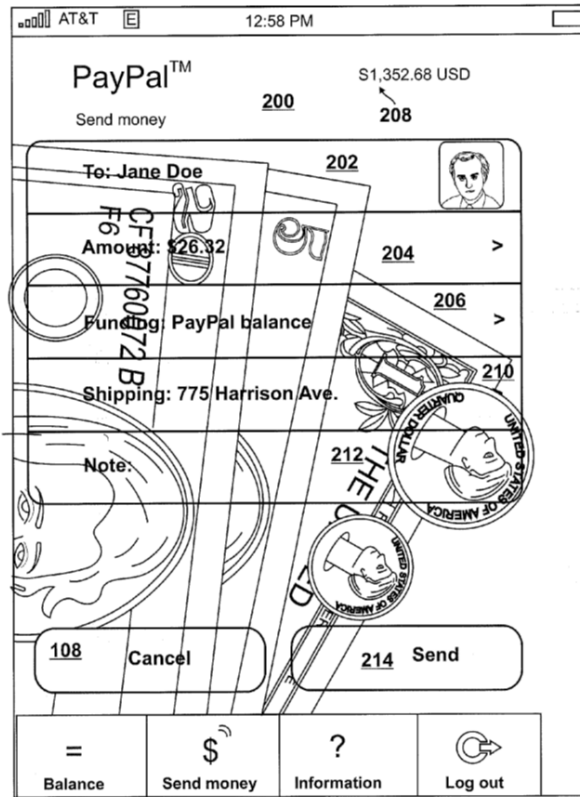


FIG. 2

APPL-1008, FIG. 2

2. Hoyos

Hoyos is directed at fraud detection with “authentication for financial transactions using biometrics.” APPL-1013, Abstract, [0002]; APPL-1003, ¶¶40-44.

Hoyos identifies that “high levels of accuracy and speed are critical” for authentication of financial transactions, identifies that one problem faced by biometric recognition systems is “the possibility of spoofing,” e.g., “a life-sized, high-resolution photograph of a person may be presented to an iris recognition system.” APPL-1013, [0009], [0011]. To address these issues, as illustrated in FIG.

1 of Hoyos below, Hoyos describes an authentication method that has high levels of accuracy and speed and protection against spoofing, which is based on a combination of biometric match and liveness analysis. APPL-1013, [0017], [0012], [0011], [0018]-[0021], claims 5-8 (describing various liveness determination techniques based on “live, human eye,” “finger or palm temperature” etc.).

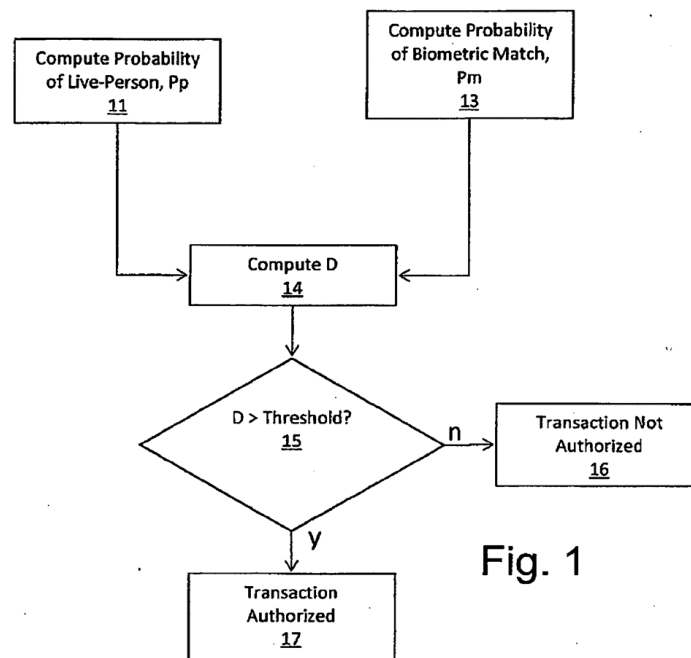


Fig. 1

APPL-1013, FIG. 1

Hoyos provides that “by combining in one algorithm the live-person result with the match result” in its biometric authentication, various advantages are achieved, including addressing spoofing; “making it much more difficult for an attempted fraudster to refine fraudulent methods” by eliminating clear feedback; greatly reducing “the reject rate of true authentic” by using the liveness

probability less sensitive to conditions like illumination changes; providing “an enormous deterrent to criminals;” and by ensuring that some live-person data is captured, providing “a means to perform customer redress.” APPL-1013, [0024], [0026], [0027], [0029].

Hoyos describes various techniques to perform liveness detection in biometric authentication system to improve fraud detection, where “the term liveness being used herein 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.” APPL-1013, [0012], [0011], [0018]-[0021], claims 5-8 (describing various liveness determination techniques based on “live, human eye [that] will respond by dilating the pupil,” “whether the first reflection and the second reflection were formed by a curved surface consistent with a human eye,” “detecting a human eye when the first portion of the first image differs from the second portion of the second image,” “measuring finger or palm temperature and comparing the resultant measured temperature to expected temperature for a human.”).

3. Varghese

Varghese titled “System and Method for Fraud Monitoring, Detection, and Tiered User Authentication” was filed by Bharosa Inc., “a leading provider of

fraud prevention and strong authentication security solutions” acquired by Oracle in 2007. APPL-1022, 1; APPL-1003, ¶¶45-46.

As shown in FIG. 14 of Varghese below, Varghese describes using multifactor real-time authentication for fraud detection for electronic transactions including financial transaction systems. APPL-1010, [0145], FIG. 14.

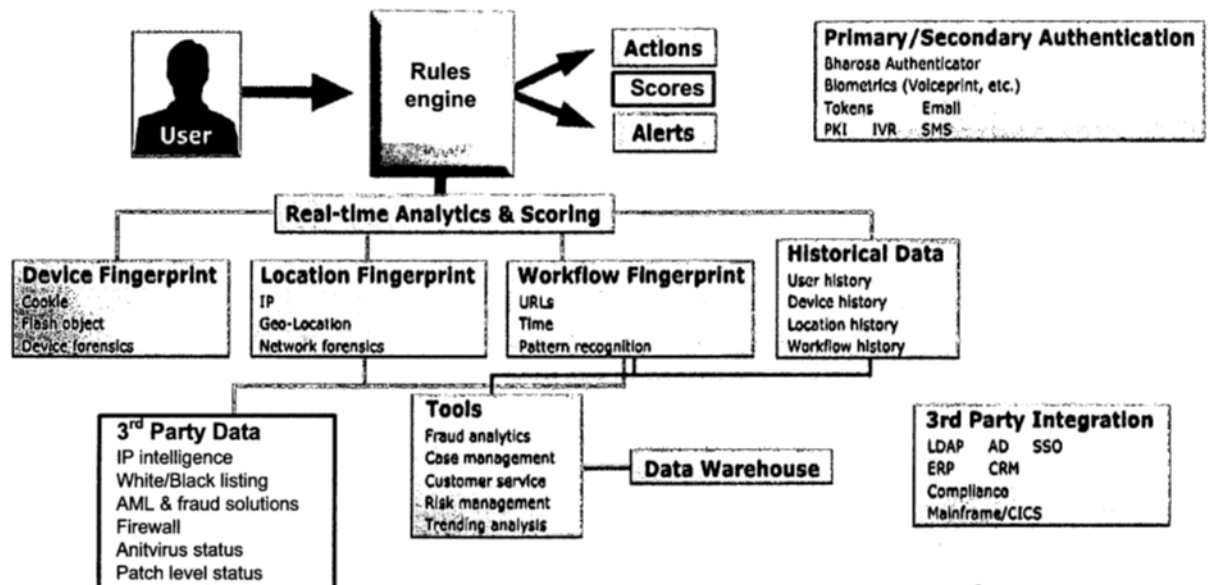


FIG. 14

APPL-1010, FIG. 14

Varghese describes performing multifactor real-time authentication (including location authentication using “Geo-Location” and voice authentication (e.g., using “Biometrics (Voiceprint, etc.)”) for improved fraud analysis. APPL-1003, ¶47; APPL-1010, FIG. 14. Varghese describes transaction authentication (“post-authentication”) separate from login authentication (“pre-authentication”), where fraud analytics “can be enforced during pre-authentication, for example

when a user is being authenticated, or during post-authentication, for example **when a user is making transaction requests.**” APPL-1010, [0097]-[0099]; *see also* APPL-1010, [0081], [0084], [0088], [0140], [0142], claim 31.

4. FFIEC Guidance

The Federal Financial Institutions Examination Council (FFIEC) is a formal U.S. government interagency body composed of five banking regulators (including FDIC) and is “empowered to prescribe uniform principles, standards, and report forms...to promote uniformity in the supervision of financial institutions.”³ On Oct. 12, 2005, FFIEC issued its guidance titled “Authentication in an Internet Banking Environment” that describes “enhanced authentication methods that regulators expect banks to use.” APPL-1037; APPL-1039, 1. The Guidance was publically available to a POSITA interested in the security electronic transactions. APPL-1039; APPL-1003, ¶¶47-52 (citing APPL-1039, APPL-1040, Google Scholar cites, archive.org links, and patent disclosures referencing Guidance as the driver for multifactor authentication in financial transacitons).

The Guidance explains that “[a]ccount fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation,” and

³ <https://web.archive.org/web/20051028001652/http://www.ffiec.gov/>.

financial institutions should implement “multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.” APPL-1037, 1-2.

Appendix of the Guidance discusses authentication techniques for the multifactor real-time authentication, including “Biometrics” (“Something a person is”/ “something you are”) and physical location authentication including “Internet Protocol Address (IPA) Location and Geo-Location.” (“Something a person has”/“something you have”). APPL-1037, 2, 7, 11-12; APPL-1010, [0035]. Biometrics techniques that include face recognition systems using facial images captured by cameras including “**tests for liveness**, such as blinking eyes.” APPL-1037, 11. Physical location authentication is used “to limit Internet users by **determining where they are** or, conversely, where they are not.” APPL-1037, 12.

5. Analogous Art

Stone, Hoyos, Varghese, Guidance are analogous art to the '010 patent, because each is at least (1) in the same field of endeavor (electronic financial transactions); or (2) reasonably pertinent to a problem with which the inventor of the '010 patent was involved (e.g., fraud detection in electronic financial transactions). APPL-1003, ¶53. Compare ('010 Patent) APPL-1001, Title (“Method, Medium, and System for Reducing Fraud”), Background of the Invention (“Fraud can also be perpetrated in the context of electronic transactions.

Electronic 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."); APPL-1008, Title ("Currency Display"), [0001]-[0004] (describing electronic financial transactions), [0045] (considering "**biometric id**" and "security"); APPL-1013, Title ("Fraud Resistant Biometric Financial Transaction System and Method"), Abstract, [0002] ("This invention relates to biometric identification and authentication systems and methods, more particularly to authentication for financial transactions using biometrics."); APPL-1010, Title ("System and Method for Fraud Monitoring, Detection, and Tiered User Authentication"), [0145] (describing additional authentication where the "service provider is a bank or other financial institution which seeks a higher security authentication interface for certain transactions.").

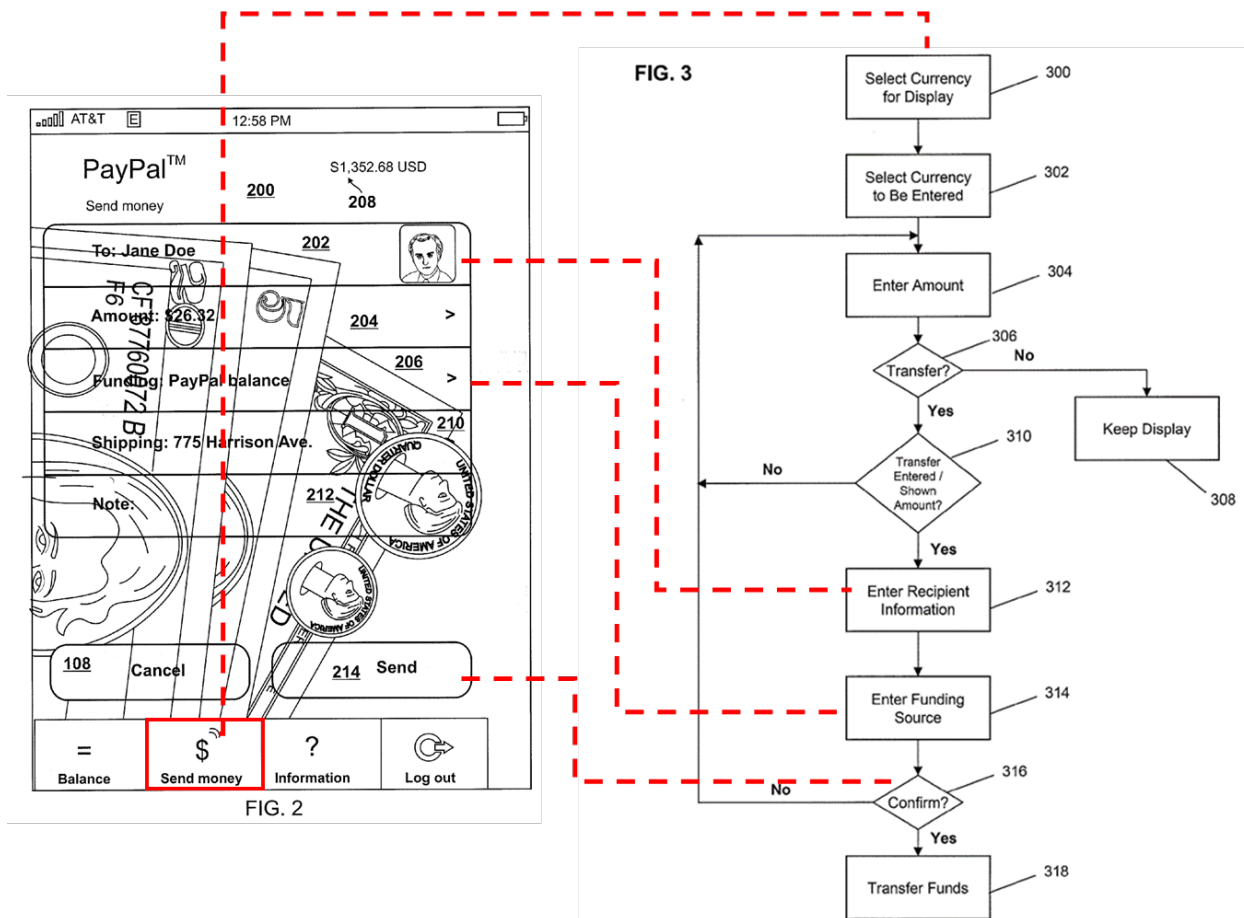
B. Ground 1: Claims 1-2, 4-6, 9-10, 12-14, 17, 20-21, and 23 are Rendered Obvious under §103(a) over Stone in view of Hoyos.

1. Combination of Disclosures/Embodiments of Stone

A POSITA would have been motivated to combine disclosures or embodiments of Stone, e.g., FIG. 2 and 3, to provide a transaction system using user interfaces (e.g., as taught by FIG. 2) for performing an electronic transaction (e.g., as taught by FIG. 3). *Boston Scientific 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."). APPL-1003, ¶¶54-58.

While FIG. 3 of Stone is a flowchart showing a method for performing an electronic transaction, and FIG. 2 shows a display on a user device, a POSITA would have understood that the display of FIG. 2 and modification thereof could be used to implement the embodiment of FIG. 3, e.g., by adding, removing, modifying components, or by using alternative design choices of buttons and icons. APPL-1008, [0055]-[0056] (“It is contemplated that various alternate embodiments and/or modifications to the present invention, whether explicitly described or implied herein, are possible in light of the disclosure. For example, steps shown in FIG.3 or described in connection with FIG. 3 may be omitted, performed in different order, modified, or added, while still achieving advantages of the present disclosure. Furthermore, the visual representation of the currency may be static or dynamic, i.e., the visual can be an animation or a storyboard of an animation showing coins rolling or any other movement.”).

An example implementation relationship with FIGs. 2 and 3 of Stone is provided below.



APPL-1008, FIGS. 2 and 3, annotated

As shown in the example implementation of Stone above, various user actions in FIG. 2 correspond to the steps of FIG. 3, e.g., block 202 corresponds to block 312, block 206 corresponds to block 314, and block 214 corresponds to block 316. After the user clicks the ““\$Send money” icon,” the user interface for a financial transaction is displayed in the portion above the bottom task bar of FIG. 2, and the method of FIG. 3 or an obvious variation thereof begins to perform.

Any modification needed for combining the embodiments of FIGS. 2 and 3 based on design needs would have been within the skills of a POSITA. For

example, while FIG. 2 does not include a user interface item corresponding to block 306 (“transfer?”) of FIG. 3, techniques for implementing user interface items (e.g., icon or button) for block 306 were well-known. As shown in the annotated figures in the example implementation, after a user click the “\$Send money” icon in the bottom task bar of FIG. 2, a financial transaction (e.g., sending money to another user) is initiated.

2. Combination of Stone and Hoyos (“Stone-Hoyos”)

A POSITA would have been motivated to apply Hoyos’ teaching of fraud resistant biometric financial transaction system 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. APPL-1013, [0015], [0017]-[0022]; APPL-1003, ¶¶59-68.

As discussed at IX.A.5, Stone and Hoyos each are analogous art to the ’010 patent. APPL-1003, ¶60 (APPL-1008, [0045]; APPL-1013, Title, Abstract, [0002]).

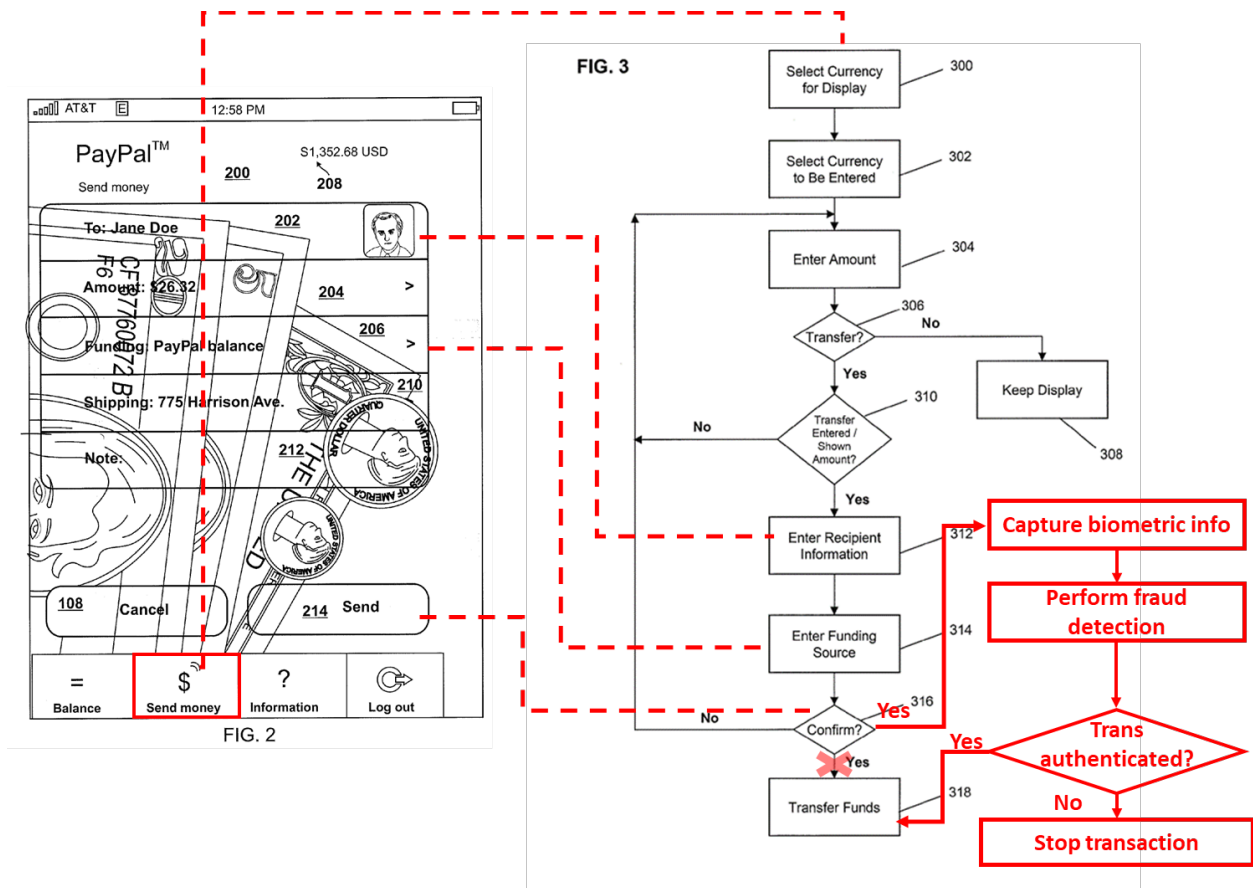
Further, it was well-known that financial transactions of Stone had a need for authentication including fraud detection (e.g., with higher levels of security for some transactions). APPL-1003, ¶61; APPL-1013, [0009], [0011]; APPL-1010, [0148] (“For example, a bank or other financial institution may wish to invoke a

higher security authentication interface during a session before transactions over a certain amount are sent to the server.”); APPL-1016, FIG. 3, [0073] (describing that for completing a financial transaction, “the transaction **must then be authenticated** before proceeding,” and “the **necessary authentication level is determined based on the transaction criteria**... based on factors such as value and type of transaction, as well as other factors.”).

In view of Stone’s need to implement authentication with fraud detection, a POSITA would have implemented biometric authentication and fraud detection as taught by Hoyos in the system of Stone. APPL-1003, ¶62. By authorizing transactions “by combining in one algorithm the live-person result with the match result,” various advantages are achieved using Hoyos’ biometric authentication method, including addressing spoofing; “making it much more difficult for an attempted fraudster to refine fraudulent methods” and thereby reducing iterative attacks by eliminating clear feedback; greatly reducing “the reject rate of true authentications” by using the liveness probability that is less sensitive to conditions like illumination changes; providing “an enormous deterrent to criminals since the system is acquiring biometric data that they have no idea can or cannot be used successfully as evidence against them;” and by ensuring that some live-person data is captured, providing “a means to perform customer redress.” APPL-1013, [0024], [0026], [0027], [0029]. Such combination is also consistent with the regulatory

drive for multifactor authentication for financial transactions, where a POSITA would have implemented the biometric authentication of Hoyos (“Something a person is”/“something you are”) together with another authentication factor. APPL-1037, 7.

To achieve such an improved financial transaction system with biometric authentication, POSITA would have been motivated to combine teachings of Stone and Hoyos according to the following Stone-Hoyos example, illustrated based on annotated FIGS. 2 and 3 of Stone describing systems and methods for performing a financial transaction (fund transfer) and incorporating Hoyos’ biometric authentication teachings. APPL-1003, ¶63; APPL-1008, FIGS. 2 and 3; APPL-1013, FIG. 1, [0017].



**Example of Stone-Hoyos
(annotated based on APPL-1008, FIGS. 2 and 3)**

As shown in the example of Stone-Hoyos above, a POSITA would have been motivated to implement Hoyos' authentication phase of the transaction authentication (e.g., including capturing images for liveness analysis and as an input image for biometric information comparison) after a user confirms a user transaction request, which is at least after a user interaction with an icon (e.g., user clicking the "\$Send money" icon of FIG. 2) to initiate the transaction request, and after user interactions with icons to continue (e.g., blocks 300-314) and confirm (e.g., block 316) the transaction request. APPL-1003, ¶64.

A POSITA would have understood that performing authentication including capturing authentication data (e.g., biometric information) after and in response to user transaction request confirmation had various benefits over the alternative design choice of using previously captured authentication information for transaction authentication (e.g., liveness analysis or for comparison with the enrollment data), including for example, risk-based contextual authentication adaptive to a particular transaction request and its assessed risk and capturing more accurate data by avoiding imposters from communicating based on stolen biometric data, reducing spoofing. APPL-1003, ¶65 (citing APPL-1013, [0028] (“A higher transaction may be authorized if the value of [decision probability] D is higher”); APPL-1010, FIG. 14, [0097]-[0099], TABLE 10; APPL-1015, FIG. 4; APPL-1035, 4:60-62; 4:66-67).

A POSITA would have reasonably expected to succeed in configuring Stone-Hoyos to leverage Hoyos’ biometric authentication functionality since its implementation would have required only routine knowledge well within the skill of a POSITA prior to the earliest effective filing date. APPL-1003, ¶66. Stone and Hoyos each reference the financial transaction system performed using user devices well-known to have/to be easily connected to cameras for obtaining photographs for face biometric. APPL-1008, [0004] (describing various user devices, which were well-known to include or easily connected with cameras);

APPL-1009, 15:22-23; APPL-1013, Title, claims 13 and 14, [0007] (“the face biometric is easy to acquire (a web camera for example).” Accordingly, a POSITA would have therefore understood and found obvious to implement, in Stone’s financial transaction system, biometric authentication including fraud detection as taught by Hoyos. APPL-1003, ¶66 (citing APPL-1013, [0040]).

It would have been within the skills of a POSITA to implement the teachings of Hoyos in the system of Stone, e.g., implementing biometric information capturing in the user device, and implementing fraud detection analysis locally using the user device, or remotely (e.g., by sending the biometric information to a payment provider device, or another remote device). APPL-1003, ¶¶67-68 (citing APPL-1016, [0040], [0042] (describing that fraud detection can “be performed **locally** or by transmission of []data to a remote source”), [0076]; APPL-1015, APPL-1016, APPL-1038); APPL-1015, FIG. 3, 4:4-10; APPL-1016, [0040], [0042]; APPL-1038, 64).

3. Claim 1

[1.0] A system, comprising:

Stone discloses or renders obvious the preamble to the extent that it’s limiting. APPL-1003, ¶¶69-72.

Specifically, as shown in FIG. 4 of Stone below, Stone describes “**a system** 400 configured to utilize the currency display over a network 402.” APPL-1008, [0040]. “System 400 includes at least a user device 404, one or more recipient 406

devices, and at least one payment provider server 408 in communication over the network 402.” APPL-1008, [0040].

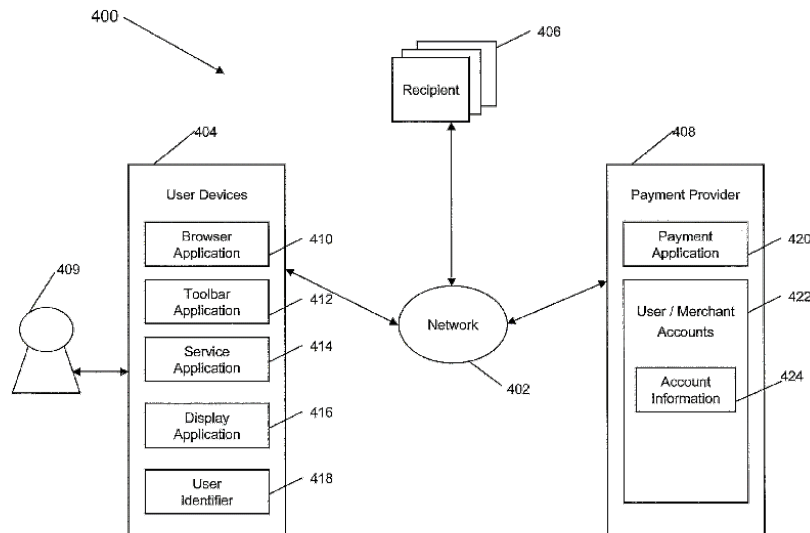


FIG. 4

APPL-1008, FIG. 4

Stone describes that “recipient devices 406 **may be the same** or have the same basic features as user device 404,” and may be implemented as “a personal computer,” “wireless telephone (e.g., cell phone), personal digital assistant (PDA), notebook computer, and/or various other generally known types of computing devices.” APPL-1008, [0044], [0046]. Stone describes that “network 402 may include the Internet and/or one or more intranets, landline networks, wireless networks, and/or other appropriate types of communication networks.” APPL-1008, [0041]. Stone further describes that its system includes software “such as program code and/or data...stored on one or more computer readable mediums.” APPL-1008, [0054].

Therefore, Stone discloses or renders obvious “[a] system” as claimed.

[1.1] one or more processors configured to:

Stone alone or Stone in view of Hoyos renders obvious this element. APPL-1003, ¶¶73-78.

First, as discussed at [1.0], Stone describes a system (e.g., system 400 of FIG. 4). The system 400 includes one or more processors (e.g., processor 504 in user device 404 alone, or in combination with other processors including the processor 504 of payment provider device 408) configured to perform processes for a transaction.

Specifically, as shown in FIG. 5 of Stone below, Stone describes “system 500 suitable for implementing embodiments of the invention, including user device 404, one or more recipient devices 406, and payment processing device 408,” where system 50 includes a processor (processing component 504). APPL-1008, [0049] (“System 500, such as part of a cell phone, personal computer and/or a network server, includes a bus 502 or other communication mechanism for communicating information, which interconnects subsystems and components, such as a **processing component 504** (e.g., processor, micro-controller, digital signal processor (DSP), etc.); APPL-1008, claim 1 (“1. A device comprising:...a **processor** configured to convert the money amount into a visual representation of a specific type of currency”).

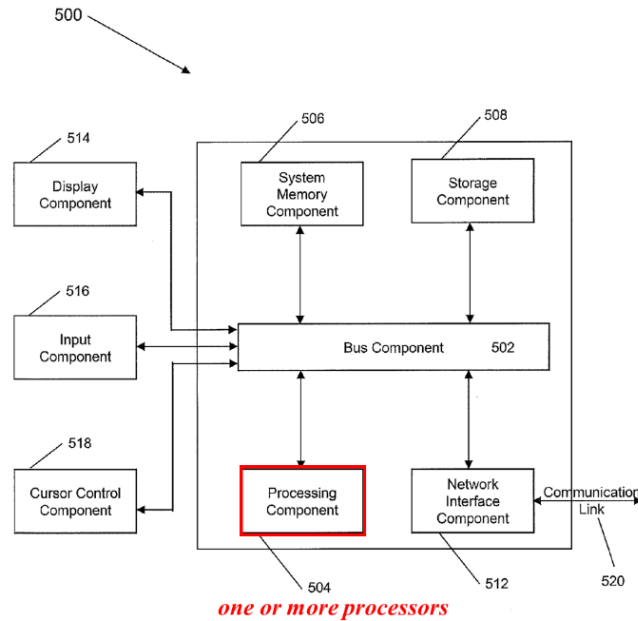


FIG. 5

APPL-1008, FIG. 5, annotated

As shown in FIG. 4 of Stone below, the system 400 includes one or more processors (e.g., processor 504 in user device 404 alone, or in combination with other processors including the processor 504 of payment provider device 408) configured to process data, such as computer program instructions, for perform processes for a transaction. *See also* APPL-1001, 2:10-13 (the '010 patent provides, “[a]s used herein, the term ‘processor’ refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.”).

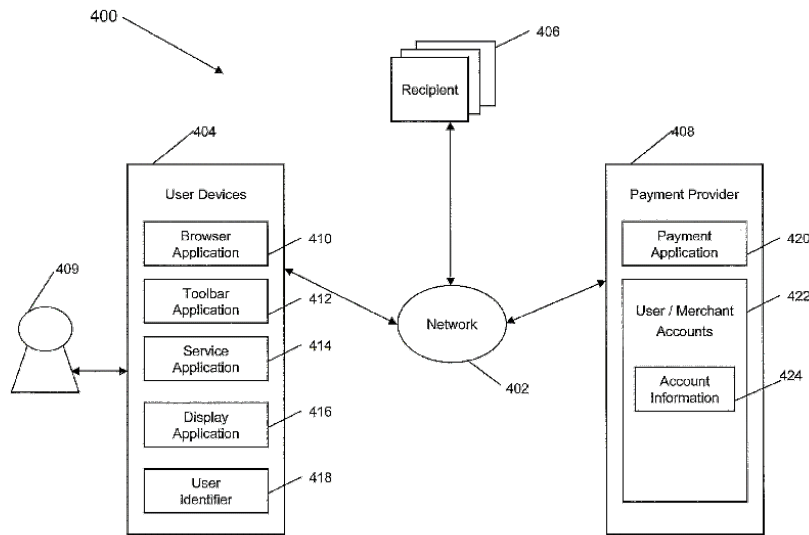


FIG. 4

APPL-1008, FIG. 4

Second, as discussed below at Ground 1:[1.2]-[1.9], Stone alone or in combination with Hoyos teaches [1.2]-[1.9], and a POSITA would have understood to modify Stone such that the one or more processors are configured to perform the processes including [1.2]-[1.9] for initiating, authenticating, and completing the electronic transaction. APPL-1003, ¶77.

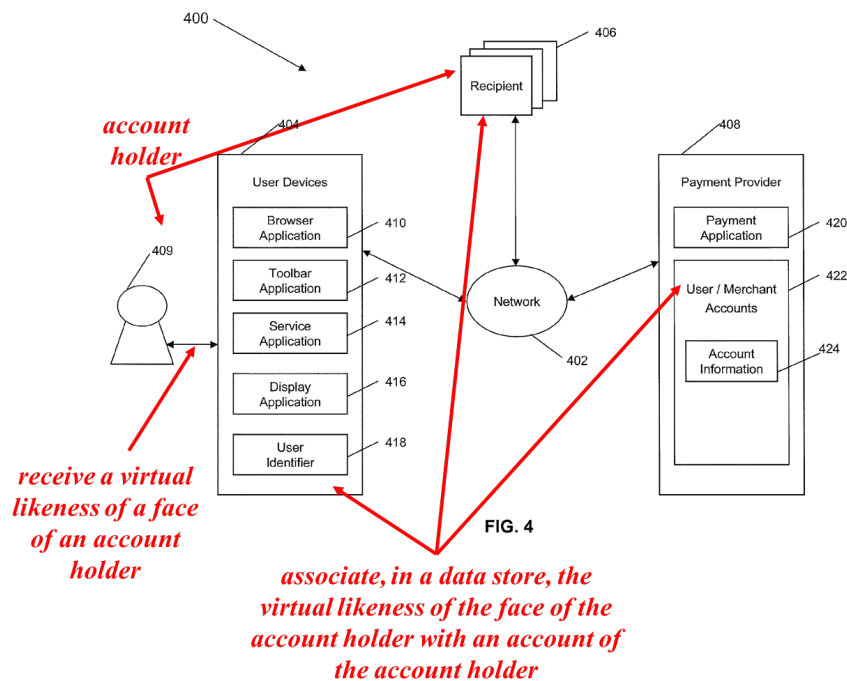
Therefore, Stone alone or Stone in view of Hoyos renders obvious “*one or more processors*” as claimed.

[1.2] receive a virtual likeness of a face of an account holder; associate, in a data store, the virtual likeness of the face of the account holder with an account of the account holder;

Stone discloses or renders obvious these elements. APPL-1003, ¶¶79-83.

First, as shown in annotated FIG. 4 of Stone below, Stone teaches one or more processors (e.g., processor 504 in user device 404 alone, or in combination

with other processors) are configured to receive a virtual likeness of a face (“photograph image”) of an account holder (user 409 (as either sender or recipient with a user account 422), and store the received photograph image in user identifier 418 of user device 408. APPL-1008, [0048] (“payment provider server 408 may be configured to maintain a plurality of user and recipient accounts 422, **each of which may include account information 424 associated with individual users, including user 409**, and the one or more recipient device 406.”); [0045] (user identifier 418 of user device 408 “**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.”); [0046] (“recipient devices 406 may be the same or have the same basic features as user device 404,” and “recipient devices 406 may include attributes related to the recipient, such as **personal** and banking information, as well as **icon information**.”); APPL-1003, ¶81 (Techniques for receiving photograph images of user profile by a user device were well-known, including e.g., “created using a digital camera function of mobile device 504 or downloaded from various servers over a communications network,” citing APPL-1019, 15:20-25); *see also* APPL-1001, claim 23 (claiming account holders to include sender and recipient, reciting “*transferring funds between the first account of the first account holder and the second account of the second account holder*”).



APPL-1008, FIG. 4, annotated

Second, Stone describes associating, using user identifier 418, in a data store (storage component 508 of user devices 404 alone, or in combination with storage component 508 of other devices including payment provider server 408), the virtual likeness of the face (photo) of the account holder (user 409) with an account (user account 422) of the account holder (user 409). APPL-1008, [0045] (“In various implementations, **user identifier 418** [including photograph image of the user] may be passed with a user money transfer request to payment provider server 408, and **user identifier 418** may be used by payment provider server 408 to **associate user 409 with a particular user account** maintained by payment provider server 408.”); [0048] (“payment provider server 408 may be configured to maintain a plurality of user and recipient accounts 422, **each of which may**

include account information 424 associated with individual users, including user 409, and the one or more recipient device 406.”), [0046] (describing similar association applies to recipient), [0020], [0036] (describing “a recipient icon on the display, such as a **picture of the recipient**”); APPL-1003, ¶82.

Therefore, Stone discloses or renders obvious this element.

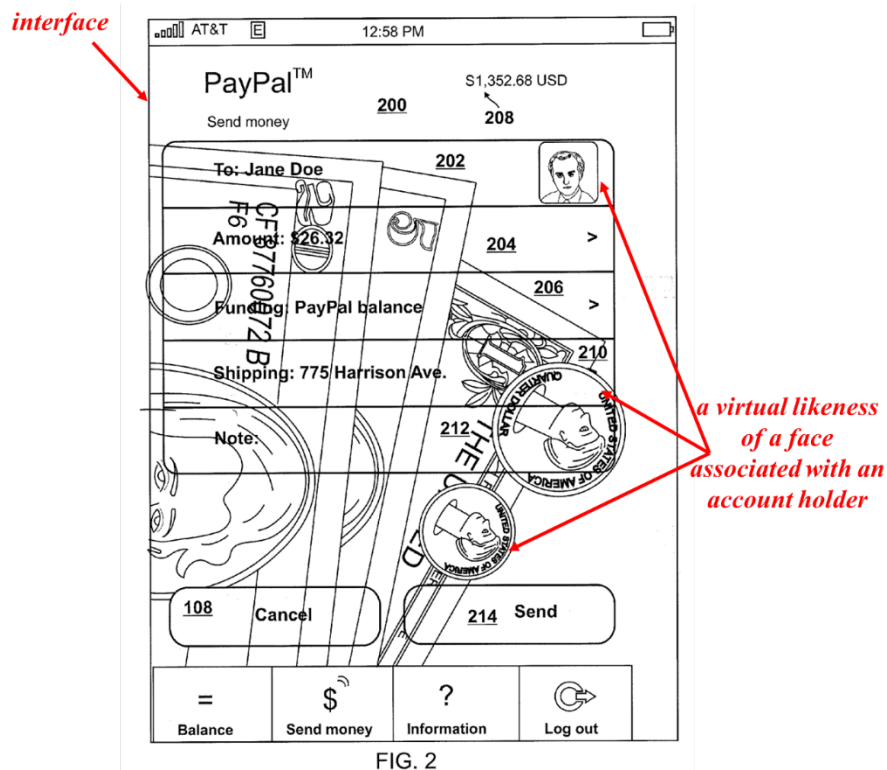
[1.3] render, in an interface, the virtual likeness of the face of the account holder;

Stone discloses or renders obvious this element. APPL-1003, ¶¶84-88.

Specifically, Stone discloses one or more processors (e.g., processor 504 in user device 404 alone, or in combination with other processors including the processor 504 of payment provider device 408) configured to *render, in an interface* (e.g., interface 100 of FIG. 1, interface 200 of FIG. 2), *the virtual likeness of the face* (e.g., either a photo of the account holder on a visual representation of the currency, or a photo of a recipient of the electronic transaction, each disclosed by Stone) *of the account holder* (user 409). The account holder could be either a sender or a recipient of a transaction. APPL-1003, ¶85.

First, as shown in annotated FIG. 2 below, Stone discloses one or more processors configured to *render, in an interface* (a display showing the visual representation of the currency), *the virtual likeness of the face of the account holder* (the photograph of the user’s face as discussed at [1.2] and [1.3] on the personalized currency). APPL-1008, claim 1 (“1. A device comprising: an input

device configured to allow a user to enter a money amount; a processor configured to convert the money amount into a visual representation of a specific type of currency; and **a display showing the visual representation of the currency.**”); APPL-1008, [0007] (“The display foreground can include recipient name, amount, funding source, shipping address, etc....In other embodiments, the user may select or create his own currency for display, such as casino chips, gold bars, **personalized currency with the user’s photo**, etc. In another embodiment, the user can slide or swipe money to visual representations of other people on the screen or table to effect a money transfer.”).



APPL-1008, FIG. 2, annotated (see also FIG. 1)

Second, and additionally, as shown in annotated FIG. 2 of Stone above, Stone's photo of recipient (as shown in FIG. 2 below next to the name box 202) also discloses "*render[ing], in an interface, the virtual likeness of the face of the account holder*" as recited. APPL-1008, [0024] ("FIG. 2 shows a display 200 on a device illustrating another example of an embodiment of the present disclosure. The device can be the same as with FIG. 1. In this example, display 200 has a **name box 202 indicating the recipient of funds as well as a picture of the recipient**...and a send button 214 to transfer the funds in noted in box 204."); *see also* APPL-1008, [0020], [0036] (describing that for choosing the recipient of the transaction, "the user display may visually show other users" using "a recipient icon on the display, such as a **picture of the recipient**").

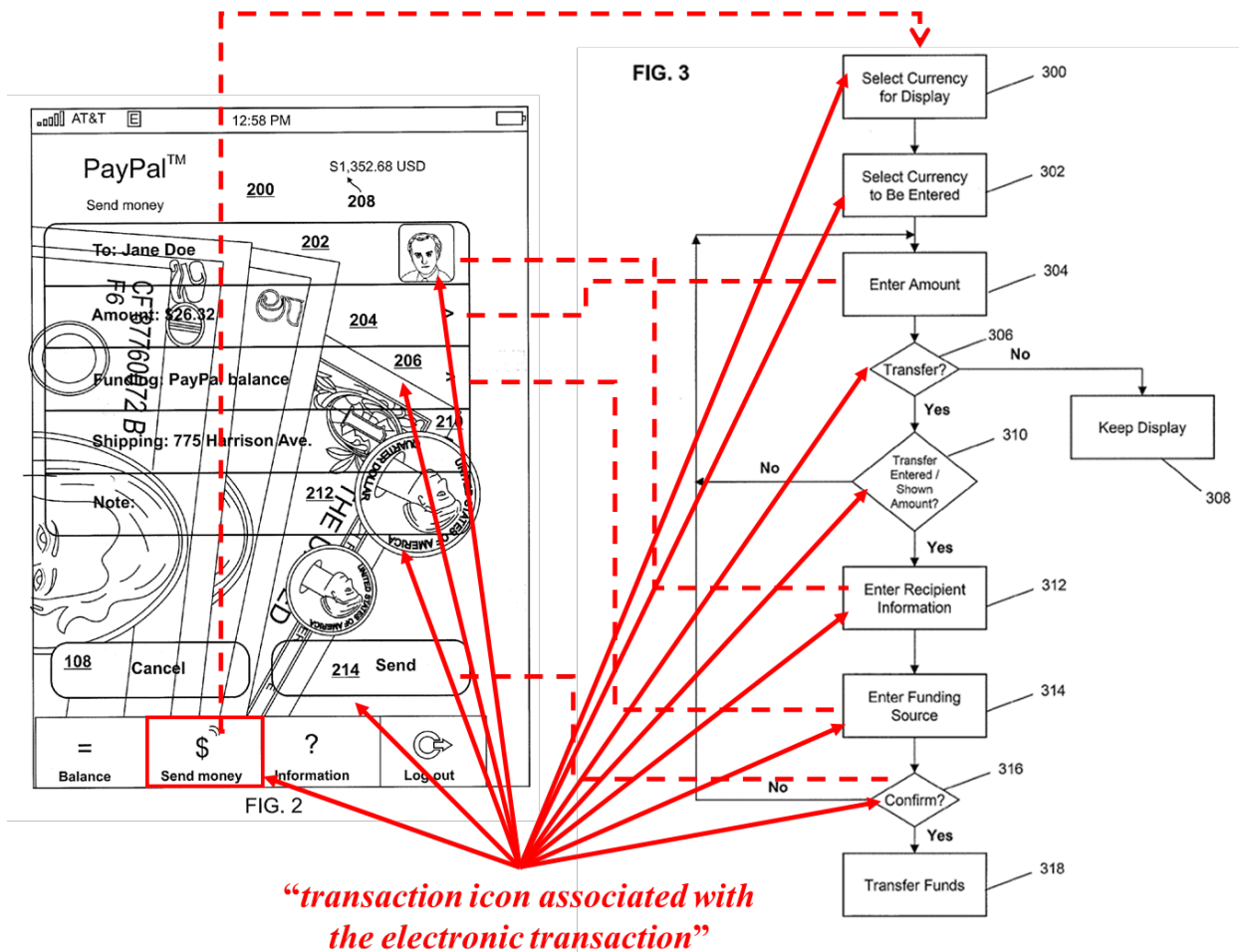
Therefore, Stone discloses or renders obvious "*render, in an interface, the virtual likeness of the face of the account holder*" as claimed.

[1.4] render a transaction icon associated with an electronic transaction, wherein the transaction icon is rendered in the interface with the virtual likeness of the face of the account holder;

Stone discloses or renders this element obvious. APPL-1003, ¶¶89-92.

First, as shown in annotated FIGS. 2 and 3 of Stone below, each of the annotated control elements (e.g., "\$Send money," 202, 206, 214, personalized currency, 300, 302, 306, 312, 314, and 316) and other control elements (e.g., "Send," "Confirm," or "Proceed" described in Stone) teaches a transaction icon in

the interface with the account holder image (e.g., interface of FIG. 2), and the transaction icon is associated with the electronic transaction as claimed, because each of these annotated items/blocks is implemented 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. APPL-1003, ¶90.



APPL-1008, FIGS. 2 and 3, annotated

Second, to the extent that any of the control elements described above is not explicitly described as a transaction icon in Stone, a POSITA would have been

motivated to implement the control elements using a transaction icon, because icon and button are alternative design choices for control elements, and using transaction icons provides “a more visually rich interface.” APPL-1008, [0016], [0004] (recognizing that “icon” and “button” are alternative design choices, stating that “[t]he consumer typically clicks on an icon or button to make the transfer.”), [0038] (describing using icons for improved visual presentation, stating “the display may show the specific card, such as a PayPal card, Visa, MC, AMEX, etc., as contrasted to a generic representation of a card or no visual at all.”), [0035]; see also e.g., APPL-1008, [0024] (“In this example, display 200 has a name box 202 indicating the recipient of funds as well as a picture of the recipient,...and a send button 214 to transfer the funds in noted in box 204.”), [0025] (describing “[s]ending can be the user tapping on an appropriate button on the display, such as ‘Send,’ ‘Confirm,’ or ‘Proceed’”, where a POSITA would have understood to implement “Confirm?” (block 316) of FIG. 3), [0020], [0036] (describing “drag[ging] the currency to the other user’s icon to transfer the funds to the other user,” or sliding the currency to the recipient’s icon); APPL-1003, ¶91.

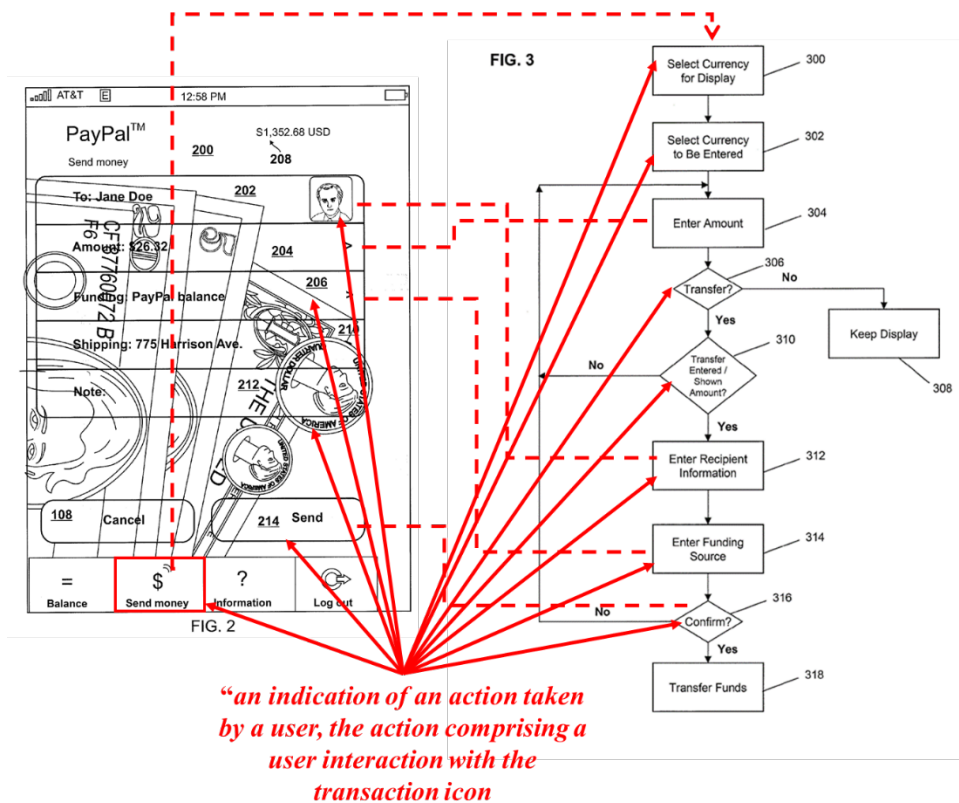
Accordingly, Stone discloses or renders obvious this element.

[1.5] receive an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the interface with the virtual likeness of the face of the account holder;

Stone discloses or renders this element obvious. APPL-1003, ¶¶93-98.

First, as discussed at [1.4], each of the annotated control elements of Stone (e.g., “\$Send money,” 202, 206, 214, personalized currency, 300, 302, 306, 312, 314, and 316) and other control elements (e.g., “Send,” “Confirm,” or “Proceed” described in Stone) teaches a transaction icon associated with the electronic transaction as claimed. APPL-1003, ¶94.

Second, as shown in annotated FIGS. 2 and 3 of Stone below, the processor is configured to receive an indication of an action taken by a user, the action comprising a user interaction with each of these transaction icons. APPL-1003, ¶95.



APPL-1008, FIGS. 2 and 3, annotated

Dr. Jones provides various additional examples of user interactions with transaction icons of FIG. 2 of Stone understood by a POSITA. APPL-1003, ¶96 (describing examples of user actions relating to each of the transaction icons). It was well-known that user clicking/tapping on/sliding/dragging (including from/to) an icon discloses an “an interaction by a user with an icon” as claimed. APPL-1003, ¶96 (citing APPL-1020, 27, 34-36; APPL-1019, 6:24-26); APPL-1008, [0024], [0020], [0036]). For example, in response to a user interaction with (e.g., clicking/tapping on) the “\$Send Money” icon, the one or more processors receive an indication of user action for initiating a send money transaction request, and in response, a corresponding interface 200 for a send money transaction is displayed. It was well-known that clicking/tapping on/sliding/dragging (including from/to) an icon by a user discloses an “*an interaction by a user with an icon*” as claimed. APPL-1003, ¶96 (citing APPL-1020, 27, 34-36; APPL-1019, 6:24-26).

Similarly, to the extent that FIG. 2 does not explicitly include transactions icons for the blocks of FIG. 3 or other control elements of Stone, a POSITA would have implemented, in the user interface, corresponding transaction icons for these blocks, to serve as a visual indicator to the user for various user interactions associated with the electronic transaction (e.g., blocks 300, 302, 306 of FIG. 3 or other user actions associated with the transaction request). APPL-1003, ¶97; APPL-1008, [0025].

Accordingly, Stone discloses or renders obvious this element.

[1.6] capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information associated with a user;

Stone in view of Hoyos renders this element obvious. APPL-1003, ¶¶99-104.

First, as shown in FIG. 1 of Hoyos below, Hoyos discloses fraud resistant biometric authentication, which includes capturing biometric contextual information (e.g., “acquiring biometric data from a person” including images, palm temperature, etc.) used for fraud detection, and some captured biometric information (e.g., facial images, “finger or palm temperature”) is used to compute probability of liveness (block 11) and some captured biometric information (e.g., facial images, iris, fingerprint image, finger vein image, palm vein image, or other imagery”) is used to compute probability of biometric match (block 13). APPL-1003, ¶100; APPL-1013, [0017].

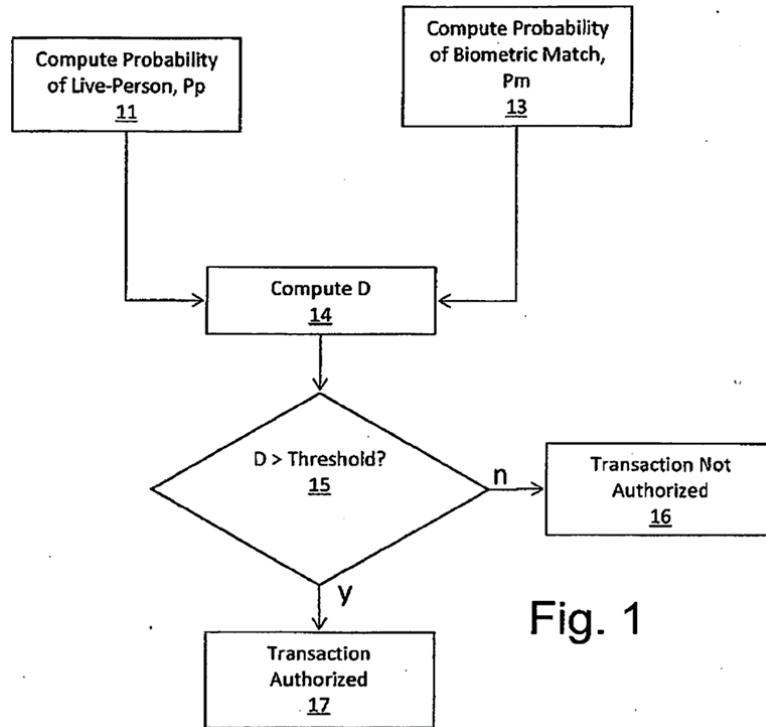


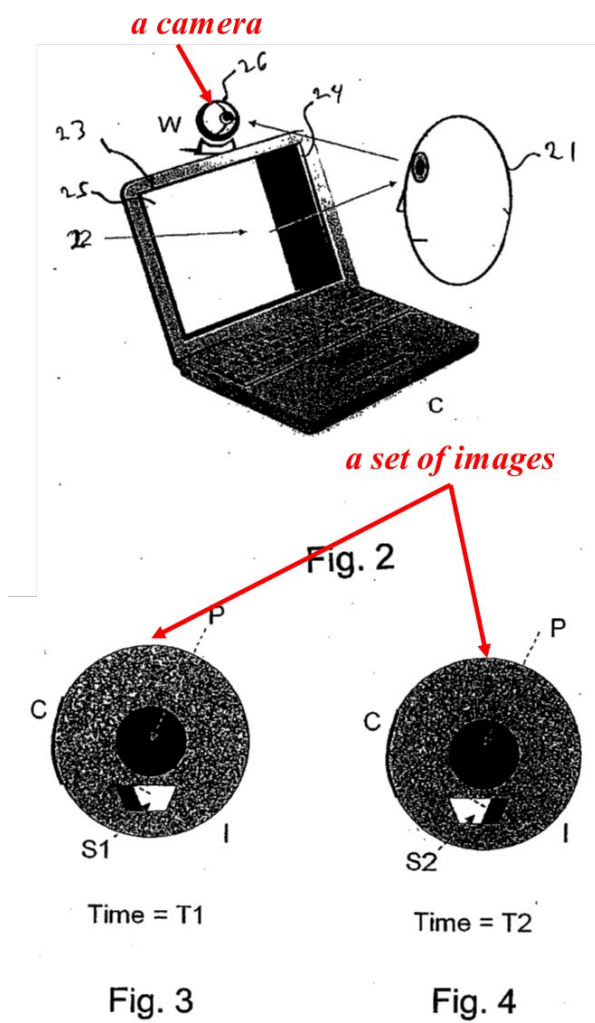
Fig. 1

APPL-1013, FIG. 1

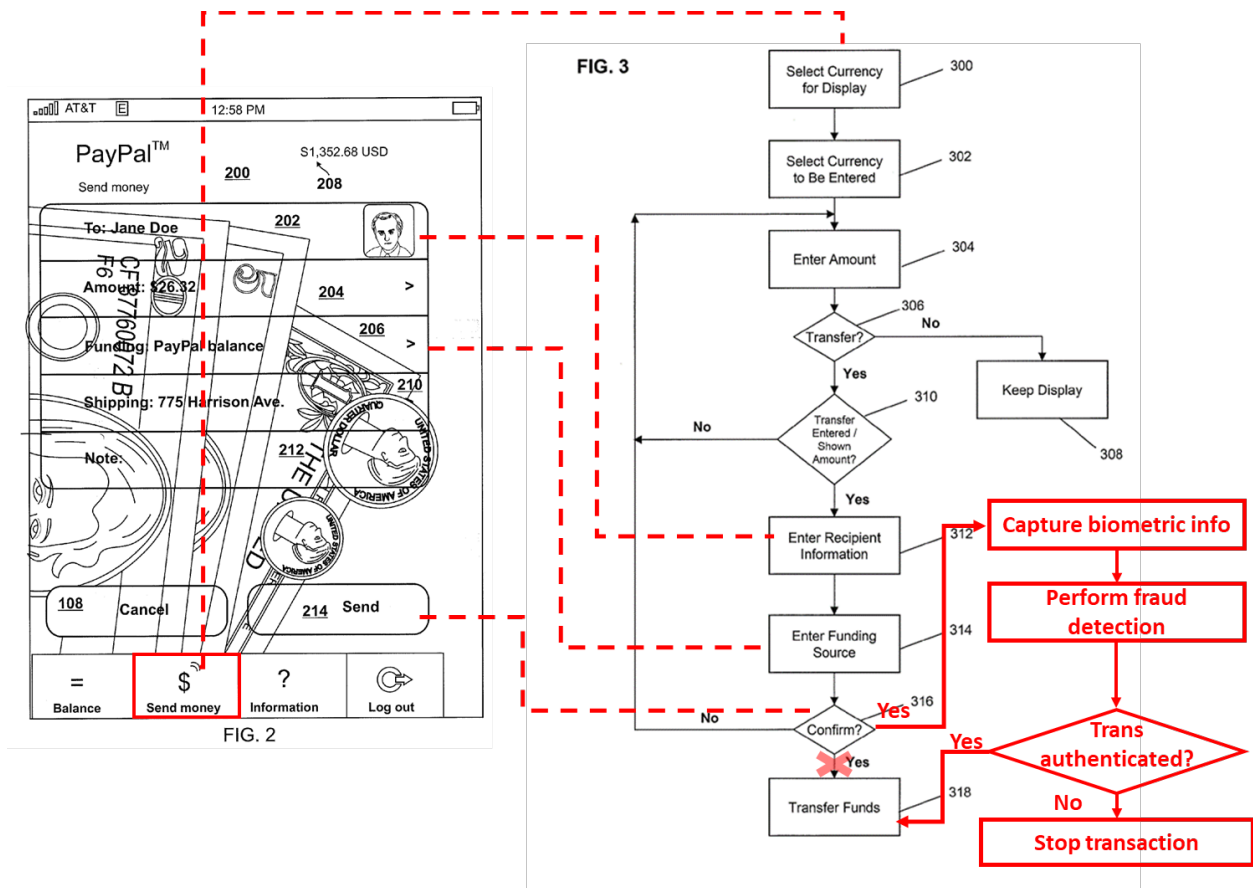
For example, Hoyos describes that biometric information includes a set of user facial images (e.g., portion thereof containing a representation of a human eye) captured using a camera (e.g., web-camera 26), in addition to “finger or palm temperature,” images for “facial features” comparison, “iris recognition, fingerprint image recognition, finger vein image recognition, or palm vein image recognition,” “other imagery,” and/or other authentication information “as will occur to those ordinarily skilled in the pertinent arts.” APPL-1013, [0003], [0012], [0018]-[0022], [0040], claims 5-10, 13-15 ; APPL-1003, ¶101 (it was well-known to capture a sequence of images (e.g., still images or video) and use adjacent

(successively captured) images/frames of a human face for liveness analysis, citing APPL-1011, Abstract; APPL-1012, Abstract).

As an example, and shown in annotated FIGS. 2, 3, and 4 of Hoyos below, Hoyos describes techniques for capturing the set of biometric information for liveness analysis, where a camera (web-camera 26) is used to capture a set of images (“obtaining first image of a user positioned in front of a computer screen from a first perspective; obtaining a second image of the user positioned in front of the computer screen from a second perspective”). APPL-1013, claim 7; [0034] (referring to FIG. 2, describing capturing multiple images for calculating the probability of a live person); claims 5-8. While FIGS. 3 and 4 of Hoyos below illustrate only the eye portions, a POSITA would have understood that Hoyos captures images of a user’s face which includes the eye portions. APPL-1003, ¶102 (citing APPL-1013, [0018]-[0020], claim 7).



APPL-1013, FIGS. 2, 3, 4, annotated



**Example of Stone-Hoyos
(annotated based on APPL-1008, FIGS. 2 and 3)**

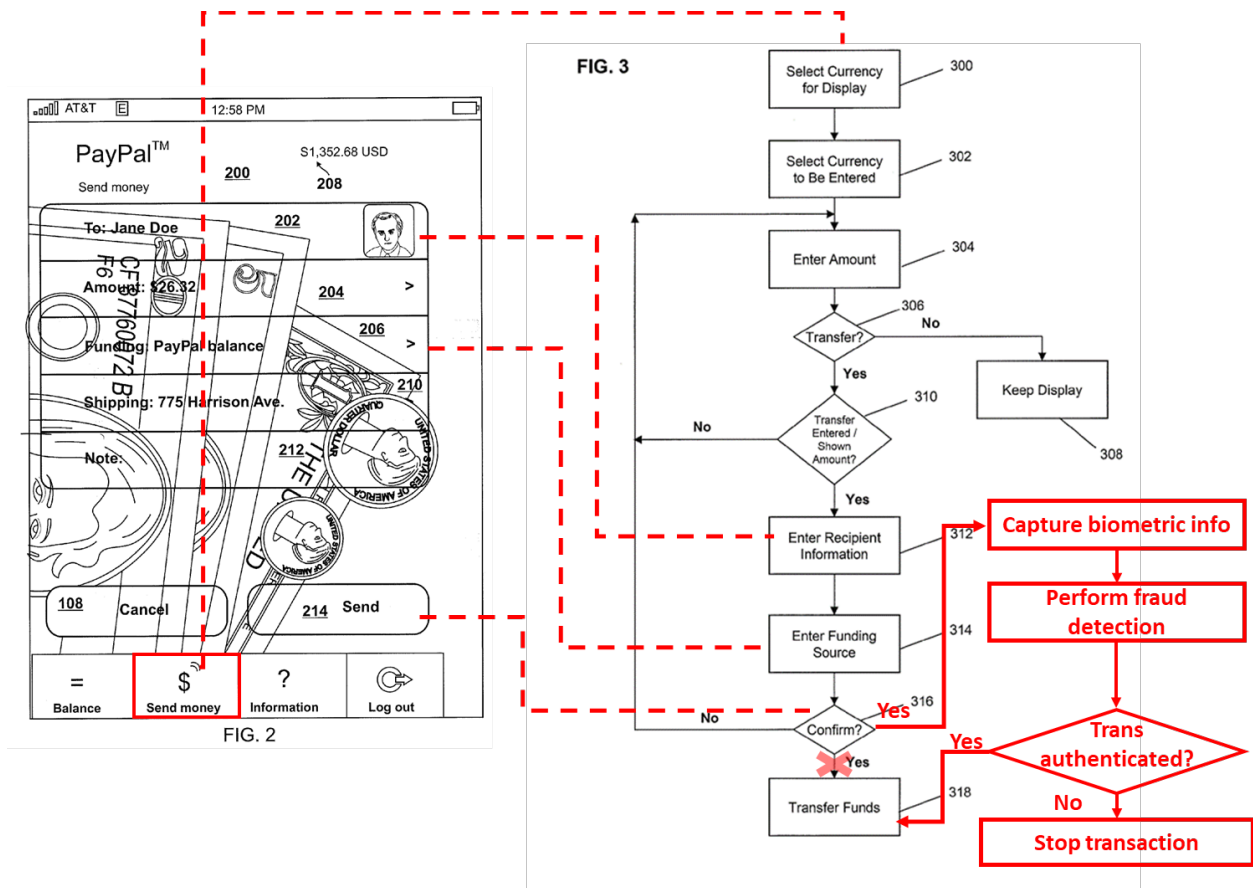
As shown in the example of Stone-Hoyos above, a POSITA would have applied Hoyos' teachings of biometric authentication including capturing biometric information (including capturing using a camera, a set of images) in Stone, for improved authentication and fraud prevention, for the benefit of providing "biometric authentication systems and methods for financial transactions for improved deterrent against attempted fraudulent transactions, and decreased rejection of valid customers" as described in Hoyos. APPL-1013, [0015]; APPL-1003, ¶103; IX.B.2: Combination of Stone and Hoyos.

Therefore, Stone in view of Hoyos renders obvious this element.

[1.7] perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises determining, based at least in part on the captured biometric information, that the user is alive; and

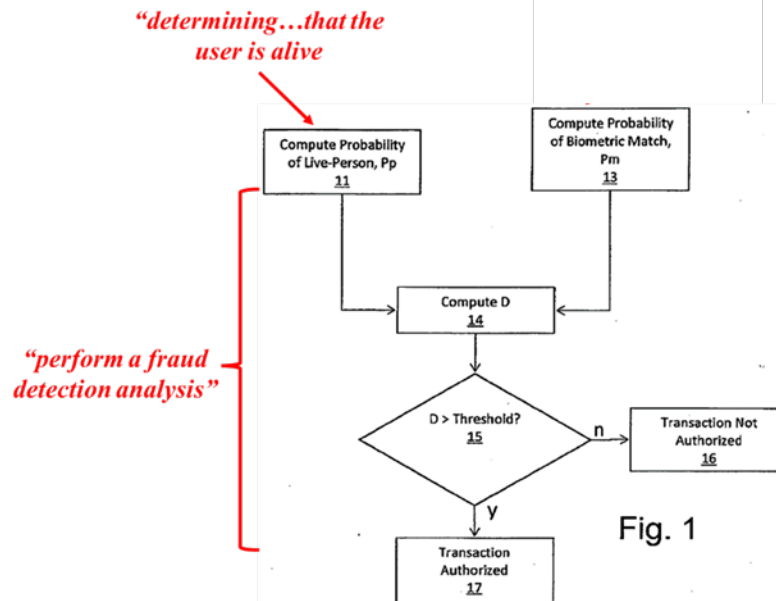
Stone in view of Hoyos renders this element obvious. APPL-1003, ¶¶105-110.

As shown in example Stone-Hoyos below, Hoyos' biometric authentication, as applied in Stone-Hoyos, describes a fraud detection analysis of the captured contextual information that includes determining, based on the captured biometric information, that the user is alive. APPL-1003, ¶106.



**Example of Stone-Hoyos
(annotated based on APPL-1008, FIGS. 2 and 3)**

Specifically, as shown in FIG. 1 of Hoyos below, Hoyos performing fraud detection analysis of the set of captured biometric information, and provides an authentication decision based on a combination of liveness analysis (e.g., based on captured images, finger or palm temperatures) and biometric match (e.g., based on captured facial features, iris, fingerprint, finger vein, palm vein, etc.). APPL-1003, ¶107 (citing APPL-1013, [0017]-[0022], [0040], claims 1, 5-8).



APPL-1013, FIG. 1, annotated

Hoyos describes that its authentication system to provide fraud resistant biometric financial transaction includes blocks to “compute 11 the **probability, Pp, 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, Pp.**” APPL-1013, [0017], FIGS. 2-4, [0034]-[0037], claims 5-7; APPL-1003, ¶108 (Hoyos describes various liveness analysis techniques, e.g., based on successively captured photos).

Hoyos describes various techniques to perform liveness detection by computing the probability of liveness in biometric authentication to improve fraud detection, where “the term liveness being used herein 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.” APPL-1013, [0012], [0011], [0018]-[0021], claims 5-8 (describing various liveness determination techniques based on “live, human eye [that] will respond by dilating the pupil,” “whether the first reflection and the second reflection were formed by a curved surface consistent with a human eye,” “detecting a human eye when the first portion of the first image differs from the second portion of the second image,” “measuring finger or palm temperature and comparing the resultant measured temperature to expected temperature for a human.”); APPL-1003, ¶109 (it was well-known to capture a sequence of images (e.g., video) and use adjacent (successively captured) images/frames of a human face for liveness analysis); APPL-1011, Abstract; APPL-1012, Abstract.

Therefore, Stone in view of Hoyos renders obvious this element.

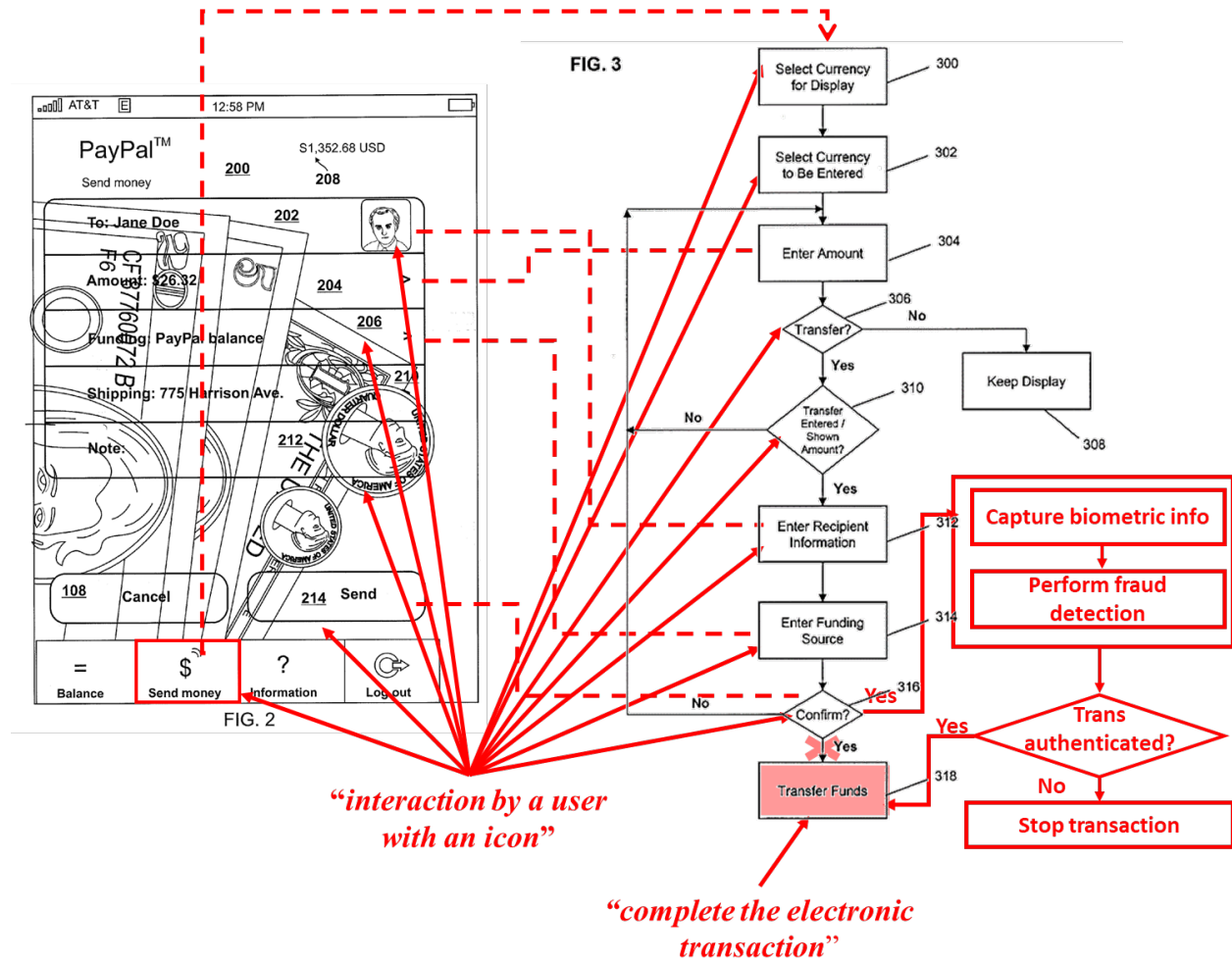
[1.8] based at least in part on both the user interaction with the transaction icon ...and performing the fraud detection analysis..., complete the electronic transaction; and

Stone in view of Hoyos renders this element obvious. APPL-1003, ¶¶111-115.

First, as discussed at [1.6], Stone-Hoyos discloses the user interaction as claimed, and as discussed at [1.8], Stone-Hoyos discloses the fraud detection analysis as claimed.

Second, continuing with Stone-Hoyos, the combination teaches completing the electronic transaction (e.g., performing transferring funds at block 318) based

at least in part on both the user interaction with the transaction icon (as discussed at [1.5]) and performing the fraud detection analysis with liveness analysis (as discussed at [1.7]).



**Example of Stone-Hoyos
(annotated based on APPL-1008, FIGS. 2 and 3)**

Specifically, as shown in the example of Stone-Hoyos, the transaction is completed **after and based on both** (1) the user interaction (e.g., "\$Send money," "214 Send"/block 316("confirm")) to indicate that the user initiates, continues, and confirms to complete the transaction, and (2) the transaction authenticated decision

by the fraud detection analysis (as discussed at [1.8]), as taught by Hoyos. APPL-1013, FIG. 1, block 17 (“Transaction Authorized” after fraud detection analysis provides a transaction authorization); *see also* ’010 patent, claim limitation [23.4] (“wherein completing the electronic transaction...comprises transferring funds”).

Therefore, Stone in view of Hoyos renders this element obvious.

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

Stone discloses or renders obvious this element. APPL-1003, ¶¶116-119.

First, as discussed at [1.1], Stone alone or in view of Hoyos renders obvious one or more processors (e.g., processor 504 in user device 404 alone, or in combination with other processors including the processor 504 of payment provider device 408) configured to perform processes for an electronic transaction.

Second, Stone further discloses a memory (memory component 506 of FIG. 5) coupled to a processor 504 in each device of the system including e.g., user devices 404, and the memory is configured to provide the processor with instructions (e.g., “instructions to create and display the proper currencies, convert currency, display various types of graphics showing transfer of currency, etc.”). APPL-1008, [0050] (“In accordance with embodiments of the invention, system 500 performs specific operations by **processor 504** **executing one or more sequences of one or more instructions contained in system memory component 506**. Such instructions may be read into system memory component

506 from another computer readable medium, such as static storage component 508”), FIG. 5, [0049], [0054].

Therefore, Stone discloses or renders obvious this element, and Stone in view of Hoyos renders obvious claim 1 in its entirety.

4. Claim 2

[2.0] The system of claim 1 wherein the transaction icon includes a graphical representation of an amount of money.

Stone discloses or renders obvious this element. APPL-1003, ¶¶120-123.

First, as discussed at [1.5] and [1.6], Stone discloses the virtual currency as an example transaction icon. Stone describes examples where user may send funds by “**drag[ging] the currency** to the other user’s icon to transfer the funds to the other user,” or sliding the currency to the recipient’s icon. APPL-1008, [0020]; [0036]. As such, the virtual currency teaches a “transaction icon” associated with an electronic transaction as claimed.

Second, Stone discloses that the transaction icon (virtual currency) includes a graphical representation of an amount of money. APPL-1008, [0006] (“The user’s device, such as a mobile phone, displays the actual currency **representing the entered amount** on background of the display or screen.”); APPL-1008, [0023] (“The user has entered \$26.32 in funds box 104, such as by using the phone touchpad. Display 100 shows **the actual currency representing this amount**, namely one twenty dollar bill, one five dollar bill, one one dollar bill, one quarter,

one nickel, and two pennies.”); APPL-1008, [0024] (“So, display 200 differs from display 100 in the amount of information provided on the screen. However, as with display 100, the actual currency representation is still present in the background.”).

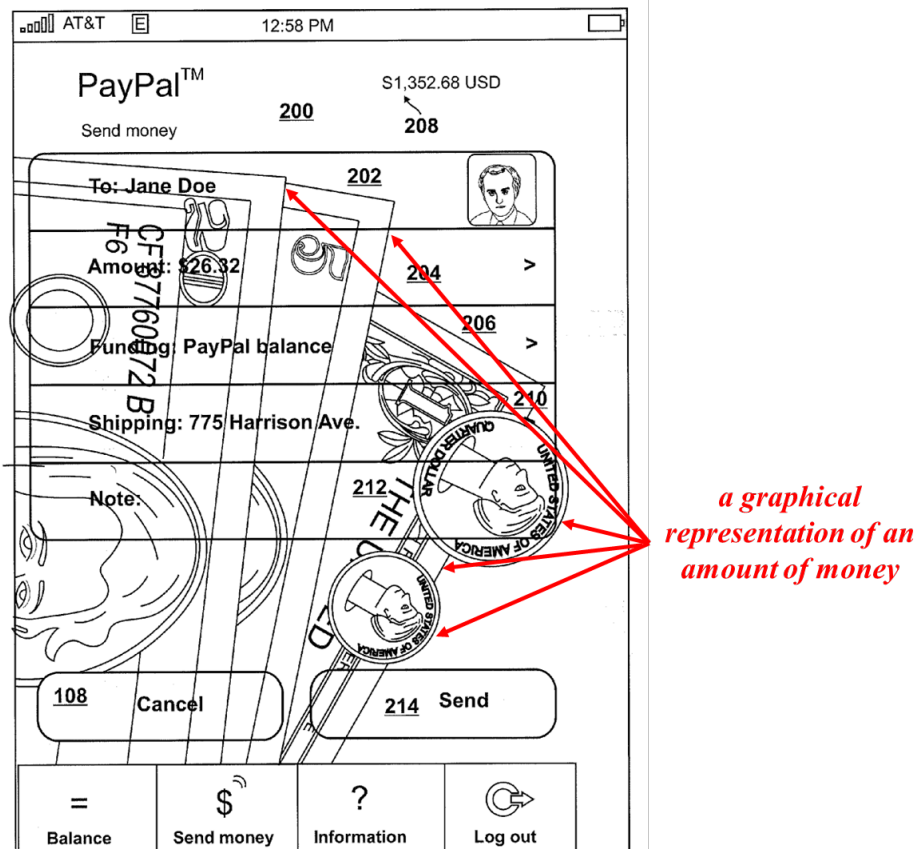


FIG. 2
APPL-1008, FIG. 2, annotated

Therefore, Stone discloses or renders obvious “*the transaction icon includes a graphical representation of an amount of money*” as claimed, and Stone in view of Hoyos renders obvious this claim.

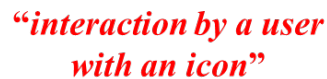
5. Claim 4

[4.0] The system of claim 1 wherein the transaction icon includes a graphical representation of a payment form.

Stone discloses or renders obvious this element. APPL-1003, ¶¶124-127.

First, as shown in example of Stone below, the icon “funding source box 206”/block 314 teaches that the icon represents a form of payment (“such as PayPal, a bank, a credit card, a debit card, etc.”), because Stone discloses clicking on that icon to make a transfer from a selected funding source. APPL-1008, [0034]; *see also* APPL-1008, [0004] (“The consumer typically clicks on **an icon or button** to make the transfer.”); APPL-1008, FIG. 2, [0024] (display including “a funding source box 206, indicating the source or account where the user’s funds will be transferred from.”). Furthermore, Stone describes that after the funding source is selected at step 314, “if the user still wants to proceed with the transfer, the user confirms the transaction, such as by **tapping** an appropriate button, and the shown funds are transferred to the desired recipient in step 318.” APPL-1008, [0035]. Further, Stone itself describes using a visual image to present the selected funding source in the display. APPL-1008, [0038] (“the display may show the specific card, such as a PayPal card, Visa, MC, AMEX, etc., **as contrasted to** a generic representation of a card or no visual at all.”). It would have been obvious to a POSITA to implement the funding source selection using an icon with the visual representation of the payment for improved visual presentation. APPL-1008,

APPL-1003, ¶125.



APPL-1008, FIGS. 2 and 3 (annotated)

APPL-1003, ¶126.

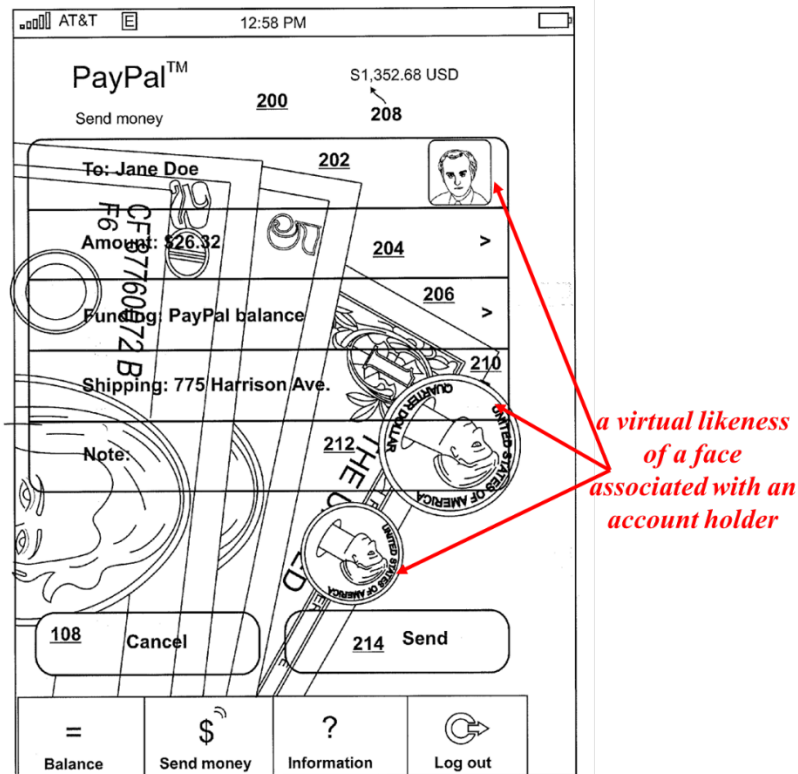
Therefore, Stone in view of Hoyos renders obvious this claim.

6. Claim 5

[5.0] The system of claim 1 wherein the virtual likeness comprises a photograph of the account holder.

Stone discloses or renders obvious this element. APPL-1003, ¶¶128-130.

As discussed at [1.2]-[1.3], Stone discloses that *a virtual likeness of a face* includes a photograph of the account holder, where the account holder is a sender, a recipient, or another user, e.g., where the account holder image (on the currency or as profile image) is rendered using “photograph image” of user identifier 418. APPL-1008, [0007] (displaying “personalized currency with **the user’s photo**,” [0024] (displaying “a picture of the recipient”), [0020], [0036]; APPL-1003, ¶129; see also APPL-1041, FIG. 6, claims 3-7 (describing using photos (e.g., downloaded from social media sites) as contact photos).



APPL-1008, FIG. 2, annotated

Therefore, Stone in view of Hoyos renders obvious this claim.

7. Claim 6

[6.0] The system of claim 1 wherein the virtual likeness comprises an avatar selected by the account holder.

Stone discloses or renders obvious this element. APPL-1003, ¶¶131-133.

Specifically, Stone combined with a POSITA's knowledge that avatar selected by the account holder is a well-known alternative of a picture for a user icon renders this element obvious. APPL-1003, ¶132. Stone's electronic transaction system provides a social networking aspect for connecting people, and user-selected avatar is a well-known user icon option for online identity. APPL-

1003, ¶132 (citing APPL-1008, FIG. 2, [0020], [0036]; APPL-1036, [0002]). As such, a POSITA would have been motivated to provide the option of user selection of an avatar as a user icon (e.g., for profile icon as sender, recipient, or other users, or on visual currency), because avatar was a well-known alternative design choice of pictures for user icon, where avatar has the benefits of providing an online identity that balances personal expression and privacy, and on the other hand, user picture has the benefits of enhanced personal recognition and trust. APPL-1003, ¶132 (citing APPL-1009, 9:30-35 (“a profile picture or avatar of Baker can be displayed on mobile device 104”); APPL-1047, 801 (avatar providing an online identity that balances personal expression and privacy))).

Therefore, Stone in view of Hoyos renders obvious this claim.

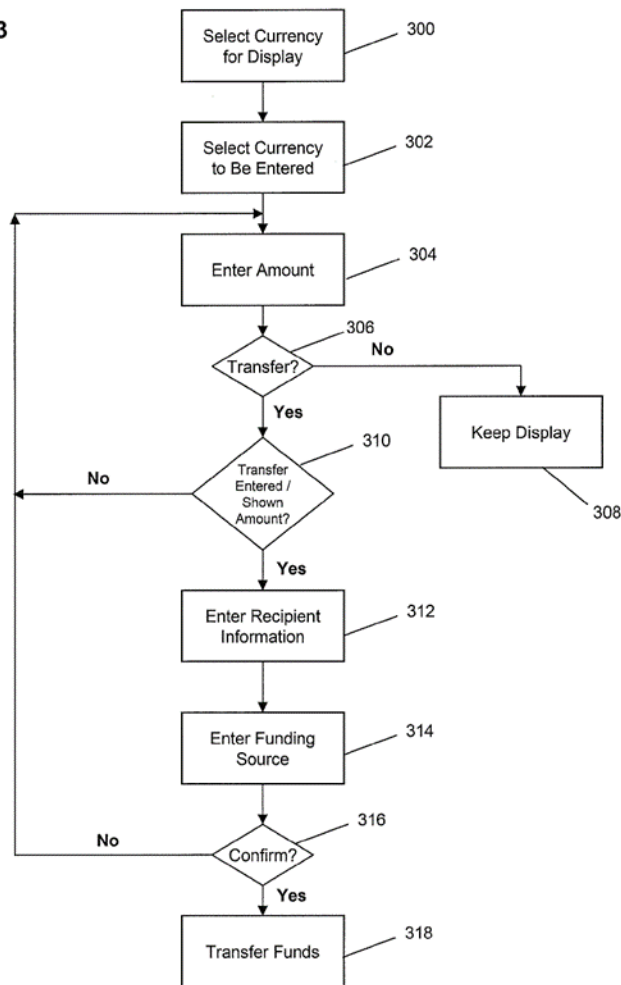
8. Claim 9

[9.0] A method, comprising:

Stone discloses or renders obvious the preamble to the extent that it is limiting. APPL-1003, ¶¶134-136.

For example, FIG. 3 of Stone describes a method for fund transfer. APPL-1008, [0029]-[0036]. Stone describes various steps of the method, including for example, selection and amount entering steps (e.g., steps 300, 304, and 314), confirmation steps (e.g., steps 306 and 316), and fund transfer step (step 318).

FIG. 3



APPL-1008, FIG. 3

Therefore, Stone discloses or renders obvious “[t]he method” as claimed.

[9.1]-[9.4]

Stone discloses or renders obvious these elements for reasons discussed at [1.2]-[1.5]. APPL-1003, ¶¶137-140.

[9.5]-[9.7]

Stone in view of Hoyos renders obvious these element for reasons discussed at [1.6]-[1.8]. APPL-1003, ¶¶141-143. Accordingly, claim 9 is obvious over Stone

and Hoyos.

9. Claims 10, 12, 13, 14

Stone discloses or renders obvious elements [10.0], [12.0], [13.0] and [14.0] for reasons discussed at [2.0], [4.0], [5.0], and [6.0]. APPL-1003, ¶¶144-147.

Accordingly, these claims are also obvious over Stone and Hoyos.

10. Claim 17

[17.0] A computer program product embodied in a non-transitory computer readable storage medium and comprising computer instructions for:

Stone discloses or renders obvious the preamble to the extent that it is limiting. APPL-1003, ¶¶148-150.

As discussed at [1.0], [1.1], and [1.9], Stone describes a system including one or more processors and a memory (*a non-transitory computer readable storage medium*) configured to provide the processors with instructions. In Stone, a computer program product is embodied in the memory and includes these instructions. APPL-1008, [0054] (“Software...such as program code and/or data, may be stored on one or more computer readable mediums”); APPL-1003, ¶149.

Therefore, Stone discloses or renders obvious this element.

[17.1]-[17.5]

Stone discloses or renders obvious these elements for reasons discussed at [1.2]-[1.5]. APPL-1003, ¶¶151-157.

[17.6]-[17.8]

Stone in view of Hoyos renders obvious these elements for reasons

discussed at [1.6]-[1.9]. APPL-1003, ¶¶155-157. Accordingly, claim 17 is obvious over Stone and Hoyos.

11. Claim 20

[20.0] The system of claim 1 wherein the captured biometric information associated with the user includes a fingerprint.

Stone in view of Hoyos renders obvious this element. APPL-1003, ¶¶158-161.

As discussed at [1.7] and [1.8], Hoyos teaches capturing biometric information associated with a user for fraud detection based on both liveness analysis and recognition using matching, where the probability of match includes fingerprint matching. APPL-1013, [0012] (“biometric recognition systems using **fingerprint**,”), [0015], [0017]-[0021], [0022] (“The probability of a match, P_m , can be calculated...by...**fingerprint image recognition**.”), claim 10.

Such use of a fingerprint is also consistent with Stone’s disclosure of “biometric id,” which is well-known to include fingerprint identification information for fingerprint recognition. APPL-1003, ¶160; APPL-1008, [0045]; APPL-1010, [0079] (“**biometric identification information (e.g., fingerprints, retinal scans, or the like)**”).

As such, in Stone-Hoyos, a POSITA would have been motivated to implement capturing fingerprint for fraud detection analysis, as taught by Hoyos, for improved security, because fingerprint authentication has high accuracy, is less

intrusive than face images, and is a mature and well-tested technology. APPL-1037, 10.

Therefore, claim 20 is obvious over Stone and Hoyos.

12. Claim 21

[21.0] The system of claim 1 wherein the captured biometric information comprises a plurality of photographs, and wherein the fraud detection analysis comprises an analysis of the plurality of photographs to determine that the user is alive.

Stone in view of Hoyos renders obvious this element and claim for reasons discussed at [1.7] and [1.8]. APPL-1003, ¶¶162-164 (citing APPL-1013, claim 7 (“wherein [probability of liveness] Pp is calculated by steps comprising...**obtaining first image** of a user positioned in front of a computer screen from a first perspective; **obtaining a second image** of the user positioned in front of the computer screen from a second perspective”).

13. Claim 23

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

Stone discloses or renders obvious this element for reasons discussed at [1.1] and [1.2], where the account includes a sender (a first account holder) with a sender account (a first account). APPL-1003, ¶165.

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

Stone discloses or renders obvious this element for reasons discussed at

[1.2], where the analysis of receiving and associating a photograph image of a applies to multiple account holders (including sender, recipient, and other users) of Stone's system, including a recipient account (a second account) of the recipient account holder (a second account holder). APPL-1003, ¶166.

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

Stone discloses or renders obvious this element. APPL-1003, ¶¶167-169.

Specifically, as discussed at [1.2] and shown in annotated FIG. 2 below, Stone teaches rendering a destination image comprising the photo/picture (virtual likeness of the face) of the recipient (the second account holder).

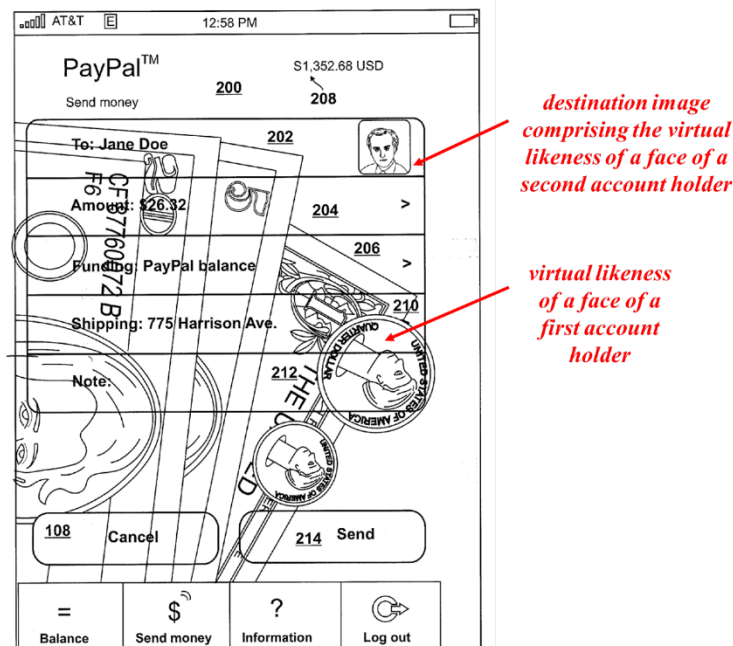


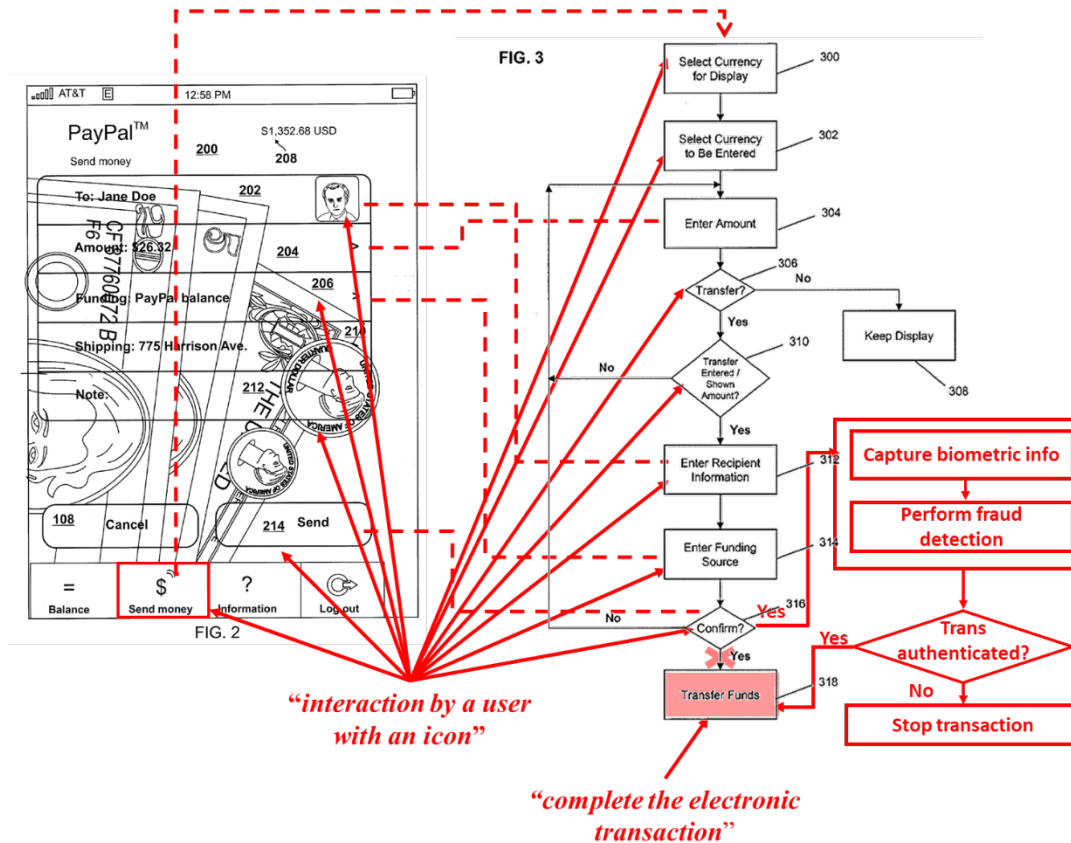
FIG. 2
APPL-1008, FIG. 2, annotated

Accordingly, Stone discloses or renders obvious this element.

[23.3] wherein completing the electronic transaction...comprises transferring funds between the first account...and the second account....

Stone in view of Hoyos renders obvious this element. APPL-1003, ¶¶170-174.

As discussed at [1.8], Stone in view of Hoyos renders obvious “*completing the electronic transaction*” as claimed, where Stone describes that completing the electronic transaction includes transferring funds (e.g., at 318) between the first account (sender) and the second account (recipient). APPL-1008, [0035] (“the shown funds are transferred [from the first account holder] to the **desired recipient** in step 318.”).



**Example of Stone-Hoyos
(annotated based on APPL-1008, FIGS. 2 and 3)**

Accordingly, claim 23 is obvious over Stone and Hoyos.

C. Ground 2: Claims 7, 15, and 22 are Rendered Obvious under §103(a) over Stone-Hoyos-Varghese.

1. Combination of Stone, Hoyos, and Varghese (“Stone-Hoyos-Varghese”)

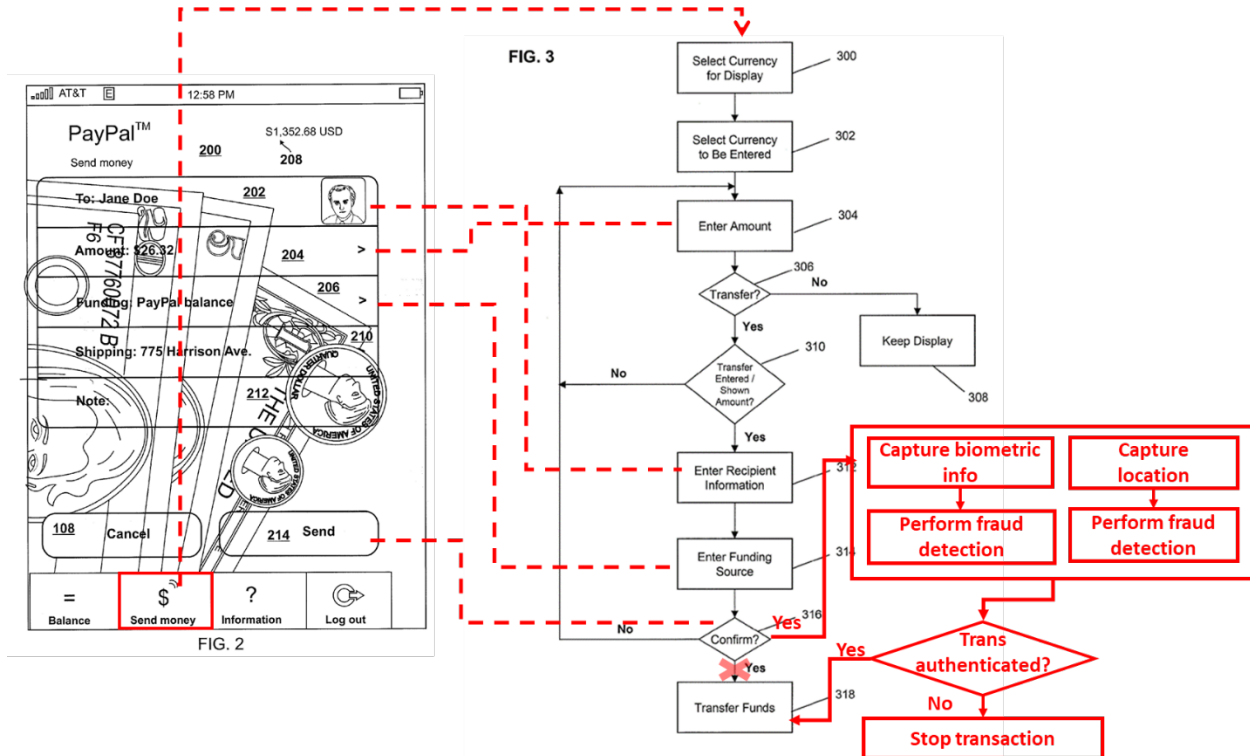
POSITA would have been motivated to apply Varghese’s teaching of multifactor real-time authentication for user transaction requests, including location authentication (capturing physical location data and performing fraud detection based on the physical location determined thereupon) in Stone-Hoyos for improved security for financial transactions. APPL-1003, ¶¶175-183.

As discussed at IX.A.5, like Stone and Hoyos, Varghese is analogous art to the '010 patent, and describes providing 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. APPL-1010, [0145]; APPL-1003, ¶176.

In view of Stone's need to implement fraud detection with high levels of accuracy and the regulatory drive for using multifactor authentication for financial transactions, a POSITA would have implemented Varghese's multifactor real-time authentication including location authentication for user transaction requests in Stone-Hoyos, for improved security. APPL-1003, ¶177 (citing APPL-1016, [0036]); APPL-1037, 1-3. Specifically, in Stone-Hoyos-Varghese, a POSITA 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. APPL-1003, ¶177 (citing APPL-1010, [0012], [0035]; APPL-1016, [0043]; APPL-1037, 7-12); APPL-1016 [0043] (describing GPS location authentication

used together with other authentication, GPS location authentication).

Based on the combined functionality of Stone, Hoyos, and Varghese, a POSITA would have been motivated to implement the following example Stone-Hoyos-Varghese for performing a financial transaction. APPL-1003, ¶178.



Example of Stone-Hoyos-Varghese (annotated based on APPL-1008, FIGS. 2 and 3)

Similar to the reasons discussed above at IX.B.2, as shown in the example of Stone-Hoyos-Varghese above, a POSITA would have been motivated to implement Varghese’s multifactor real-time authentication (including capturing authentication data and performing fraud detection thereupon) for user transaction request (also referred to as “post-authentication”) **after** a user confirms a user transaction request, 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 interactions with icons to continue (e.g., blocks 300-314) and confirm (e.g., 316) the transaction request. APPL-1003, ¶179; APPL-1010, FIG. 14, [0091], [0097]-[0099] (real-time fraud analysis enforced “during post-authentication, for example when a user is making transaction requests”), [0148], TABLE 10; APPL-1016, [0043]; APPL-1010,; APPL-1015, FIG. 4; APPL-1013, [0028]; APPL-1016, FIG. 3, [0036], [0043], [0073]; APPL-1035, 4:60-62, 4:66-67.

A POSITA 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 skill of a POSITA prior to the earliest effective filing date. APPL-1003, ¶181. For example, a POSITA would have understood to implement the enrollment phase of authentication during user registration in Stone to capture high-confidence enrollment data, and implement the authentication phase of transaction authentication (e.g., capturing biometric data and location and performing fraud analysis thereupon) after user initiates and confirms a transaction request, for providing real-time, risk-based authentication adaptive to the risk of the transaction. APPL-1003, ¶181.

Moreover, Stone already describes detection of user location, e.g., using GPS or other location-determining method. APPL-1008, [0026] (describing that

detection of the location of the user “may be determined through GPS or any other location-determining method”). Varghese describes capturing location data (e.g., IP address) and determining location based thereon (e.g., using a “geolocation service”). APPL-1010, [0140], APPL-1010, [0093] (“Location can most easily be estimated from the device’s IP address and the hierarchy of networks linking the device to the Internet.”). A POSITA would have therefore understood and found obvious to implement, in Stone, fraud detection based on location (e.g., determined using GPS, IP address, or any other suitable location-determining method) as taught by Varghese, together with biometric authentication with liveness test as taught by Hoyos, and provide multifactor real-time authentication for financial transactions. APPL-1016, [0041]; APPL-1008, [0026]; APPL-1010, [0140]; APPL-1037, 7.

2. Claims 7 and 15

[7.0/15.0] The system of claim 1/method of claim 9 wherein the captured contextual information further comprises at least one of physical location information and information spoken by the user.

Stone-Hoyos-Varghese renders this element obvious. APPL-1003, ¶¶184-191.

First, as shown in annotated FIG. 14 of Varghese below, Varghese describes, after the user confirms user transaction requests (referred to as “post-authentication”), capturing real-time contextual information including capturing real-time physical location information, which is used to determine a user physical

location for fraud analysis, where the “**Real-time** Analytics & Scoring” for authentication uses “**Location** Fingerprint” including “IP, **Geo-Location**, Network Forensics.” APPL-1010, [0097]-[0099], [0074], [0140] (describing capturing location data including IP address and determining the physical location using a “geolocation service” based on the user IP address); APPL-1003, ¶186 (citing APPL-1010, [0074], [0089], [0093], [0109]).

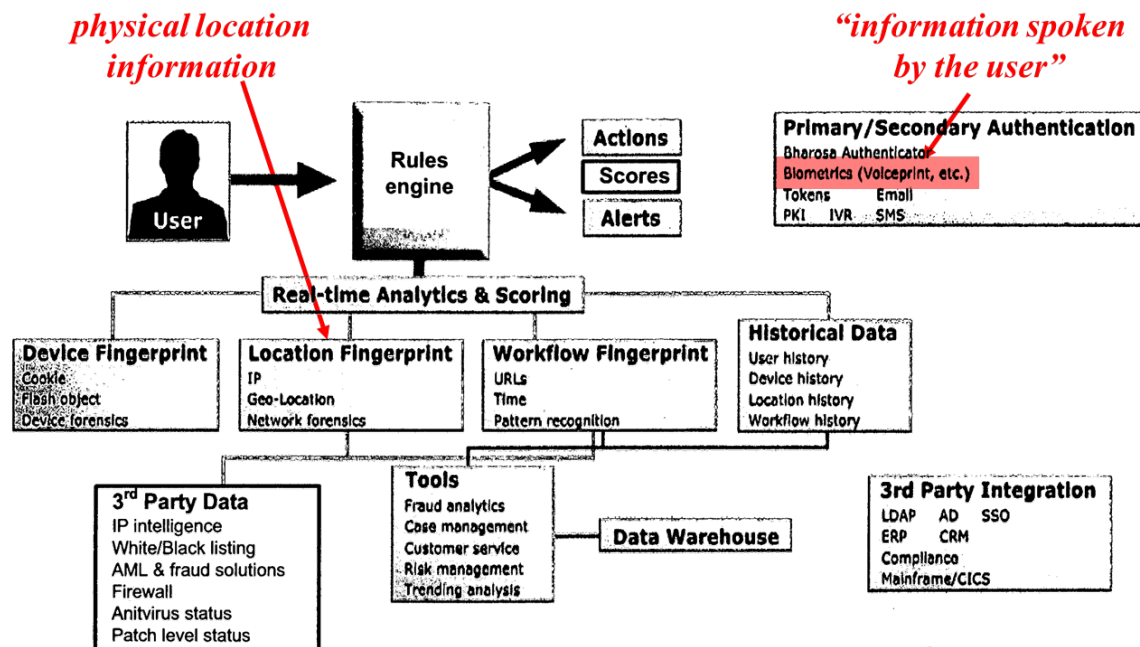


FIG. 14

APPL-1010, FIG. 14, annotated

A POSITA would have understood “real-time” authentication as described in Varghese includes both real-time capture and real-time analysis of authentication data. APPL-1003, ¶187 (citing APPL-1016, [0043]-[0044]; APPL-

1035, 4:60-62, 4:66-67 (describing using various “**real-time biometric data**”); APPL-1037, 10 (describing “live scan” for capturing biometrics data)).

Varghese’s data captured for “post-authentication,” including physical location information (for location authentication) and information spoken by the user (for voice authentication) is contextual information of the transaction, e.g., a user location from which the transaction request originates. APPL-1003, ¶188 (citing APPL-1010, [0081], [0140], [0142], claim 31).

Varghese teaches using the captured contextual information for fraud detection. APPL-1010, [0088], [0012] (“Further, certain geographic locations are known to contain an inordinate number of identity thieves. It is therefore advantageous to know where an attempt to access a server originates from.”); APPL-1010, [0078] (describing security protocols including “**call to provide voice recognition**”), [0079] (describing “**obtaining voice prints**”), [0084].

A POSITA would have been motivated to apply Varghese’s teachings of using multifactor real-time authentication including one or both of location authentication and voice authentication for fraud detection analysis in Stone, together with Hoyos’ biometric authentication, for improved and more secure financial transactions, by providing multifactor real-time authentication (e.g., using biometric authentication of Hoyos together with location authentication of location

authentication, and/or additionally with voice authentication). APPL-1003, ¶190 (citing APPL-1016 [0036]); APPL-1037, 7-13; *see also* IX.C.1.

Accordingly, Stone-Hoyos-Varghese renders obvious claims 7 and 15.

3. Claim 22

[22.0] The system of claim 1 wherein the captured contextual information further comprises captured physical location information associated with the user, and wherein performing the fraud detection analysis further comprises determining a physical location of the user based at least in part on the captured physical location information.

Stone-Hoyos-Varghese renders obvious this element. APPL-1003, ¶¶193-195.

As discussed at [7.0/15.0], Stone-Hoyos-Varghese teaches performing location authentication based on the captured physical location information. Furthermore, Varghese’s location authentication describes determining a physical location of the user based at least in part on the captured physical location information, e.g., by using “geolocation by IP address for determining the geographic latitude and longitude corresponding to a user by comparing the user’s IP address with known locations of other nearby servers and routers.” APPL-1010, [0140], [0012] (“certain geographic locations are known to contain an inordinate number of identity thieves. It is therefore advantageous to know where an attempt to access a server originates from.”). Stone itself describes detection of the location of the user “may be determined through GPS or any other location-determining method”). APPL-1008, [0026]. Further, it was well-known to perform location

authentication based on physical location data, e.g., geo-location using IP address and network information, GPS location, etc. APPL-1003, ¶194 (APPL-1016, [0036]);

Accordingly, Stone-Hoyos-Varghese renders obvious this claim.

D. Ground 3: Claims 1-2, 4-7, 9-10, 12-15, 17, 20-23 are Rendered Obvious under §103(a) over Stone in view of FFIEC Guidance.

Ground 3 relies on the same analysis and evidence as provided above in Ground 1 regarding Stone’s disclosure. The analysis of Stone as applied in Ground 3 is substantially similar to the analysis of Stone as applied in Ground 1. APPL-1003, ¶196.

1. Combination of Stone and FFIEC Guidance (“Stone-Guidance”)

A POSITA would have been motivated to apply Guidance’s teaching of multifactor real-time contextual-based and risk-based authentication in Stone for the benefits of improved security and boosted customer confidence for service providers even not subject to FFIEC supervision, and the additional benefits of FFIEC compliance for federal supervised financial institutions. APPL-1003, ¶¶197-200.

First, as discussed at IX.A.5, Guidance is analogous art to the ’010 patent. APPL-1003, ¶198.

Second, Guidance “addresses why financial institutions regulated by the

agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services.” APPL-1037, 1. A POSITA would have understood that the multifactor, real-time, risk-based authentication taught by Guidance provides “improved authentication technologies” for reducing fraud and identity theft and improving customer protection, for service providers of financial transactions even not regulated by FFIEC. APPL-1022, 1. As such, a POSITA would have been motivated to apply the multifactor, real-time, risk-based authentication taught by Guidance in Stone, because Stone had a need for authentication for fraud detection (e.g., with higher levels of security for higher-risk financial transactions). APPL-1003, ¶199 (citing APPL-1013, [0009], [0011]; APPL-1010, [0148]; APPL-1016, FIG. 3, [0073]).

A POSITA would have reasonably expected to succeed in configuring Stone to implement the multifactor, real-time, risk-based authentication functionality taught by Guidance, since its implementation would have required only routine knowledge well within the skill of a POSITA prior to the earliest effective filing date. APPL-1003, ¶200 (citing APPL-1039, 1; APPL-1008, [0041]-[0042] (describing user devices implemented with any appropriate computing devices (e.g., personal computer, wireless telephone, etc.) with wired and/or wireless communication over network)). For example, a POSITA would have understood to

implement the enrollment phase of authentication during user registration in Stone to capture high-confidence enrollment data, and implement the authentication phase of authentication (e.g., capturing biometric data and location and performing fraud analysis thereupon) after user initiates and confirms a transaction request, for providing risk-based authentication adaptive to the risk of the transaction. APPL-1003, ¶200.

2. Claim 1

[1.0] A system, comprising:

Stone discloses or renders obvious the preamble to the extent that it is limiting for the reasons discussed at Ground 1:[1.0]. APPL-1003, ¶201.

[1.1] one or more processors configured to:

Stone alone or Stone-Guidance renders obvious this element. APPL-1003, ¶¶202-205.

First, Stone renders obvious this element for the reasons discussed at Ground 1:[1.1]. APPL-1003, ¶203.

Second, as discussed below at Ground 3:[1.2]-[1.9], Stone alone or in combination with Guidance teaches [1.2]-[1.9], and a POSTA would have understood to modify Stone such that the one or more processors are configured to perform the processes including [1.2]-[1.9] for initiating, authenticating, and completing the electronic transaction. APPL-1003, ¶204.

Accordingly, Stone alone or Stone-Guidance renders obvious this element.

[1.2]-[1.5]

Stone discloses or renders obvious this element for the reasons discussed at Ground 1:[1.2]-[1.5]. APPL-1003, ¶¶206-209.

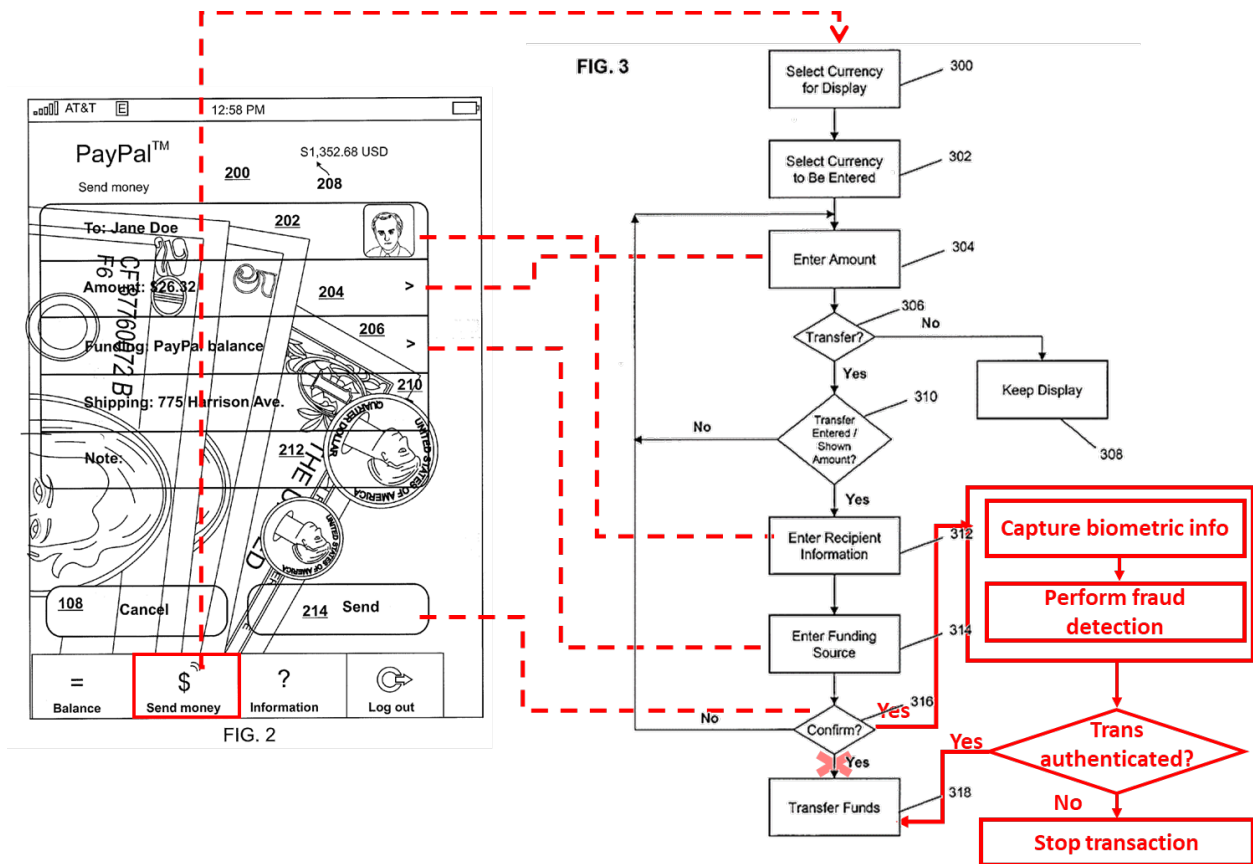
[1.6] capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information associated with a user;

Stone-Guidance renders this element obvious. APPL-1003, ¶¶210-215.

First, Guidance describes multifactor, real-time, risk-based contextual authentication for electronic transactions, including biometric authentication (including capturing biometric information including “facial scans” using “live scan” of the user for face recognition). APPL-1037, 9-11 (describing face recognition); APPL-1003, ¶211. Guidance describes “face recognition” is one of the biometric techniques with “increasingly gaining acceptance.” APPL-1037, 10-11. Guidance describes that during real-time transaction authentication, the results of live scan, e.g., facial scans captured using cameras, “are compared with the registered templates stored in the system,” and the transaction is authorized if there is a match. APPL-1037, 10-11; APPL-1003, ¶211.

Second, as shown in example Stone-Guidance below, a POSITA would have been motivated to implement (in Stone) the multifactor real-time authentication (including capturing the live data and performing the fraud detection analysis) as taught by Guidance to provide improved security for electronic transactions. APPL-1003, APPL-1003, ¶212. Specifically, a POSITA would have

been motivated to implement the capturing after a user confirms the parameters of a transaction request, (e.g., after a user confirms a transaction request at block 316 Stone, thereby subsequent to user interaction with any of the transaction icons associated with “\$Send money,” 202, 206, 214, personalized currency, blocks 300, 302, 306, 312, 314, and 316) as claimed, for the benefit of providing real-time risk-based authentication for fraud analysis. APPL-1003, ¶212; APPL-1037, 1-2 (requiring multifactor authentication for “high-risk transactions,” and authentication methods should depend upon risk assessment), 10 (using “live-scan process” for biometrics), 12 (performing location authentication “in a real-time environment).



Example of Stone-Guidance (annotated based on APPL-1008, FIGS. 2 and 3)

As such, in Stone-Guidance, capturing the contextual data including biometric data (and other contextual data for other factor(s) in the multifactor authentication, e.g., and location data) and fraud analysis thereafter as taught by Guidance is performed after user transaction request confirmation, 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 interactions with icons to continue (e.g., blocks 300-314) and confirm (e.g., block 316) the transaction request. APPL-1003, ¶213. This has various benefits over the alternative design

choice of using a previously captured and stored data (e.g., for liveness analysis or for comparison with the enrollment data), including enabling contextual authentication adaptive for the specific transaction based on transaction information (e.g., type, amount) for improved fraud detection (APPL-1010, FIG. 14, [0091], TABLE 10, APPL-1016 [0043]), providing more accurate and updated real-time information for real-time authentication (APPL-1010, [0148]; APPL-1015, FIG. 4). APPL-1003, ¶213 (it was well-known to provide higher level authentication for higher risk transactions (e.g., a \$10,000 transfer request with a higher risk than a \$10 transfer request), citing APPL-1037, 3-4 (describing risk-based authentication including evaluating risks in light of customer transaction capabilities, transaction types (e.g., bill payment, wire transfer, loan origination)).

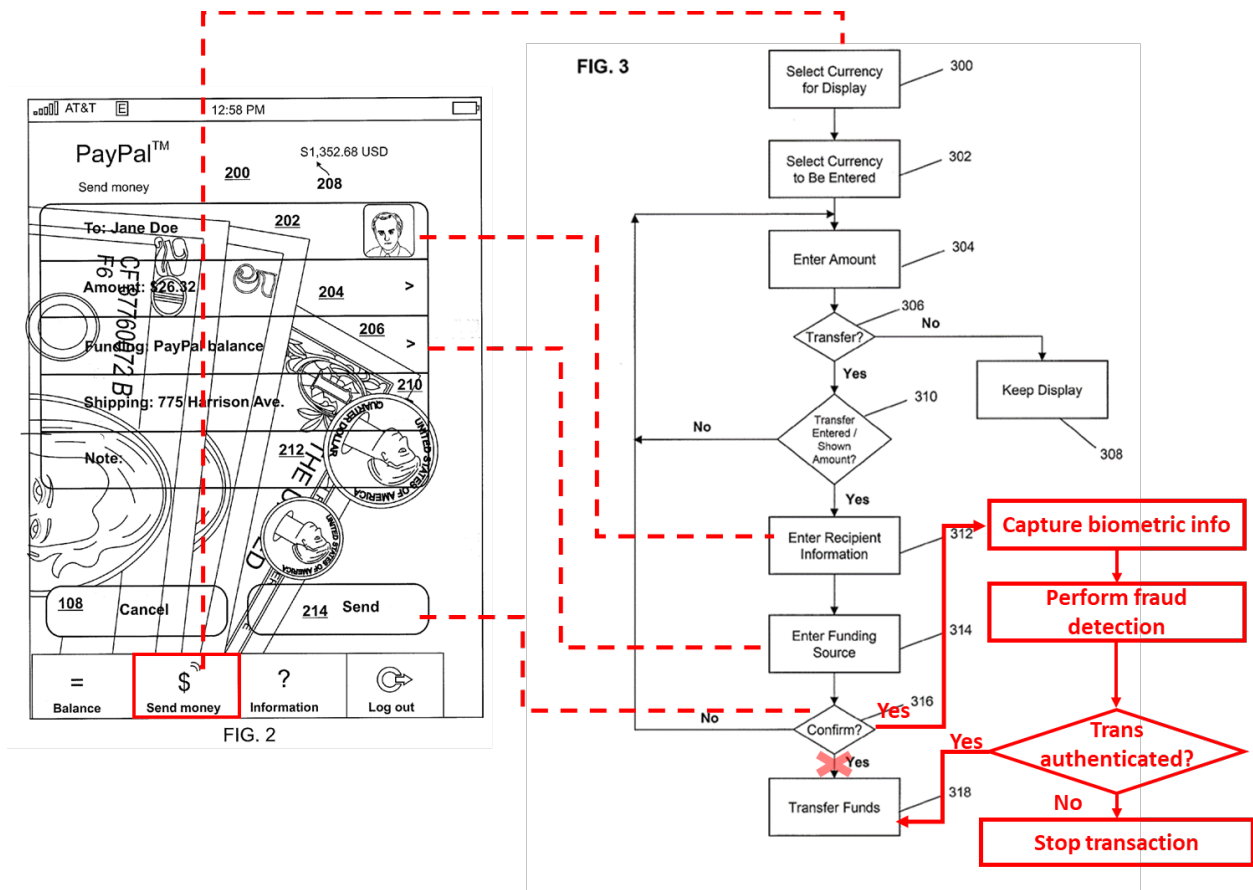
Accordingly, in Stone-Guidance, subsequent to an indication of a user action with a transaction icon (e.g., any of the transaction icons associated with “\$Send money,” 202, 206, 214, personalized currency, blocks 300, 302, 306, 312, 314, and 316), contextual information comprising biometric information (e.g., facial images by video cameras for liveness detection) associated with the user is captured as taught in Guidance, which renders obvious this element.

Therefore, Stone-Guidance renders obvious this element.

[1.7] perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises determining, based at least in part on the captured biometric information, that the user is alive; and

Stone-Guidance renders this element obvious. APPL-1003, ¶¶216-219.

First, as discussed at Ground 3:[1.7], in Stone-Guidance, the multifactor real-time authentication as taught by Guidance as applied in Stone includes face recognition, which performs a fraud detection analysis (e.g., face recognition analysis to detect fraud) of the captured biometric information (e.g., facial scans captured by cameras including video cameras). APPL-1037, 2 (“An effective authentication system is necessary for compliance with requirements to...**reduce fraud**”), 7, 9-10 (describing biometric technologies with fraud detection analysis of the captured biometric data, where “results of a live scan” are “compared with the registered templates stored in the system” to “identify and authenticate the customer” if there is a match). A POSITA would have understood that by that biometric authentication teaches a fraud detection analysis by detecting fraud based on whether there is a match. APPL-1003, ¶217.



Example of Stone-Guidance (annotated based on APPL-1008, FIGS. 2 and 3)

Second, the fraud detection analysis (e.g., face recognition analysis to detect fraud) of Guidance as applied in Stone-Guidance teaches determining, based at least in part on the captured biometric information (e.g., facial scans captured by cameras including video cameras), that the user is alive, because Guidance teaches facial scan applications use “tests for **liveness**, such as blinking eyes,” and “[t]esting for liveness reduces the chance that the person requesting access is using a photograph of an authorized individual.” APPL-1037, 11. Indeed, techniques for liveness tests based on facial images from cameras were wellknown. APPL-1003,

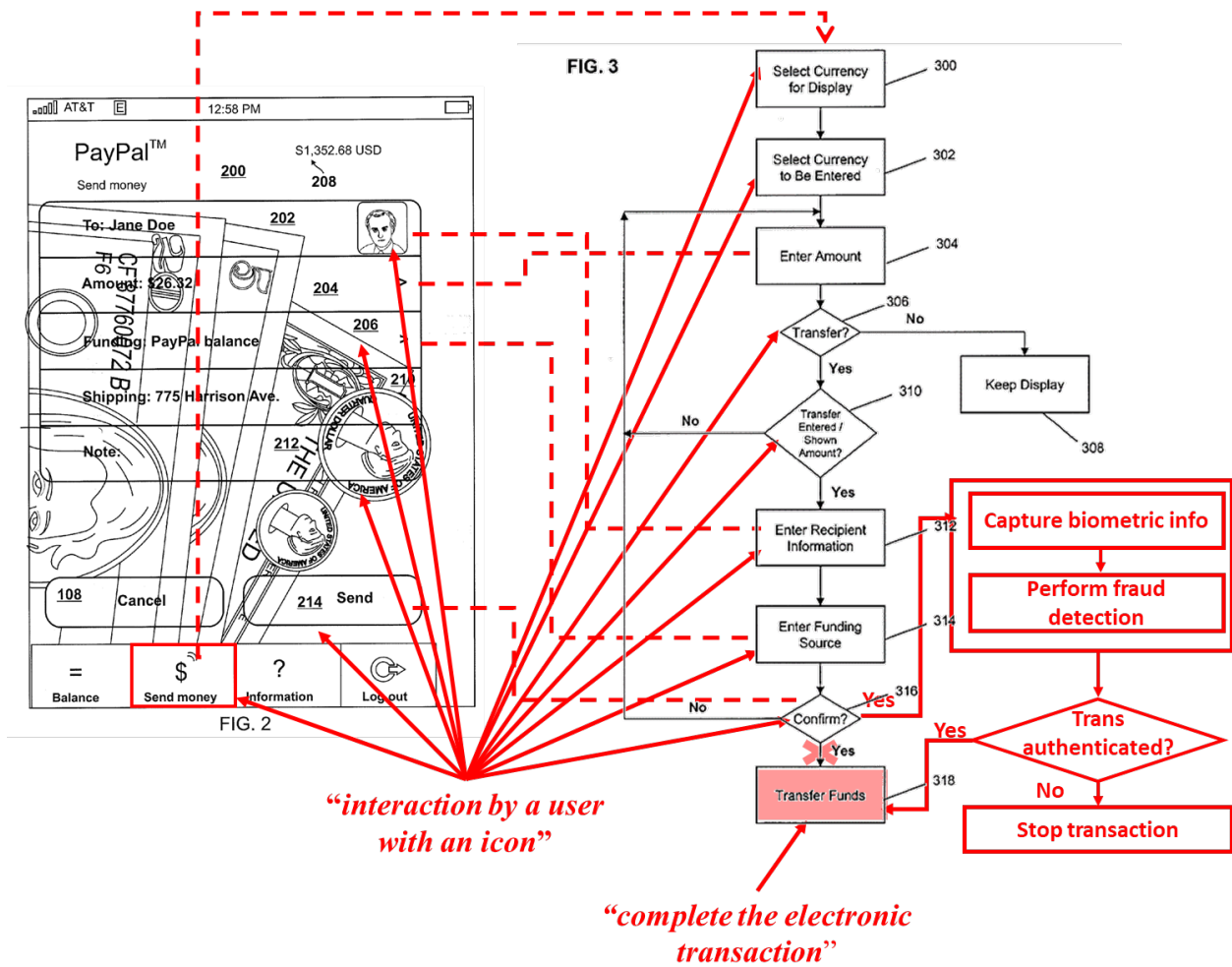
¶218 (citing APPL-1044, 2; APPL-1013, FIGS. 2-4, claims 5-6; APPL-1011, Abstract; APPL-1012, Abstract).

Therefore, Stone-Guidance renders obvious this element.

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

Stone-Guidance renders this element obvious. APPL-1003, ¶¶220-224.

Specifically, Stone as applied in Stone-Guidance teaches completing the electronic transaction (e.g., performing transferring funds at block 318 of FIG. 3 of Stone) based on **both** (1) the user interaction indicating that the user's indication of initiating, continuing/confirming the transaction request (see [1.5]), and (2) authorization of the transaction request based on the fraud detection analysis (see [1.7]). APPL-1003, ¶221 (citing APPL-1008, [0035] ("the shown funds are transferred to the desired recipient in step 318")); APPL-1013, FIG. 1, block 17 ("Transaction Authorized" after fraud detection analysis); parent patent 9,972,010, claim 23 ("completing the electronic transaction...comprises transferring funds")).



Example of Stone-Guidance (annotated based on APPL-1008, FIGS. 2 and 3)

Therefore, Stone-Guidance renders this element obvious.

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

Stone discloses or renders obvious this element for reasons discussed at Ground 1:[1.9]. APPL-1003, ¶¶225. Accordingly, claim 1 is obvious over Stone and Guidance.

3. Claims 2, 4, 5, 6

Stone discloses or renders obvious these elements for the reasons discussed

at Ground 1: Claims 2, 4, 5, and 6. APPL-1003, ¶¶226-229. Accordingly, these claims are also obvious over Stone and Guidance.

4. Claim 7

[7.0] The system of claim 1 wherein the captured contextual information further comprises at least one of physical location information and information spoken by the user.

Stone-Guidance renders obvious this element. APPL-1003, ¶¶230-235.

First, Guidance describes multifactor real-time authentication using a combination of authentication techniques, including physical location authentication and biometrics authentication including voice authentication.

For location authentication, Guidance describes authentication based on “geo-location technology” to “limit Internet users by determining where they are.” APPL-1037, 12. It was well-known that geo-location technology captures physical location information (e.g., user IP address and other associated network information) for determining the physical address of the user. APPL-1003, ¶232 (citing APPL-1010, [0140] (“Geolocation by IP address is a technique of determining the geographic latitude and longitude corresponding to a user by comparing the user’s IP address with known locations of other nearby servers and routers.”). Furthermore, Stone already describes detection of the location of the user “may be determined through GPS or any other location-determining method”). APPL-1008, [0026]. Additionally, various technologies for capturing physical location information were well-known, including e.g., geo-location using

IP address and network information, GPS location information, etc. APPL-1003, ¶232 (citing APPL-1016, [0036]).

For voice authentication, Guidance describes biometrics authentication including “voice recognition” based on “voice pattern” of a user. APPL-1037, 7, 10. Additionally, Guidance describes that the “multifactor authentication methodology may also include ‘out-of-band’ controls for risk mitigation,” where “[t]he telephoned party [e.g., originating individual] is asked for a predetermined word, phrase, or number that verifies that the transaction was legitimate and confirms the dollar amount.” APPL-1037, 3, 12. The “voice recognition,” alone or with “out-of-band” call verification of Guidance teaches capturing contextual information spoken by the user, e.g., for comparison with the registered templates stored in the system. APPL-1037, 9-10; APPL-1003, ¶233 (citing APPL-1033, FIG. 3, 1438).

In Stone-Guidance, a POSITA would have been motivated to implement a multifactor real-time authentication implementing one or all of location authentication and voice authentication based on risk assessment (e.g., different risks for transaction of different types and amounts) as taught by Guidance for improved fraud detection analysis more secure financial transactions. APPL-1003, ¶234 (citing APPL-1016 [0036] (describing multifactor authentications including

fingerprint validation, PIN validation, voice biometric validation, facial recognition validation, or GPS location validation); APPL-1037, 7). *See also* IX.D.1.

Accordingly, Stone-Guidance renders obvious this claim.

5. Claim 9

[9.0]-[9.4]

Stone discloses or renders obvious these elements for reasons discussed at Ground 1:[9.0], [1.2], [1.3], [1.4], and [1.5]. APPL-1003, ¶¶236-240.

[9.5]-[9.7]

Stone-Guidance renders obvious these elements for reasons discussed at Ground 3:[1.6], [1.7], and [1.8]. APPL-1003, ¶¶241-243. Accordingly, claim 9 is obvious over Stone and Guidance.

6. Claims 10, 12, 13, 14

Stone discloses or renders obvious these element for reasons discussed at Ground 3:[2.0], [4.0], [5.0], and [6.0]. APPL-1003, ¶¶244-247. Accordingly, these claims are also obvious over Stone and Guidance.

7. Claim 15

Stone-Guidance renders obvious this claim for reasons discussed at Ground 3:[7.0]. APPL-1003, ¶248.

8. Claim 17

[17.0]-[17.4]

Stone discloses or renders obvious these elements for reasons discussed at

Ground 3:[1.0], [1.2], [1.3], [1.4], and [1.5]. APPL-1003, ¶¶249-253.

[17.5]-[17.7]

Stone-Guidance renders obvious these elements for reasons discussed at Ground 3:[1.6], [1.7], and [1.8]. APPL-1003, ¶¶254-256. Accordingly, claim 17 is obvious over Stone and Guidance.

9. Claim 20

[20.0] The system of claim 1 wherein the captured biometric information associated with the user includes a fingerprint.

Stone-Guidance renders obvious this element. APPL-1003, ¶¶257-261.

First, as discussed at [1.6]-[1.7], Guidance as applied in Stone-Guidance teaches multifactor real-time authentication including biometrics authentication, e.g., face recognition.

Second, Guidance teaches that fingerprint recognition is one of the biometric techniques for use in its multifactor real-time authentication. APPL-1037, 10-11. In Stone-Guidance, a POSITA would have been motivated to include fingerprint recognition in the multifactor real-time authentication, because fingerprint recognition is “increasing gaining acceptance,” and “among the most mature and accurate of the various biometric method of identification.” APPL-1037, 10-11.

Such use of fingerprint is also consistent with Stone’s disclosure of “biometric id,” which is well-known to include fingerprint identification

information for fingerprint recognition. APPL-1003, ¶260; APPL-1008, [0045], APPL-1010, [0079].

As such, it would have been obvious for a POSITA to implement fingerprint authentication, including capturing fingerprint, for fraud detection in Stone-Guidance for improved security.

Therefore, Stone-Guidance renders obvious this claim.

10. Claim 21

[21.0] The system of claim 1 wherein the captured biometric information comprises a plurality of photographs, and wherein the fraud detection analysis comprises an analysis of the plurality of photographs to determine that the user is alive.

Stone-Guidance renders obvious this element. APPL-1003, ¶¶262-264.

Specifically, Guidance teaches performing an analysis of the plurality of photographs to determine that the user is alive, because Guidance describes face recognition that uses facial scans captured by “video cameras” (where frames of the captured video are a plurality of photographs) and/or “several cameras collecting image data from different angles,” and the facial scans are analyzed for “tests for liveness, such as blinking eyes.” APPL-1037, 11. Indeed, techniques for liveness tests using a plurality of photographs (e.g., based on blinking eyes or other liveness tests) were well-known. APPL-1003, ¶263 (citing APPL-1044, 2; APPL-1013, FIGS. 2-4, claims 5-6).

Therefore, Stone-Guidance renders obvious this claim.

11. Claim 22

[22.0]

Stone-Guidance renders obvious this element for reasons discussed at Ground 3:[7.0]. APPL-1003, ¶265.

As discussed at Ground 3:[7.0] above, the captured physical location information associated with the user is contextual information, because it is associated with where the user originates the transaction request, and the location authentication includes performing the fraud detection analysis by determining a physical location of the user based on the captured physical location information. APPL-1037, 12 (performing fraud analysis to “limit Internet users by determining where they are or, conversely, where they are not.”). Therefore, Stone-Guidance renders obvious this claim.

12. Claim 23

[23.0]-[23.2]

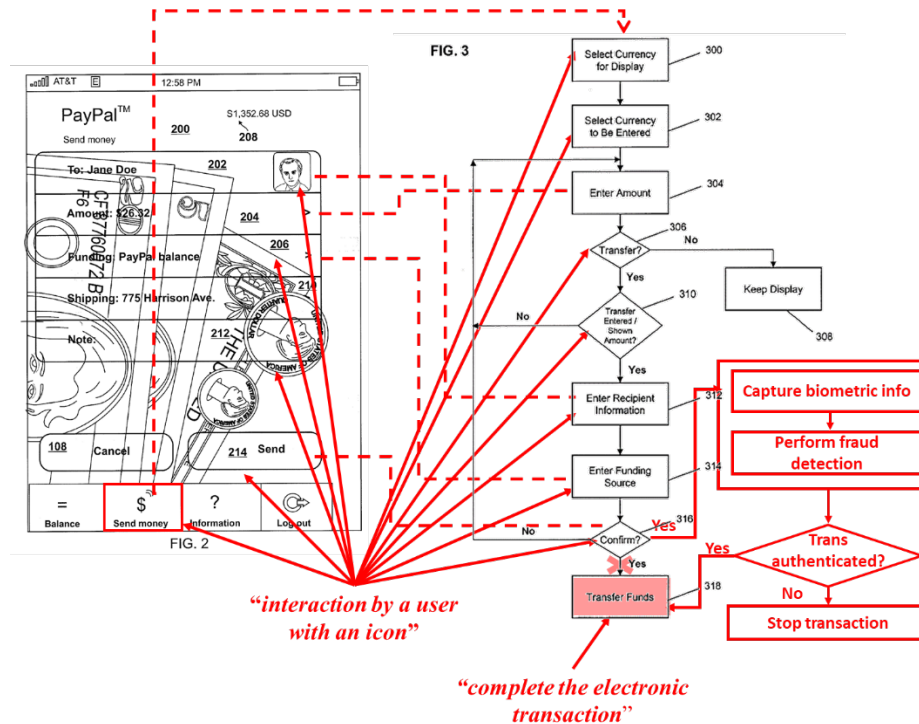
Stone discloses or renders obvious the element for reasons discussed at Ground 1: [23.0]-[23.2]. APPL-1003, ¶¶266-268.

[23.3] *wherein completing the electronic transaction...comprises transferring funds between the first account...and the second account....*

Stone-Guidance renders obvious this element. APPL-1003, ¶¶269-274.

As discussed at Ground 3:[1.8], Stone-Guidance renders obvious “*completing the electronic transaction*” as claimed, where Stone discloses that completing the electronic transaction includes transferring funds between the first

account and the second account. APPL-1008, [0035]. As shown in the example of Stone-Guidance below, after passing the fraud detection based on liveness analysis, funds are transferred at block 318 (completing the electronic transaction).



Example of Stone-Guidance (annotated based on APPL-1008, FIGS. 2 and 3)

Accordingly, Stone-Guidance renders obvious this claim.

X. DISCRETIONARY DENIAL IS NOT WARRANTED

Petitioner respectfully submits that the Board should not exercise its discretion under 35 U.S.C. §§314(a) or 325(d) to deny this Petition.

The Board should not exercise its discretion under 35 U.S.C. §§314(a) or 325(d) to deny this Petition.

A. The *Fintiv*⁴ factors favor institution.

Denial would be improper based on factors in *Apple v. Fintiv*, IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020) (precedential). Patent Owner asserted the '010 patent against Apple in WDTX-1-23-cv-00324 (“the Parallel District Court Proceeding”). *See supra* Section II.B.

First, this Petition presents compelling evidence of unpatentability of the Challenged Claims. *See* Section IX. Therefore, the Board should not deny institution based on parallel litigation. APPL-1025, 2, 4-5, 9 (Director Memo).

Second, the *Fintiv* factors weigh in favor of institution.

- Factor 1 is neutral. Apple has not yet requested a stay pending resolution of this IPR.
- Factors 2 and 5 favor institution. Although the current scheduling order projects a trial date of December 4, 2024 (APPL-1028, 4), median time-to-trial statistics for WDTX indicate 25.8 months (mid-June 2025, based on March 24, 2023 complaint). *See* APPL-1025, 8-9

⁴ Apart from Apple’s showing that *Fintiv* favors institution, the *Fintiv* framework should not be followed because it is legally invalid. The framework (1) exceeds the Director’s authority, (2) is arbitrary and capricious, and (3) was adopted without notice-and-comment rulemaking.

(median time-to-trial, generally); APPL-1027, 37 (WDTX statistics).

Indeed, earlier that week, the presiding district court judge has a trial set for December 2, 2024 and December 3, 2024 making it even more likely that the projected December 4 trial date will move. Here, final written decision is due July 2025. Per the Director's Memo, PTAB will weigh factor 2 against exercise of discretion "if the median time-to-trial is around the same time or after the projected statutory deadline for the PTAB's final written decision." APPL-1027, 9. Inefficiency concerns are minimal.

- Factors 3 and 4 favor institution: The Parallel District Court Proceeding is in its early stages. Preliminary contentions have been served, a Markman hearing was held December 12, 2023, and fact discovery just opened. At the hearing, the Court indicated that it was adopting preliminary constructions applying plain and ordinary meaning and denied Apple's motion for transfer to NDCA, though no written order has issued. APPL-1026, 1-2. This Petition is not duplicative because it challenges claims 2, 4, 7, 12, 15, 20, 23, which are not asserted in the Parallel District Court Proceeding. *See* APPL-1029, 2. Moreover, Apple stipulates that, if the Board institutes trial, it will not pursue the same grounds raised in this Petition in the Parallel

District Court Litigation. *See Sand Revolution II, LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020). The stipulation reduces any overlap and mitigates concerns of duplicative efforts or potentially conflicting decisions.

- Factor 6 favors institution in view of compelling evidence of unpatentability of the Challenged Claims.

In short, Fintiv factors are either neutral or weigh in favor of institution.

B. *Advanced Bionics* Test Favors Institution.

In determining whether to institute an IPR, the Board may consider whether “the same or substantially the same prior art or arguments previously were presented to the Office.” §325(d); *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 at 7 (PTAB Feb. 13, 2020).

Regarding the first prong of *Advanced Bionics*, none of the applied references was presented to the Office. The Examiner did not consider Stone, Hoyos, Varghese, or Guidance during the prosecution. Moreover, they are non-cumulative, because they teach the Examiner amendment including “Examiner Amendment including *“performing the fraud detection analysis comprises determining, based at least in part on the captured biometric information, that the*

user is alive” that resulted in allowance claimed features including those provided by the reasons for allowance of the ’010 patent. *See* APPL-1002, 441-442.

XI. CONCLUSION

Petitioner has established a reasonable likelihood that Challenged Claims of the ’010 patent are unpatentable, and requests institution of *inter partes* review.

Respectfully submitted,

Dated: January 30, 2024

/David W. O'Brien/
David W. O'Brien
Lead Counsel for Petitioner
Registration No. 40,107

XII. CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24, the undersigned attorney for Petitioner declares that the argument section of this Petition (Sections I, III–XI) has 13,519 (less than 14,000) words, according to the word count tool in Microsoft Word™.

/David W. O'Brien/
David W. O'Brien
Lead Counsel for Petitioner
Registration No. 40,107

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. § 42.6(e) and 37 C.F.R. § 42.105, service was made on Patent Owner as detailed below.

Date of service January 30, 2024

Manner of service FEDERAL EXPRESS

Documents served Petition for *Inter Partes* Review, including Exhibit List; Exhibits APPL-1001–APPL-1006, APPL-1008–APPL-1029, and APPL-1033–APPL-1047

Persons served VAN PELT, YI & JAMES LLP
1 1st ST, STE 12
LOS ALTOS, CA 94022
UNITED STATES

/David W. O'Brien/
David W. O'Brien
Lead Counsel for Petitioner
Registration No. 40,107