

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

CARBYNE BIOMETRICS, LLC,

Patent Owner

IPR2024-00330

U.S. Patent No. 10,713,656

**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 '656 PATENT.....	2
A.	Summary of the '656 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	11
5.	Analogous Art.....	12
B.	Ground 1: Claims 1, 4-10, and 13-19 are Rendered Obvious under §103(a) over Stone in view of Hoyos and Varghese.	13
1.	Combination of Disclosures/Embodiments of Stone.....	13
2.	Combination of Stone and Hoyos (“Stone-Hoyos”).....	15

3.	Combination of Stone, Hoyos, and Varghese (“Stone-Hoyos-Varghese”).....	21
4.	Claim 1	26
5.	Claim 4.....	52
6.	Claim 5	53
7.	Claim 6.....	54
8.	Claim 7.....	56
9.	Claim 8.....	56
10.	Claim 9.....	57
11.	Claim 10.....	58
12.	Claims 13, 14, 15, 16, and 17	60
13.	Claim 18.....	60
14.	Claim 19.....	60
C.	Ground 2: Claims 1, 4-10, and 13-19 are Rendered Obvious under §103(a) over Stone in view of FFIEC Guidance.....	62
1.	Combination of Stone and FFIEC Guidance (“Stone-Guidance”)	62
2.	Claim 1	63
3.	Claims 4, 5, 6, 7, 8	73
4.	Claim 9.....	73
5.	Claim 10.....	74
6.	Claims 13, 14, 15, 16, and 17	74
7.	Claim 18.....	75
8.	Claim 19.....	75
D.	Grounds 3 and 4: Combination of Stone, Hoyos, Varghese, and Borovsky (Ground 3, “Stone-Hoyos-Varghese-Borovsky”) and Combination of Stone, Guidance, and Borovsky (Ground 4, “Stone-Guidance-Borovsky”) render obvious Claims 2-3 and 11-12.....	76
1.	Borovsky	76

2.	Reasons to Combine Stone and Borovsky	77
3.	Claims 2 and 11	79
4.	Claims 3 and 12	81
X.	DISCRETIONARY DENIAL IS NOT WARRANTED	81
A.	The <i>Fintiv</i> factors favor institution.	82
B.	<i>Advanced Bionics</i> Test Favors Institution	84
XI.	CONCLUSION	85
XII.	CERTIFICATE OF WORD COUNT	86
	CERTIFICATE OF SERVICE	87

PETITIONER'S EXHIBIT LIST

January 30, 2023

APPL-1001	U.S. Patent No. 10,713,656 to Jakobsson (“’656 patent”)
APPL-1002	Prosecution File History of U.S. App. No. 15/948744 (issued as ’656 patent) (“’744 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 (issued as U.S. Patent No. 8,458,041) (“’981 App”)
APPL-1007	Prosecution File History of U.S. App. No. 13/875,245 (issued as U.S. Patent No. 9,972,010) (“’245 App”)
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]	a processor configured to:
[1.2]	receive biometric information associated with an account holder; store, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder;
[1.3]	render, in one or more interfaces, a virtual likeness of a face of a recipient of an electronic transaction;
[1.4]	render, in the one or more interfaces, a transaction icon associated with the electronic transaction;
[1.5]	receive an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the one or more interfaces;
[1.6]	subsequent to receiving the indication of the action taken by the user, capture contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information and location data associated with the user;
[1.7.1]	perform a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises:
[1.7.2]	performing a comparison based at least in part on the stored biometric information and the captured biometric information; and
[1.7.3]	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 and performing the fraud detection analysis, complete the electronic transaction; and
[1.9]	a memory coupled to the processor and configured to provide the processor with instructions.
Claim 2	
[2.0]	The system of claim 1 wherein the processor is further configured to obtain the virtual likeness of the face of the recipient from a social networking site.
Claim 3	
[3.0]	The system of claim 2 wherein obtaining the virtual likeness of the face of the recipient from the social networking site comprises scraping the social networking site for the virtual likeness of the face of the recipient.
Claim 4	
[4.0]	The system of claim 1 wherein the virtual likeness of the face of the recipient was provided by the recipient.
Claim 5	
[5.0]	The system of claim 1 wherein the transaction icon comprises a graphical representation of a payment form.
Claim 6	
[6.0]	The system of claim 5 wherein the transaction icon comprises a graphical representation of money.
Claim 7	
[7.0]	The system of claim 1 wherein the virtual likeness of the face of the recipient comprises a photograph of the recipient.

Claim 8	
[8.0]	The system of claim 1 wherein the virtual likeness of the face of the recipient comprises an avatar of the recipient.
Claim 9	
[9.0]	The system of claim 1 wherein a password is not required to initiate the electronic transaction.
Claim 10	
[10.0]	A method, comprising:
[10.1]	receiving biometric information associated with an account holder; storing, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder;
[10.2]	rendering, in one or more interfaces, a virtual likeness of a face of a recipient of an electronic transaction
[10.3]	rendering, in the one or more interfaces, a transaction icon associated with the electronic transaction;
[10.4]	receiving an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the one or more interfaces;
[10.5]	subsequent to receiving the indication of the action taken by the user, capturing contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information and location data associated with the user;
[10.6.1]	performing, using a processor, a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises:

[10.6.2]	performing a comparison based at least in part on the stored biometric information and the captured biometric information; and
[10.6.3]	determining, based at least in part on the captured biometric information, that the user is alive; and
[10.7]	based at least in part on both the user interaction with the transaction icon rendered in the interface and performing the fraud detection analysis, complete the electronic transaction.
Claim 11	
[11.0]	The method of claim 10 wherein the processor is further configured to obtain the virtual likeness of the face of the recipient from a social networking site.
Claim 12	
[12.0]	The method of claim 11 wherein obtaining the virtual likeness of the face of the recipient from the social networking site comprises scraping the social networking site for the virtual likeness of the face of the recipient.
Claim 13	
[13.0]	The method of claim 10 wherein the virtual likeness of the face of the recipient was provided by the recipient.
Claim 14	
[14.0]	The method of claim 10 wherein the transaction icon comprises a graphical representation of a payment form.
Claim 15	
[15.0]	The method of claim 14 wherein the transaction icon comprises a graphical representation of money.
Claim 16	

[16.0]	The method of claim 10 wherein the virtual likeness of the face of the recipient comprises a photograph of the recipient.
Claim 17	
[17.0]	The method of claim 10 wherein the virtual likeness of the face of the recipient comprises an avatar of the recipient.
Claim 18	
[18.0]	The method of claim 10 wherein a password is not required to initiate the electronic transaction.
Claim 19	
[19.0]	A computer program product embodied in a non-transitory computer readable storage medium and comprising computer instructions for:
[19.1]	receiving biometric information associated with an account holder; storing, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder;
[19.2]	rendering, in one or more interfaces, a virtual likeness of a face of a recipient of an electronic transaction;
[19.3]	rendering, in the one or more interfaces, a transaction icon associated with the electronic transaction;
[19.4]	receiving an indication of an action taken by a user, the action comprising a user interaction with the transaction icon rendered in the one or more interfaces;
[19.5]	subsequent to receiving the indication of the action taken by the user, capturing contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information and location data associated with the user;

[19.6.1]	performing, using a processor, a fraud detection analysis of the captured contextual information associated with the electronic transaction, wherein performing the fraud detection analysis comprises:
[19.6.2]	performing a comparison based at least in part on the stored biometric information and the captured biometric information; and
[19.6.3]	determining, based at least in part on the captured biometric information, that the user is alive; and
[19.7]	based at least in part on both the user interaction with the transaction icon rendered in the interface and performing the fraud detection analysis, complete the electronic transaction.

I. INTRODUCTION

U.S. Patent No. 10,713,656 (the “’656 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 1-19 (“Challenged Claims”) of the ’656 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), to the best knowledge of the Petitioner, the ’656 patent is or was involved in the following cases:

- *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 other disclaimers, reexamination certificates, or IPR petitions addressing the ’656 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 '656 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 '656 PATENT

A. Summary of the '656 patent

The '656 patent is directed at electronic transactions, and specifically financial transaction systems. APPL-1001, Abstract. As shown in FIG. 7 below, the '656 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.

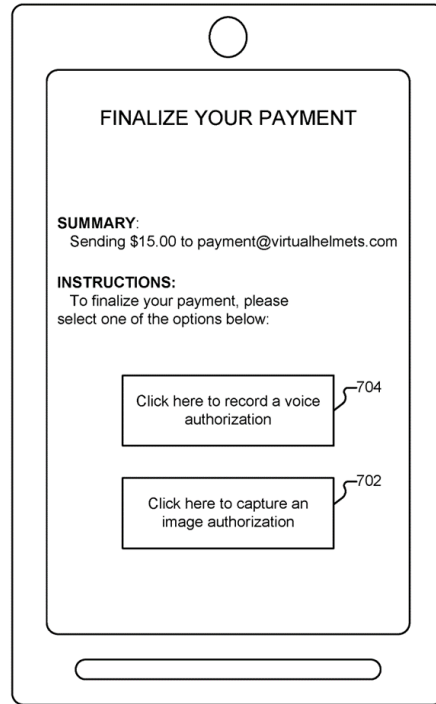


FIG. 7

APPL-1001, FIG. 7

Specifically, the '656 patent describes techniques “for confirming that the object being photographed is alive (e.g., by taking multiple photographs in rapid succession),” which make sure that the fraudster isn’t using “a printed picture of the legitimate user.” APPL-1001, 8:60-66.

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

After Patent Owner filed terminal disclaimer over patents 9,972,010 and 8,458,041, Notice of Allowance issued with Examiner Amendment including

“subsequent to receiving the indication of the action taken by the user, capture contextual information associated with the electronic transaction,” the Examiner Amendment agreed by Patent Owner at an interview to overcome Hertel (US 2009/0288012, APPL-1034), where Hertel describes capturing contextual information for login authentication. APPL-1002, 99.

As shown in IX.B and C below, Grounds in this Petition teach all features of the allowed claims, including the amended features resulting in the notice of allowance.

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, ¶21. 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, ¶¶35-36.

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 1-19 (“Challenged Claims”) of the ’656 patent are challenged.

B. Statutory Grounds for Challenges

Ground	Claims	Basis
#1	1, 4-10, and 13-19	§103(a) over Stone in view of Hoyos and Varghese
#2	1, 4-10, and 13-19	§103(a) over Stone in view of FFIEC Guidance
#3	2-3 and 11-12	§103(a) over Stone in view of Hoyos, Varghese, and Borovsky
#4	2-3 and 11-12	§103(a) over Stone in view of FFIEC Guidance and Borovsky

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, and is prior art under §102(b).

Borovsky was filed June 11, 2009 and published Dec. 16, 2010. Chatterjee was filed Dec. 2009 and issued Feb. 26, 2013. Borovsky and Chatterjee each are prior art under at least §102(e).

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 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 ’656 patent, because it is directed to financial transaction applications. APPL-1008, [0001]-[0005]; APPL-1003, ¶¶37-38.

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.

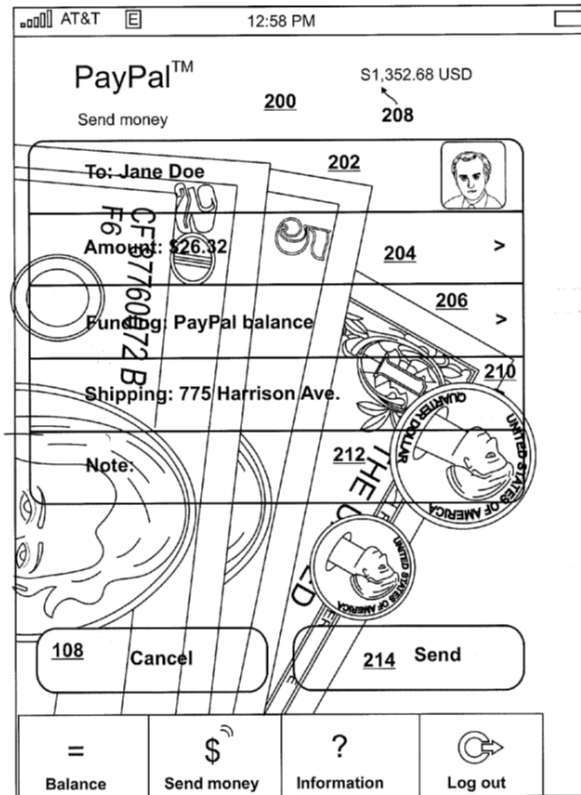


FIG. 2

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, ¶¶39-43.

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.).

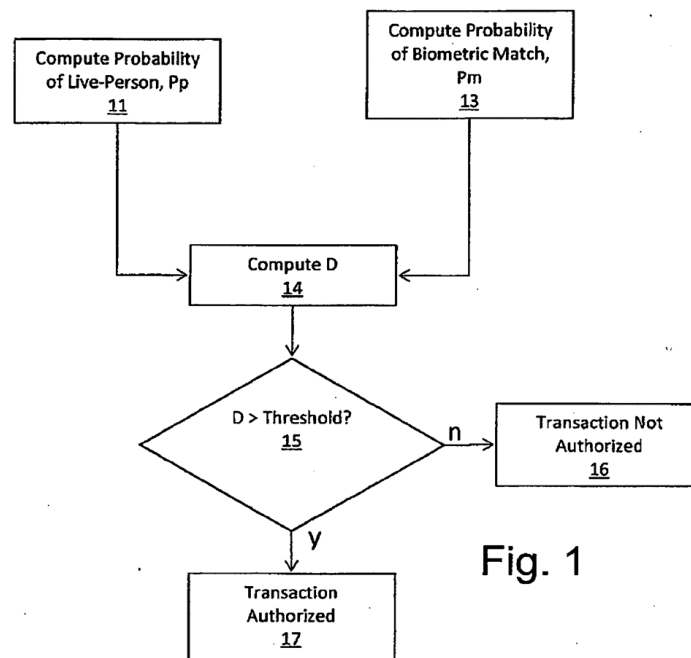


Fig. 1

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].

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, ¶¶44-46.

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.

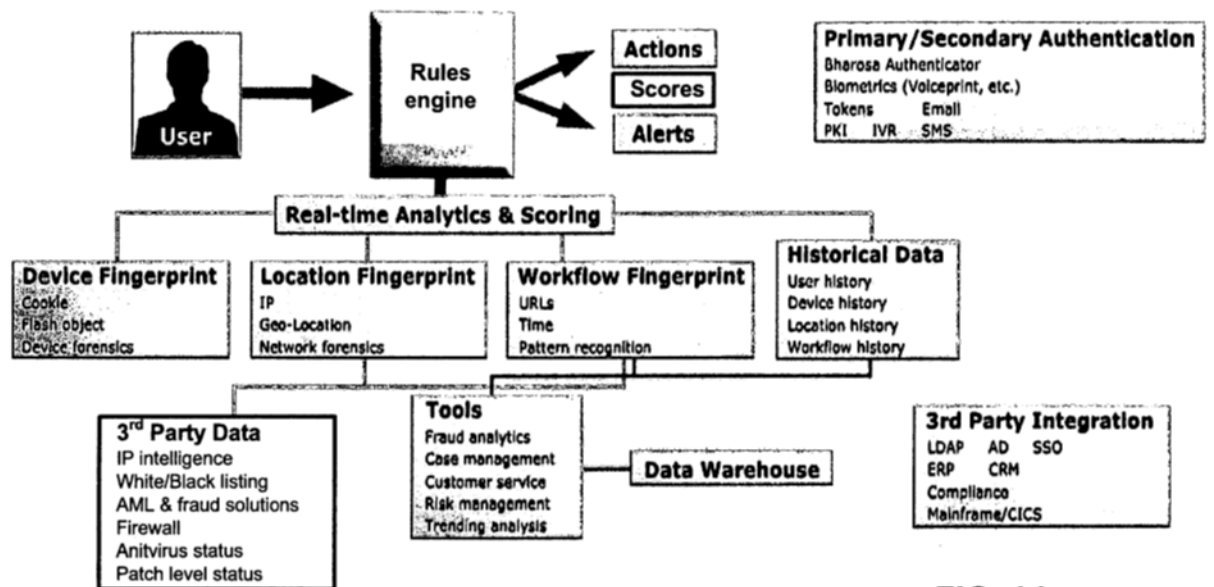


FIG. 14

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, ¶46; 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.”² 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.

² <https://web.archive.org/web/20051028001652/http://www.ffiec.gov/>.

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 transactions).

The Guidance explains that “[a]ccount fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation,” and 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 a camera 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, and Guidance are analogous art to the ’656 patent, because each is at least (1) in the same field of endeavor (computer network

applications for financial transactions); or (2) reasonably pertinent to a problem with which the inventor of the '656 patent was involved (e.g., fraud detection in electronic financial transactions). Compare 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]; APPL-1010, Title (“System and Method for Fraud Monitoring, Detection, and Tiered User Authentication”), FIG. 14, [0145]; APPL-1037, Title (“Authentication in an Internet Banking Environment”). APPL-1003, ¶53.

B. Ground 1: Claims 1, 4-10, and 13-19 are Rendered Obvious under §103(a) over Stone in view of Hoyos and Varghese.

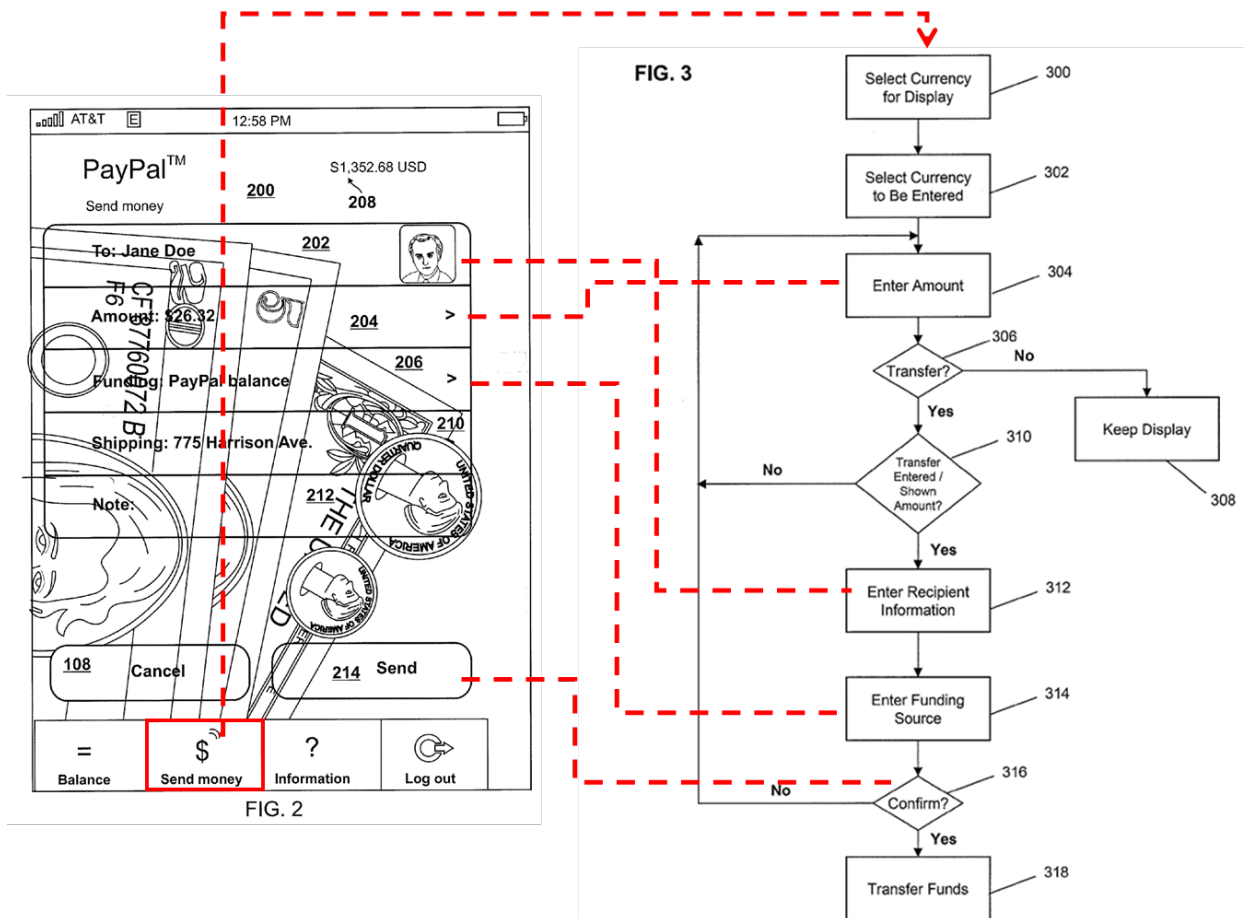
1. Combination of Disclosures/Embodiments of Stone

To the extent that Patent Owner argues that FIG. 2 and 3 are separate embodiments, 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.

A POSITA would have understood that the display of FIG. 2 and modification thereof could be used to implement the method of FIG. 3, e.g., by adding, removing, modifying components, or by using alternative design choices of buttons and icons. APPL-1003, ¶55; APPL-1008, [0055]-[0056].

An example implementation relationship with FIGS. 2 and 3 of Stone is provided below. APPL-1003, ¶56.



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., elements 202, 204, 206, and 214 correspond respectively to elements 312, 304, 314, and 316, and any modification needed for combining FIGS. 2 and 3 based on design needs would have been within the skills of a POSITA. APPL-1003, ¶¶57-58.

As an example, in Stone, after the user clicks the “\$Send money” icon of FIG. 2, the user interface for a financial transaction is displayed above the bottom task bar of FIG. 2 for performing the method of FIG. 3 or an obvious variation thereof, and a user transaction request for sending money is initiated. APPL-1003, ¶¶57-58.

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

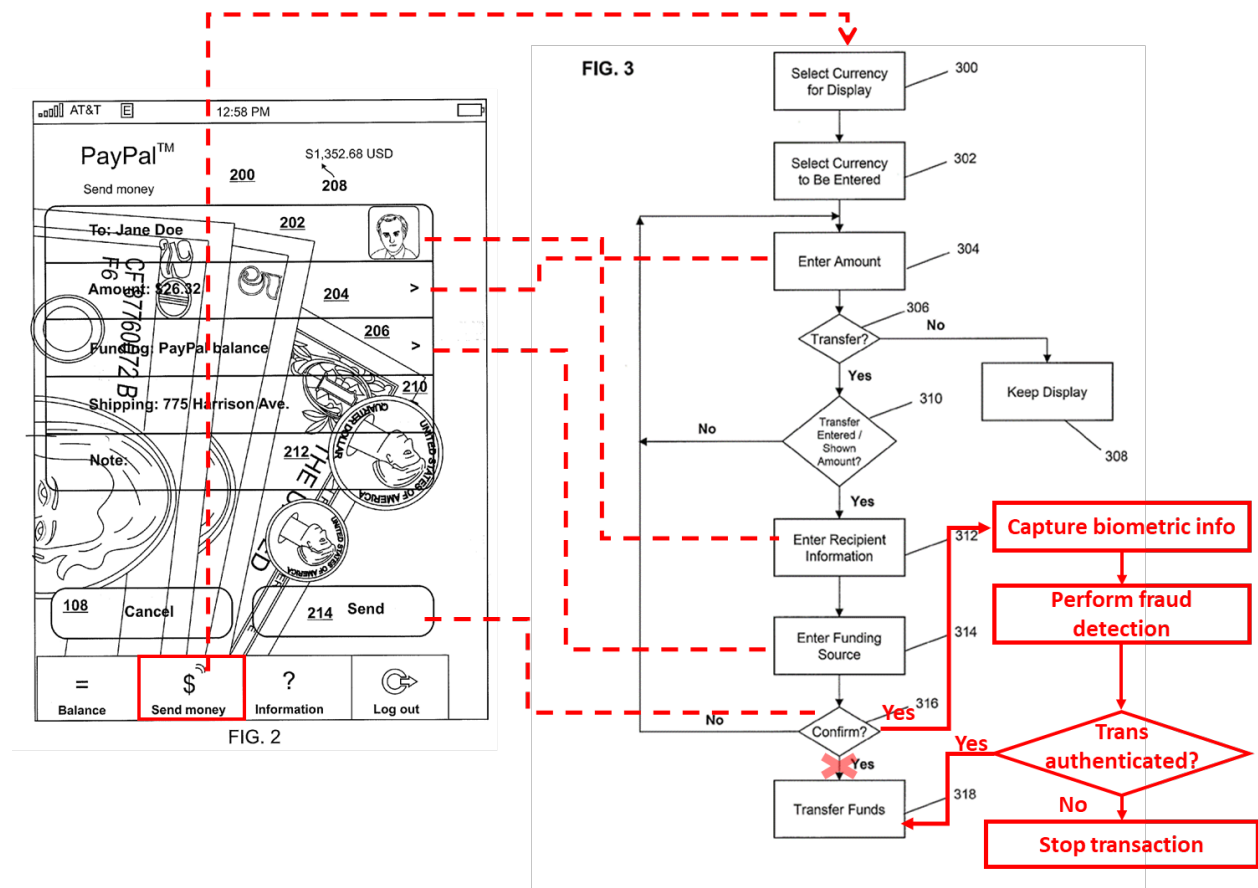
A POSITA would have been motivated to apply Hoyos’ teaching of fraud resistant biometric authentication in Stone’s financial transactions, for the benefits of improved fraud resistancy by addressing spoofing and achieving “improved deterrent against attempted fraudulent transactions, and decreased rejection of valid customers” as taught by Hoyos. APPL-1013, [0015], [0017]-[0022]; APPL-1003, ¶¶59-68.

As discussed at IX.A.5, Stone and Hoyos each are analogous art to the ’656 patent. APPL-1003, ¶60 (citing APPL-1010, [0079], APPL-1013, Title, Abstract, [0002]).

Further, it was well-known that financial transactions of Stone had a need for authentication for fraud detection (e.g., with higher levels of security for higher-risk transactions). APPL-1003, ¶61; APPL-1013, [0009], [0011]; APPL-1010, [0148]; APPL-1016, FIG. 3, [0073] (“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.”); APPL-1037, 1; APPL-1022, 1 (describing increased online fraud impacts consumer confidence and business, and “[d]riven by specific regulatory mandates such as FFIEC, PCI, and HIPAA, organizations are under pressure to proactively detect and prevent fraud”).

A POSITA would have been motivated to implement Hoyos’ spoofing-resistant biometric authentication for fraud detection in the system of Stone for “improved deterrent against attempted fraudulent transactions, and decreased rejection of valid customers.” APPL-1003, ¶62. By applying Hoyos’ biometric authentication “combining in one algorithm the live-person result with the match result,” various advantages are achieved, including spoofing prevention; reducing iterative attacks by eliminating clear feedback; reducing “the reject rate of true authentications” by using the liveness probability; 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].

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, incorporating Hoyos' biometric authentication teachings in Stone. 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)**

A POSITA would have been motivated to implement Hoyos' authentication phase for transaction authentication (e.g., capturing biometric data like 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., 316) the transaction request. APPL-1003, ¶64.

A POSITA would have understood that, compared to the alternative design choice of using previously captured authentication data as the input data for transaction authentication, performing real-time authentication using authentication data captured after and in response to user transaction request confirmation had various benefits with improved security. One example advantage is that it enables performing risk-based contextual authentication (e.g., specific authentication level requiring specific types of contextual data to capture) based on the transaction and assessed risk for improved fraud detection, where Hoyos already describes setting a higher decision threshold for a transaction with a higher amount/security type. APPL-1003, ¶65 (citing APPL-1013, [0028] (“A higher [amount] transaction may be authorized if the value of [decision probability] D is higher”); APPL-1016, FIG. 3, [0036] (“the number, type, and gradation (if any) of authentication can be varied as desired, **based on the context of the transaction**”), [0073] (“the necessary authentication level is determined based on the transaction criteria...such as value and type of transaction, as well as other factors.”). In Stone-Hoyos, a POSITA

would assess the risk of a transaction based on various transaction factors received through user interaction with icons in user interface (e.g., transaction type like “Send Money,” amount associated with elements 204/304, recipient associated with elements 202/312, source of funds associated with elements 206/314, etc.). For example, a large transaction amount would typically be considered higher risk than a small transaction amount. Similarly, an apparently unrelated overseas recipient or a person, account or banking institution on a watch list would presumably be considered a higher risk transaction than a transfer to an account owned by another customer of the same financial institution or to a person/account to whom the sender has previously transferred funds. Likewise, the source of funds, be it personal checking/savings, a business account, credit card, retirement account or trust account would likely present different risk postures, particularly in conjunctions with transaction amount and recipient information. Accordingly, a POSITA would be motivated to assess risk of a given transaction request after its factors are finalized/confirmed by the user’s indication of action taken, and performing the authentication with the risk-based authentication level. Furthermore, by capturing real-time, more accurate data, improved fraud detection and security is achieved, e.g., by avoiding imposters from communicating based on stolen biometric data and reducing spoofing. APPL-1003, ¶65 (citing APPL-1010, FIG. 14, [0097]-[0099] (real-time fraud analysis enforced “during post-

authentication, for example when a user is making transaction requests”), TABLE 10; APPL-1015, FIG. 4 (reproduced below, illustrating capturing biometric information and performing authentication after selecting desired transaction button); APPL-1035, 4:60-62 (describing real-time authentication data capture (e.g., real-time voice authentication) to “avoid imposters from communicating based on stolen biometric data”), 4:66-67).

A POSITA would have reasonably expected to succeed in configuring Stone-Hoyos, since the implementation of Hoyos’ biometric authentication in Stone would have required only routine knowledge well within the skill of a POSITA prior to the earliest effective filing date. APPL-1003, ¶66 (citing APPL-1008, [0004]; APPL-1009, 15:22-23; APPL-1013, Title, claims 13 and 14, [0007], [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; APPL-1016, [0040], [0042] (describing that fraud detection can “be performed **locally** or by transmission of []data to a remote source”); [0076].

For example, a POSITA would have been motivated to implement the fraud

detection analysis based on the biometric information **locally** on the user device of Stone for the benefits including reduced latency (e.g., by minimizing communication delays between the user device and network server), offline analysis capabilities (allowing for analysis even when the user device is offline or has limited connectivity), enhanced privacy (by reducing the amount of data that needs to be transmitted to the server and minimizing potential privacy concerns), efficient resource utilization (helping distributing the processing load to the user device), customization for device characteristics (enhancing fraud detection by considering user device specific characteristics and capabilities), improved security (where a malicious actor needs to compromise the user device system), and reduced server load for cost savings and improved scalability (especially where the system has a large user base). APPL-1003, ¶68 (citing APPL-1015, FIG. 3, 4:4-10; APPL-1016, [0040], [0042]; APPL-1038, 64 (“Biometric authentication can be implemented through systems performing the matching **either on the server or on the client side**,” where describing “security and privacy problems” and CPU-intensiveness of server side implementation, and “**relatively simple and cheap**” with security and privacy benefits of client side implementation)).

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

A POSITA would have been motivated to apply Varghese’s teaching of multifactor real-time authentication for user transaction requests, including

authentication based on physical location associated with the user and voice authentication, in Stone-Hoyos for improved security for financial transactions. APPL-1003, ¶¶69-79.

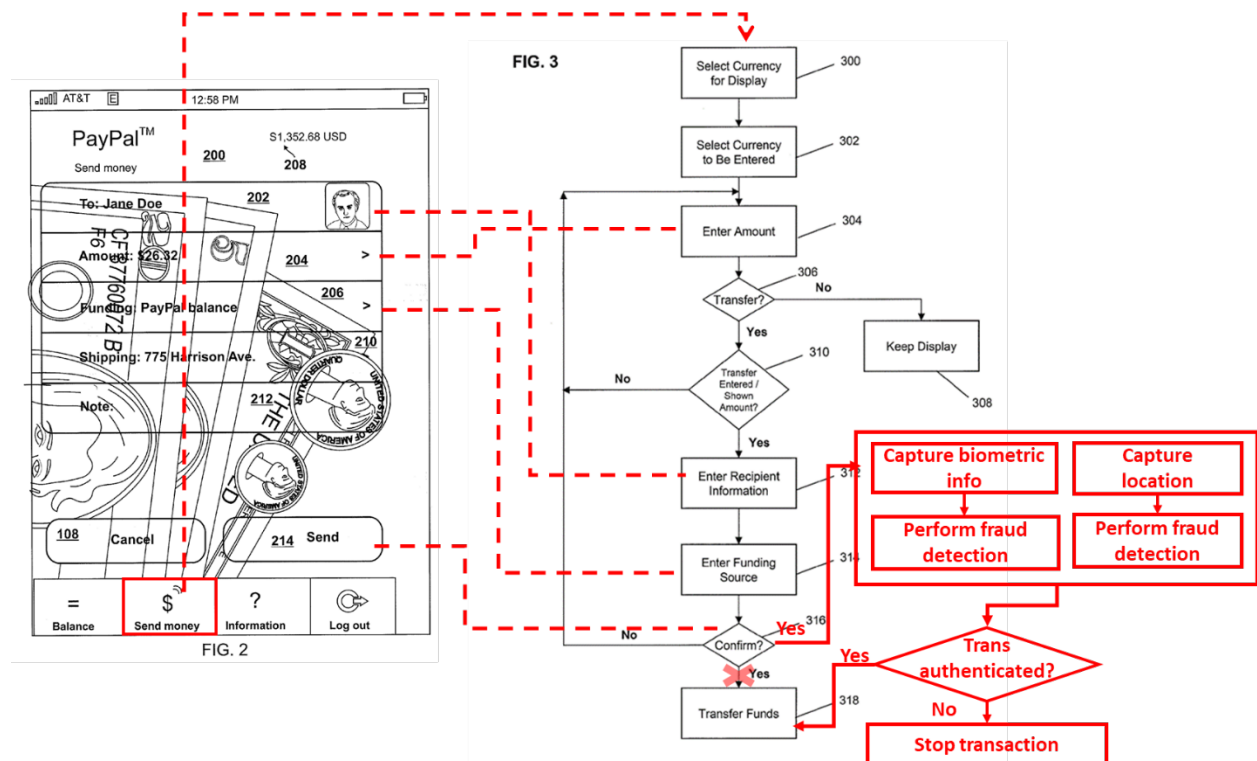
As discussed at IX.A.5, Varghese is analogous art to the '656 patent, and describes providing additional forms of authentication as needed, e.g., where the service provider is a bank or other financial institution which seeks a higher security authentication. APPL-1010, [0145]; APPL-1003, ¶70.

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, ¶71 (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, ¶71 (citing APPL-1010, [0012], [0035]; APPL-1016, [0043]; APPL-1037, 7-12).

Techniques implementing multifactor real-time authentication (including e.g., location authentication, voice authentication) to provide additional security for financial transactions, as taught in Varghese, were well-known. APPL-1003, ¶72 (citing APPL-1016, [0043]; APPL-1037, 7-14).

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, ¶73.



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

Similar to the reasons discussed above at IX.B.2, 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, ¶¶74-75; 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.

Moreover, capturing the location data after user transaction confirmation in Stone-Hoyos-Varghese for location authentication provides additional benefits in view of the location data already captured in Stone for currency display before confirmation at 316. For example, a POSITA would have been motivated to perform fraud detection based on whether the two locations (captured before for currency display and after confirmation at 316) match, for improved security. APPL-1003, ¶76.

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, ¶77. For example, a POSITA would have understood to implement the enrollment phase of transaction 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, ¶77.

Similar to the reasons discussed above at IX.B.2, it would have been within the skills of a POSITA to implement the teachings of Varghese, locally or remotely, in the system of Stone. For example, a POSITA would have implemented the location capturing taught by Varghese in the user device of Stone (e.g., using IP address, GPS, or other suitable location capturing methods). A POSITA would have understood that the fraud detection analysis based on location data could be implemented with the alternative design choices of implementing the fraud detection locally using the user device, or remotely (e.g., by sending the location data to a payment provider device, or another remote device) in the system

of Stone. APPL-1003, ¶78; APPL-1016, [0040], [0042] (describing that fraud detection can “be performed locally or by transmission of []data to a remote source”), [0076]); APPL-1038, 64.

In particular, a POSITA would have been motivated to implement the fraud detection analysis based on location locally on the user device of Stone for the benefits including reduced latency (e.g., by minimizing communication delays between the user device and network server), offline analysis capabilities (allowing for analysis even when the user device is offline or has limited connectivity), enhanced privacy (by reducing the amount of data that needs to be transmitted to the server and minimizing potential privacy concerns), efficient resource utilization (helping distributing the processing load to the user device), customization for device characteristics (enhancing fraud detection by considering user device specific characteristics and capabilities), improved security (where a malicious actor needs to comprise the user device system), and reduced server load for cost savings and improved scalability (especially where the system has a large user base). APPL-1003, ¶79 (citing APPL-1015, APPL-1016, APPL-1038).

4. Claim 1

[1.0] A system, comprising:

Stone discloses or renders obvious the preamble to the extent that it’s limiting. APPL-1003, ¶¶80-82.

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]. 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].

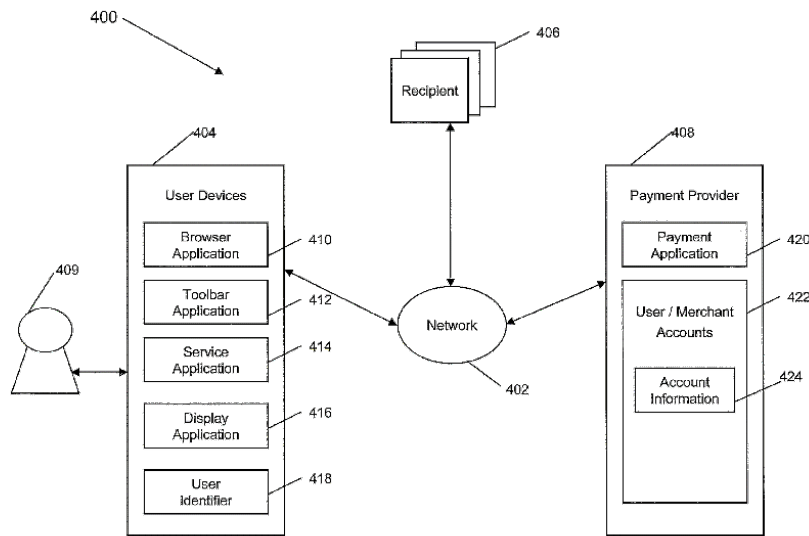


FIG. 4

APPL-1008, FIG. 4

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

[1.1] a processor configured to:

Stone alone or Stone-Hoyos-Varghese renders obvious this element. APPL-1003, ¶¶83-89.

First, the ’656 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.”). APPL-1001, 2:14-16. As such, “a processor” as claimed includes one or more devices, circuits, and/or processing cores, and Stone discloses or renders obvious “a processor” as claimed.

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...subsystems and components, such as a **processing component 504** (e.g., processor, micro-controller, digital signal processor (DSP), etc.); APPL-1008, claim 1 (“A device comprising....a **processor**”).

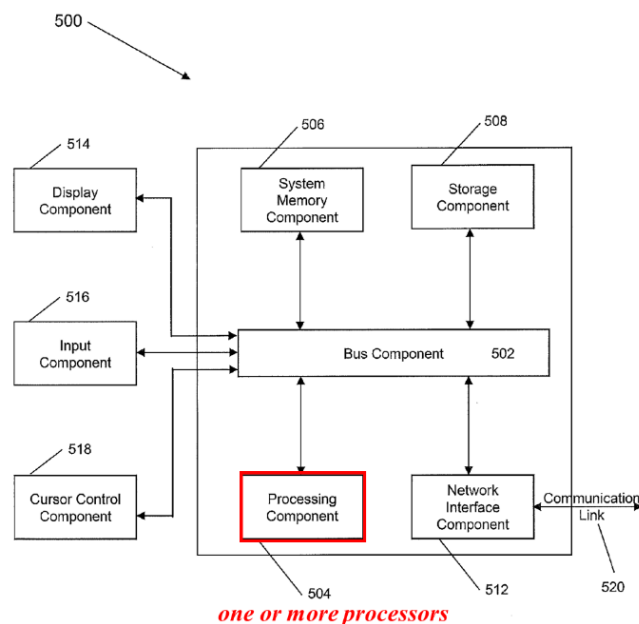


FIG. 5

APPL-1008, FIG. 5, annotated

Further, as shown in FIG. 4 of Stone below, the system 400 includes a processor (e.g., processor 504 in user device 404, alone or in combination with other processors including the processor 504 of other devices) configured to

process data, such as computer program instructions, for perform processes for a transaction. As discussed in detail at [1.2]-[1.9] below, the processor is configured to perform the steps for the transaction.

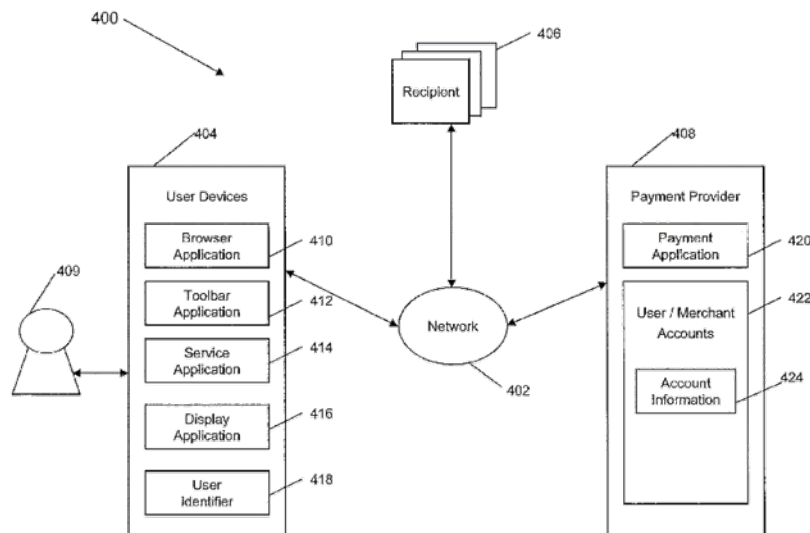


FIG. 4

APPL-1008, FIG. 4

Second, to the extent that Patent Owner argues that “a processor” requires a **single** processor (contradictory to its own definition of “processor”), Stone alone or Stone-Hoyos-Varghese renders it obvious. APPL-1003, ¶¶87-88.

Specifically, as discussed at IX.B.2 and IX.B.3, a POSITA would have been motivated to implement various steps for an electronic transaction (e.g., steps of [1.2]-[1.8] discussed below) **locally** (e.g., on the user device of Stone) or remotely (e.g., on the service provider of Stone). For example, a POSITA would have been motivated to implement the authentication steps (including capturing data and fraud detection analysis based thereupon) locally for the benefits including reduced

latency, offline analysis capabilities, enhanced privacy, efficient resource utilization, customization for device characteristics, improved security. APPL-1003, ¶88 (citing APPL-1015, APPL-1016); APPL-1015, FIG. 3, 4:4-10; APPL-1016, [0040], [0042], [0076]. As such, to the extent that Patent Owner argues that “a processor” requires a **single** processor, Stone alone or Stone-Hoyos-Varghese renders obvious this limitation because it teaches using a single processor of the user device to perform the processes discussed at [1.2]-[1.8] below.

Therefore, Stone alone or Stone-Hoyos-Varghese renders obvious this element.

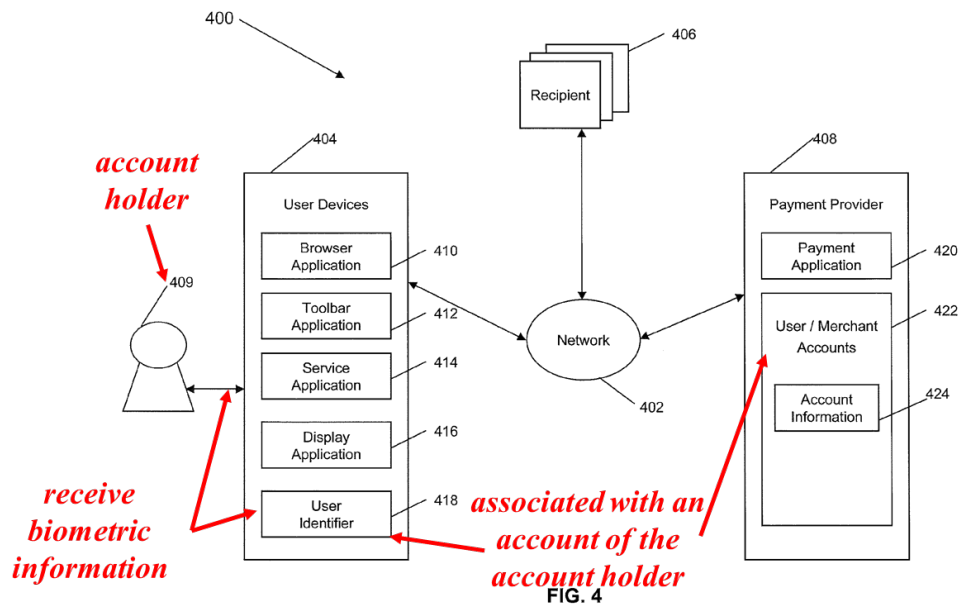
[1.2] receive biometric information associated with an account holder; store, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder;

Stone alone or Stone-Hoyos-Varghese renders obvious these elements.

APPL-1003, ¶¶90-95.

First, as shown in FIG. 4 of Stone below, Stone describes receiving from an account holder (user 409), biometric information (to be stored as “biometric id”) associated with the account holder (user 409); and storing the biometric information as “biometric id” in a data store (storage component 508) of user device 404, where the stored “biometric id” is a user attribute of user identifier 418 associated with an account (account 422) of the account holder (user 409) . APPL-1008, [0045] (“**User identifier 418** may include **attributes related to the user**,

such as personal information (e.g.,...**biometric id**”); APPL-1003, ¶91 (explaining that a POSITA would have understood that “biometric id” means “biometric identification information,” citing APPL-1013, [0079]).



APPL-1008, FIG. 4, annotated

Specifically, it is basic fundamental knowledge of biometric authentication, that Stone’s biometric information/“biometric id” is typically received and stored on user device 404 during an enrollment/registration process, and is also referred as “enrollment data” used for subsequent comparison with the later captured data to provide an authentication decision. APPL-1003, ¶92 (citing APPL-1014, [0009]; APPL-1021, Abstract; APPL-1023, 8:3-9:39; APPL-1013, [0003]; APPL-1024, 3:6-11; APPL-1033, FIG. 3; APPL-1037, 9-11).

Second, as shown in annotated FIG. 4 of Stone below, Stone describes that the received biometric information is associated with an account holder (user 409), and the biometric information (“biometric id”) of user identifier 418 stored in user device 404 is associated with a user account 422 of the account holder 409 (account of the account holder), where user identifier 418 is used for identifying the account 422. APPL-1003, ¶93; APPL-1008, [0045], [0048].

Third, to the extent that Patent Owner argues that Stone does not explicitly describe “biometric id” as the reference biometric information for comparison in authentication, Hoyos expressly describes receiving and storing biometric information during enrollment, and the stored biometric information is used for comparison with subsequent captured biometric data during transaction authentication. APPL-1003, ¶94 (citing APPL-1013, [0003] (“Biometric identification and authentication systems...are known to be useful for [] comparing biometric data acquired from an individual to stored sets of biometric data of known “enrolled” individuals”). As discussed at IX.B.2, a POSITA would have been motivated to apply Hoyos’ fraud-resistant biometric authentication system in Stone, including implementing Hoyos’ teaching of capture and store enrollment biometric data during enrollment for subsequent comparison in transaction authentication.

Therefore, Stone alone or Stone-Hoyos-Varghese renders obvious this

element.

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

Stone discloses or renders obvious this element. APPL-1003, ¶¶96-99.

Specifically, as shown in annotated FIG. 2 of Stone below, Stone discloses that the processor is configured to *render, in one or more interfaces* (e.g., interface 200 of FIG. 2), *a virtual likeness of a face* (e.g., recipient icon including “a picture of the recipient”) *of a recipient of an electronic transaction* (e.g., picture of recipient next to the name box 202 of FIG. 2). APPL-1008, FIG. 2, [0024] (“display 200 has a **name box 202 indicating the recipient of funds as well as a picture of the recipient**”), [0020], [0036] (discussing providing “a **recipient icon** on the display, such as a **picture of the recipient**”), [0048]. APPL-1003, ¶97.

Stone’s “**recipient icon** on the display, such as a **picture of the recipient**” teaches using a photograph of the recipient for display, because photographs for recipient icon are quick and easy for users to take and upload, especially with the availability of digital cameras, and because photographs may increased transaction confidence. APPL-1003, ¶98 (a POSITA would have understood Stone’s disclosure of “**photograph image**” as a user attribute applies to both user device and recipient device, which would be used as recipient icon, citing APPL-1008, [0045], [0046]).

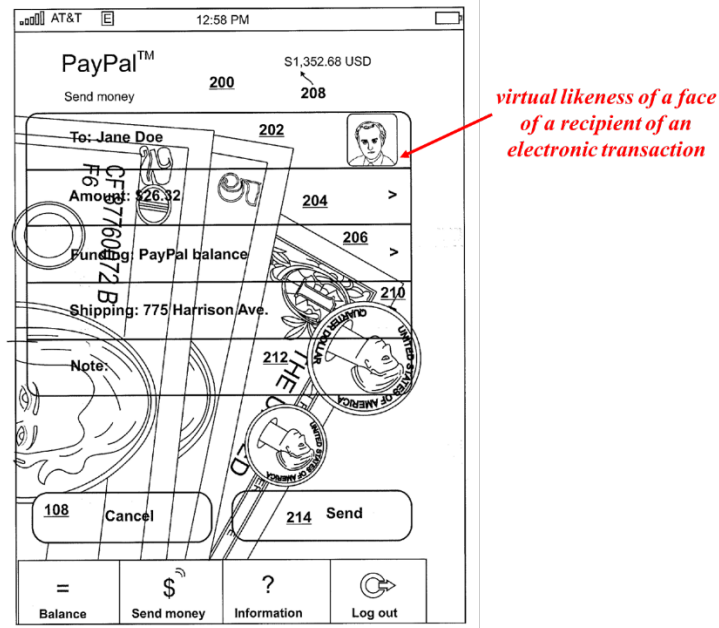


FIG. 2
APPL-1008, FIG. 2, annotated

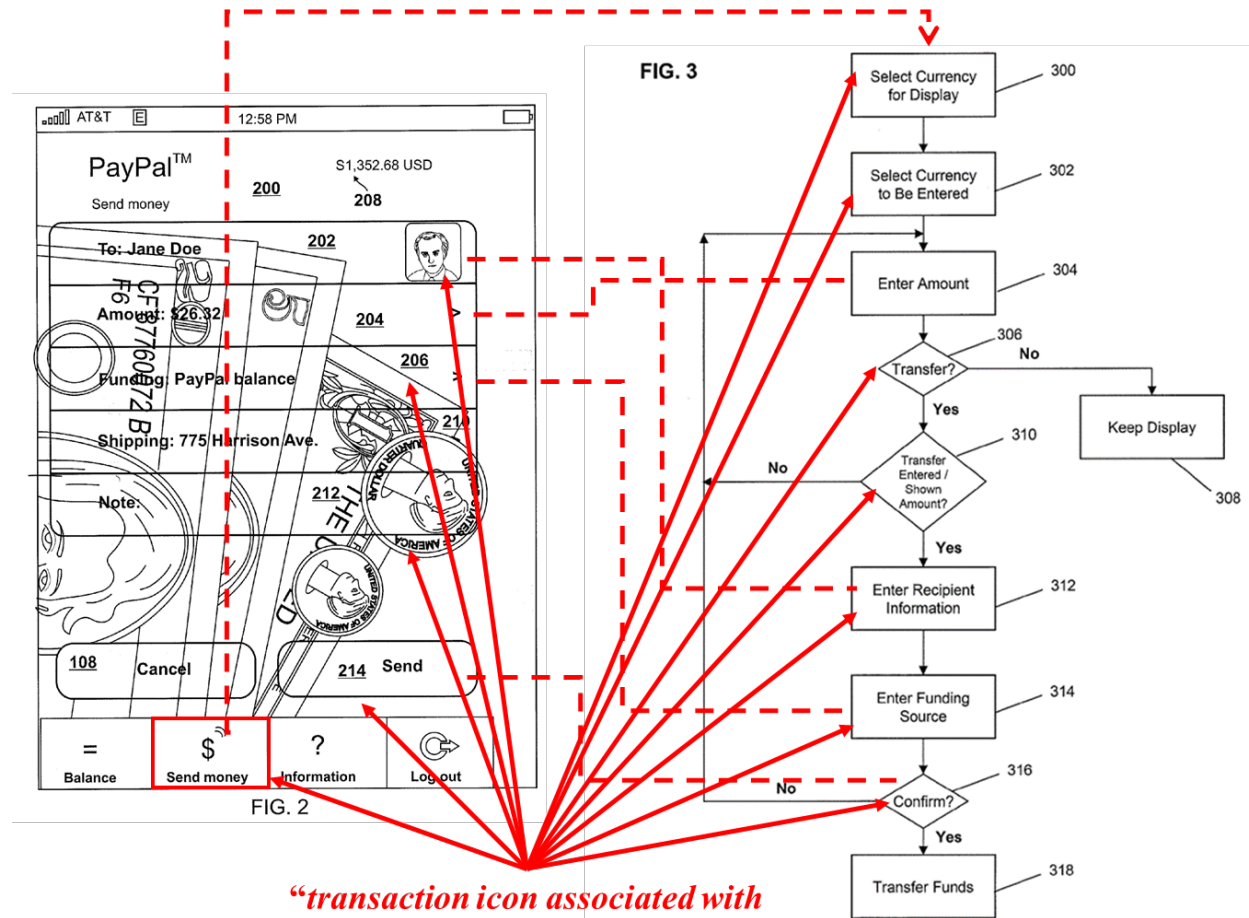
Therefore, Stone discloses or renders obvious this element.

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

Stone discloses or renders obvious this element. APPL-1003, ¶¶100-103.

First, as shown in annotated FIGS. 2 and 3 of Stone below, **each** of the annotated control elements/blocks (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, because it was well-known to implement each of these annotated items using a transaction icon in the interfaces to provide a visual indicator for various user interactions to

initiate, continue, and/or confirm the transaction request associated with the electronic transaction. APPL-1003, ¶101.



*“transaction icon associated with
the electronic transaction”*

APPL-1008, FIGS. 2 and 3, annotated

Second, to the extent that any of the control items described above is not explicitly described as a transaction icon in Stone, a POSITA would have been motivated to implement the control items using a transaction icon, because icon and button are alternative design choices for control elements, and using transaction icons provides “a more visually rich interface.” 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.”), APPL-1003, ¶102 (citing APPL-1008, [0038] (describing using “specific card” visual for payment cards for improved visual presentation), [0024], [0035], [0025], [0020], [0036]).

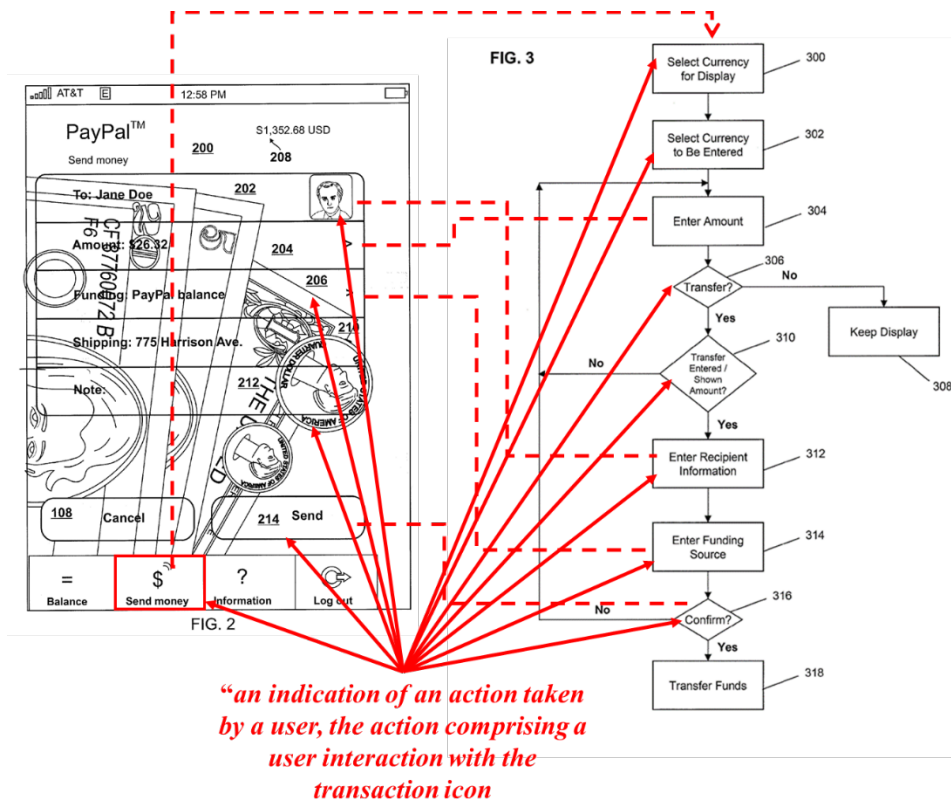
Therefore, Stone discloses or renders obvious this element.

[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 one or more interfaces;

Stone discloses or renders obvious this element. APPL-1003, ¶¶104-109.

First, as discussed at [1.4], each of the annotated control elements/blocks 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, ¶105.

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, ¶106.



APPL-1008, FIGS. 2 and 3, annotated

For example, in response to a user interaction with (e.g., clicking/tapping on) the “\$Send Money” icon, the processor receives an indication of user action for initiating a send money transaction request, and in response, a corresponding interface 200 for a send money transaction is displayed. APPL-1003, ¶107.

Dr. Jones describes in detail examples of user interactions (e.g., user clicking/tapping on/sliding/dragging (including from/to)) relating to each of the transaction icons, and the processor receiving an indication in response to the user interactions. APPL-1003, ¶108 (citing APPL-1020, 27, 34-36; APPL-1019, 6:24-26; APPL-1008, [0024], [0020], [0036]).

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., 300, 302, 306 of FIG. 3 or other user actions associated with the transaction request). APPL-1003, ¶109; APPL-1008, [0025].

Accordingly, Stone discloses or renders obvious this limitation.

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

Stone-Hoyos-Varghese renders this element obvious. APPL-1003, ¶¶111-122.

First, as shown in annotated FIG. 14 of Varghese below, Varghese describes real-time risk-based contextual authentication, including capturing real-time contextual information (e.g., “biometrics” and “location” data associated with the user), after the user submits its transaction request (referred to as “post-authentication” in Varghese, compared to “pre-authentication” including authentication for user login request). APPL-1003, ¶112. Varghese describes an example for capturing location data by capturing location data (user IP address) and determining the physical location using a “geolocation service” based on the

user IP address. APPL-1013, [0140]. A POSITA would have implemented any suitable geolocation techniques well-known in the art could be used to capture location data, e.g., capturing a GPS data. APPL-1016, [0041]; APPL-1008, [0026] (describing that detection of the location of the user “may be determined through GPS or any other location-determining method”).

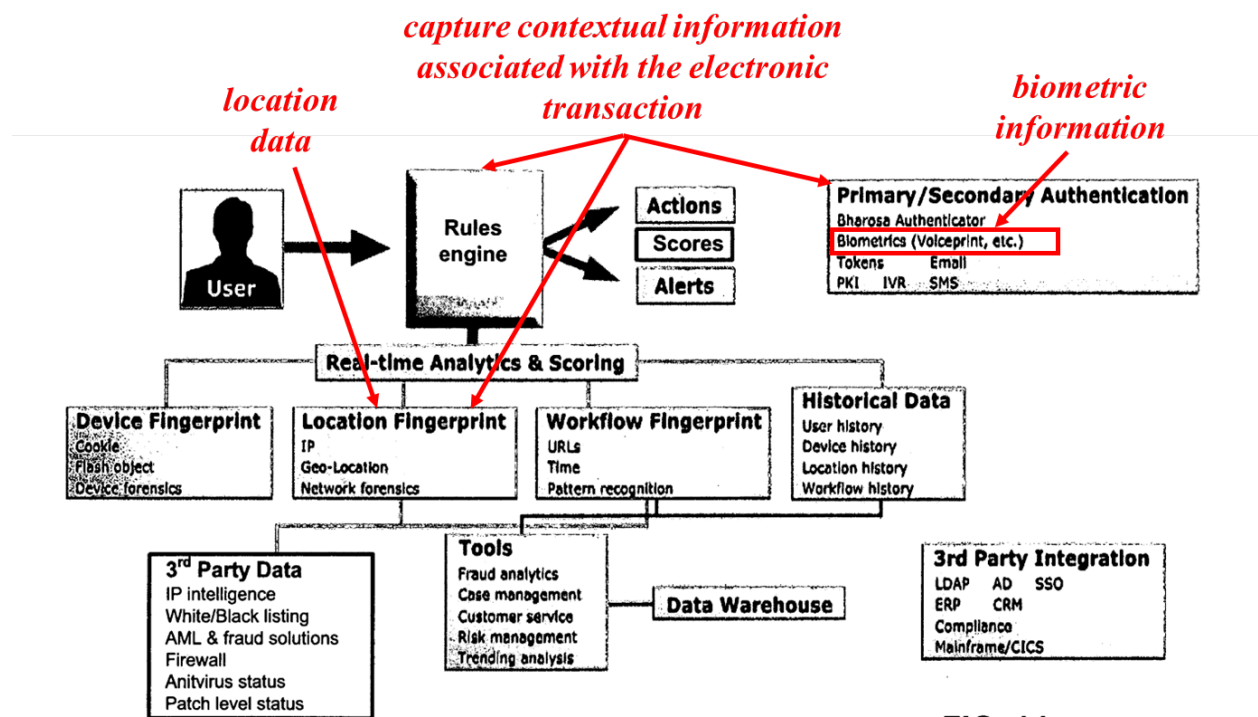


FIG. 14

APPL-1010, FIG. 14, annotated

Specifically, Varghese describes “post-authentication” real-time risk-based contextual authentication, where real-time contextual information (e.g., “biometrics” and “location” data associated with the user) are captured after the user submits its transaction request and used for real-time risk analysis for risk-based authentication. APPL-1010, FIG. 14, [0097]-[0099] (describing that these

authentication/fraud detection techniques “can be enforced...**during post-authentication**, for example when a user is making transaction requests” separate from login authentication), [0074], [0089]. Varghese describes, “[l]ocation information and device information are important criteria, **especially** in the pre-authentication period,” and as such, describing that location information is an important criterion in **both** pre-authentication and post-authentication. APPL-1003, ¶113; APPL-1010, [0093], [0109].

A POSITA would have understood “real-time” authentication of Varghese includes both real-time capture and real-time analysis of authentication data. APPL-1003, ¶114 (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,” specifically, the location data captured for location authentication for fraud detection, is contextual information of the transaction, e.g., a user location from which the transaction request originates. APPL-1003, ¶115; APPL-1010, [0081], [0140], [0142], claim 31.

Second, 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 based thereupon. APPL-1003, ¶116; APPL-1013, [0017].

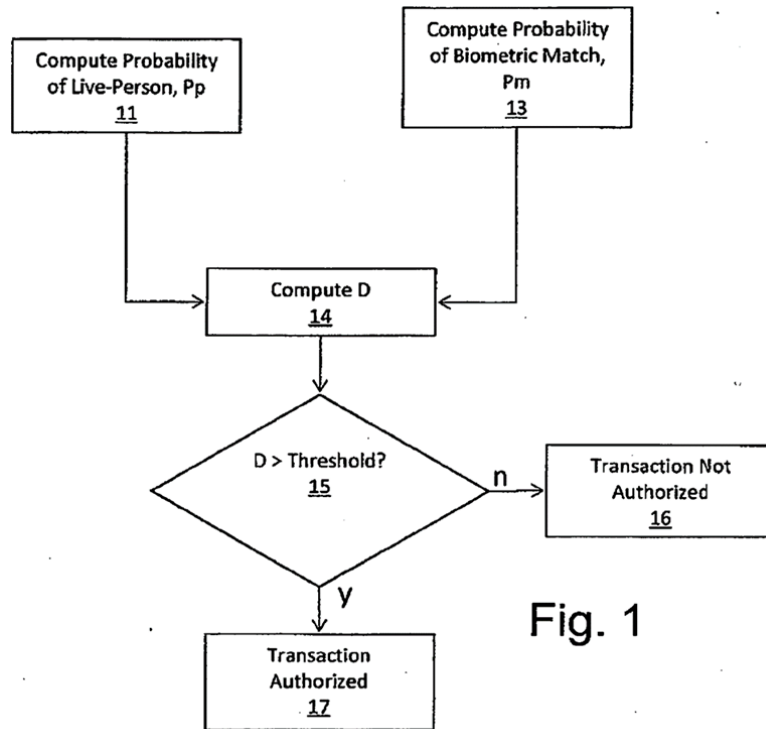
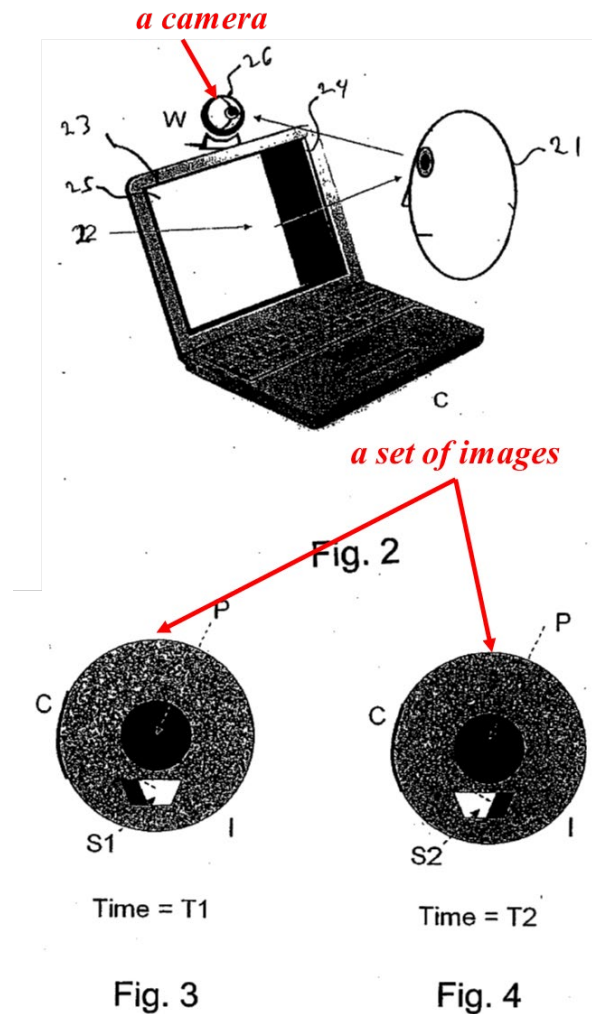


Fig. 1

APPL-1013, FIG. 1

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]; APPL-1003, ¶117 (citing APPL-1011, Abstract; APPL-1012, Abstract); APPL-

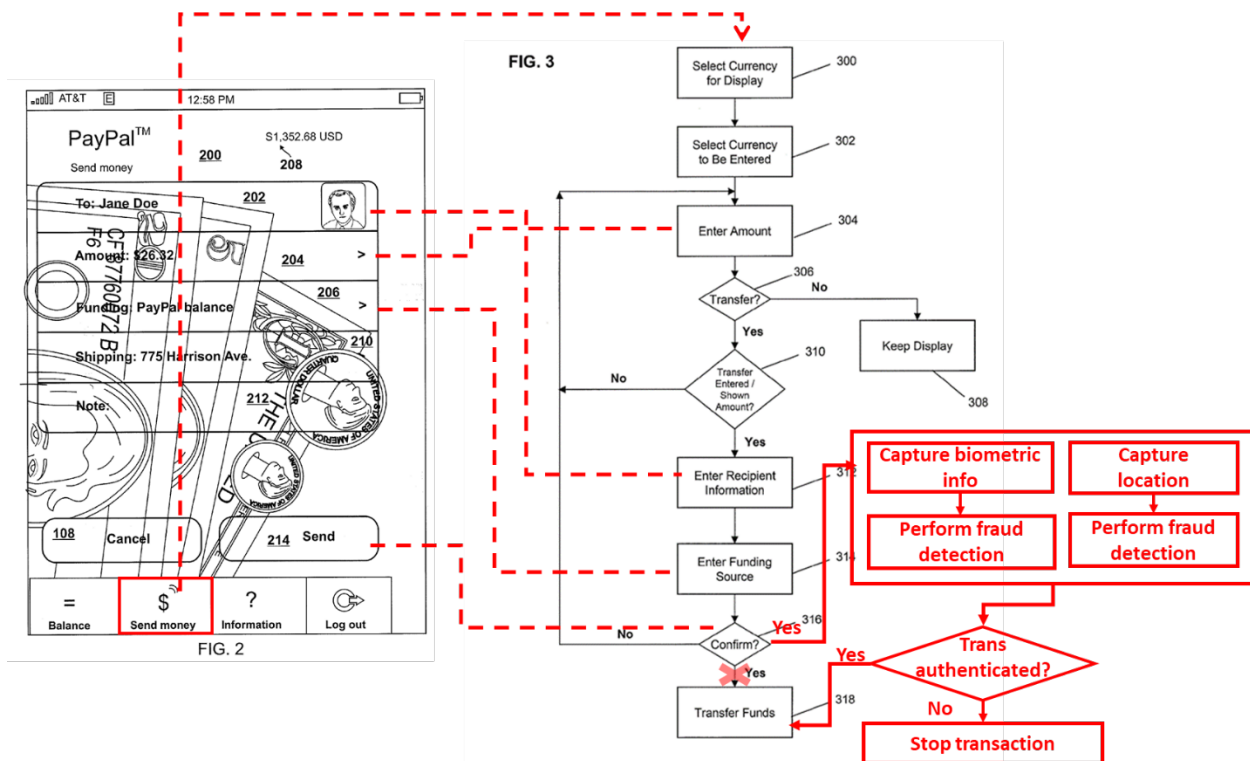
1003, ¶118 (describing in detail that an example of biometric information is capturing a set of images using a camera, citing APPL-1013, [0034], claims 5-8; FIGS. 2-4, [0018]-[0020], claim 7).



APPL-1013, FIGS. 2-4, annotated

Third, as shown in example Stone-Hoyos-Varghese below and discussed at IX.B.2 and 3, a POSITA would have been motivated to apply multifactor real-time contextual-based authentication including location authentication taught by

Varghese and fraud-resistant biometric authentication taught by Hoyos in electronic financial transaction system of Stone for fraud detection, which is performed **subsequent to** user transaction confirmation (e.g., after user interaction with any of the icons for initiating, continuing, and confirming the transaction request) for improved security. A POSITA would have been motivated to implement the following example Stone-Hoyos-Varghese for performing a financial transaction: APPL-1003, ¶119.



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

A POSITA would have been motivated to implement the multifactor real-time authentication as taught by Varghese and Hoyos (including capturing the contextual data including biometric data and location data for fraud analysis) 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., 316) the transaction request, for the benefits of risk-based contextual authentication adaptive for the specific transaction based on transaction information, more accurate real-time information for real-time authentication, and performing fraud analysis based on locations captured before and after transaction request for improved security. APPL-1003, ¶120; APPL-1010, FIG. 14, [0091], [0097]-[0099], [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; *see also* IX.B.2-3.

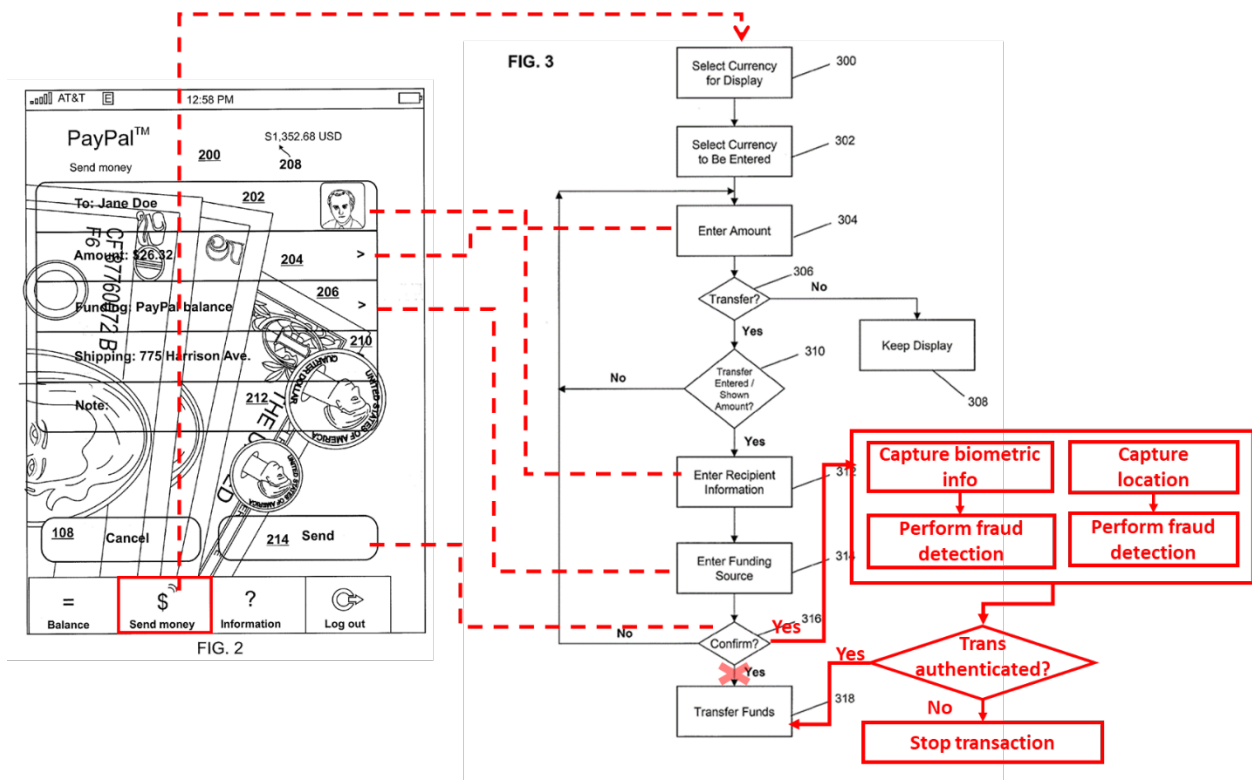
Accordingly, Stone-Hoyos-Varghese renders obvious this element.

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

Stone-Hoyos-Varghese renders this element obvious. APPL-1003, ¶¶123-125.

Specifically, as discussed at [1.6] above and at [1.7.2]-[1.7.3] in detail below, and shown in example Stone-Hoyos-Varghese below, in the implemented multifactor real-time authentication, analysis based on the captured biometrics and location data (including biometric authentication analysis as taught by Hoyos and

location analysis as taught by Varghese) is performed for fraud detection analysis, after the user confirms the transaction request at 214/316 and after contextual biometrics and location data associated with the transaction request and user are captured. APPL-1003, ¶¶124-125.



Example of Stone-Hoyos-Varghese

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

Therefore, Stone-Hoyos-Varghese renders obvious this element.

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

Stone-Hoyos-Varghese renders this element obvious. APPL-1003, ¶¶126-

131.

First, Stone-Hoyos-Varghese teaches this limitation, because it was fundamental knowledge that biometric authentication—such as that in Stone-Hoyos-Varghese—performs a comparison based at least in part on the stored biometric information (obtained and stored during its enrollment stage) and the captured biometric information (*e.g.* captured through live scan at its transaction authentication stage), as discussed at [1.2]. APPL-1003, ¶127; APPL-1014, [0009]; APPL-1021, Abstract; APPL-1023, 8:3-9:39; APPL-1013, [0003]; APPL-1024, 3:6-11; APPL-1033, FIG. 3; APPL-1037, 9-10.

Second, Stone-Hoyos-Varghese teaches this limitation, because as shown in annotated FIG. 1 of Hoyos, Hoyos' biometric authentication, as applied in the combination, performs a comparison (block 13 of FIG. 1) based at least in part on the stored biometric information and the captured biometric information. APPL-1003, ¶¶128-129 (citing APPL-1013, [0033] (describing computing and using “the **probability of a biometric match, P_m**” for authentication decision), [0003]).

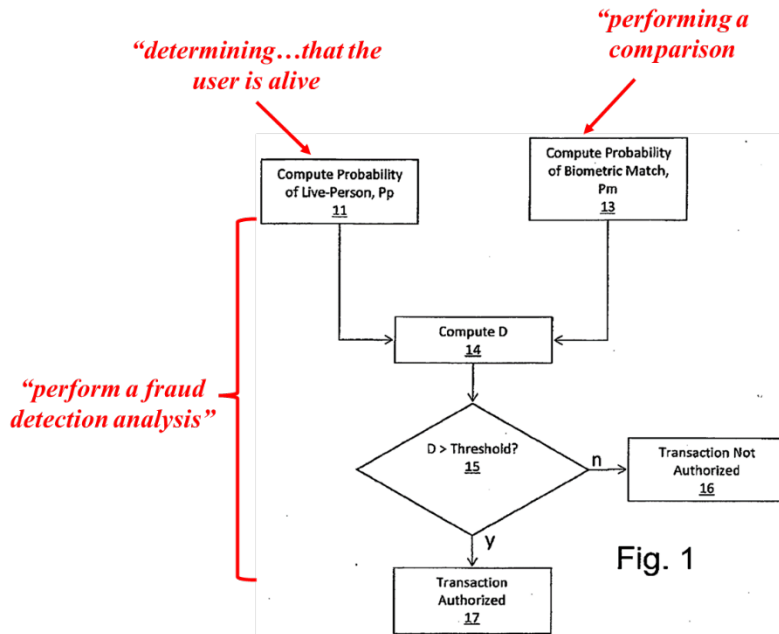


Fig. 1

(Hoyos) APPL-1013, FIG. 1, annotated

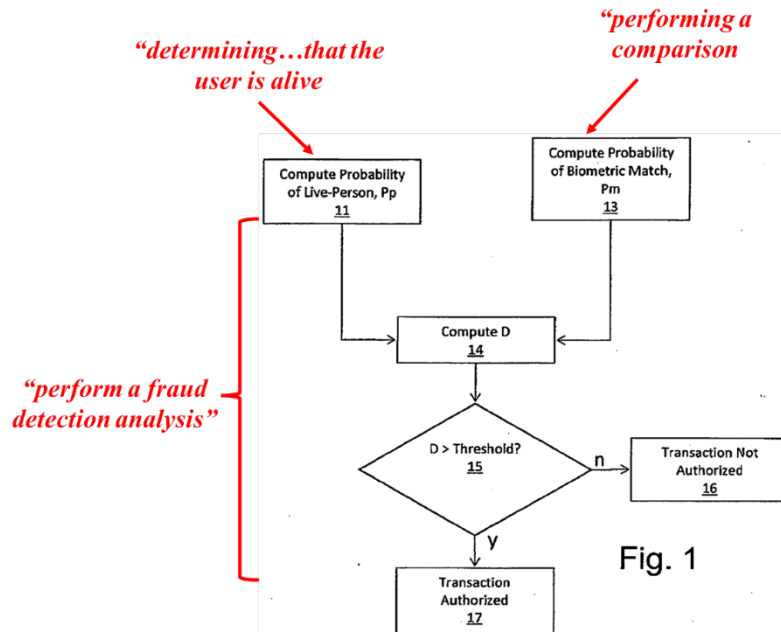
Additionally, in Stone-Hoyos-Varghese, in addition to Hoyos' biometric authentication based on a combination of comparison and liveness analysis, for some transactions with a higher risk, a POSITA would have been motivated to apply additional biometric authentication including voice authentication (e.g., for transaction requests requiring higher-level security) as taught by Varghese, which similarly teaches comparison of live capture with previously stored voice samples. APPL-1003, ¶130 (citing APPL-1010, FIG. 14, [0079]; APPL-1033, FIG. 3, 1438).

Therefore, Stone-Hoyos-Varghese renders obvious this element.

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

Stone-Hoyos-Varghese renders this element obvious. APPL-1003, ¶¶132-136.

As shown in annotated FIG. 1 of Hoyos below, Hoyos' biometric authentication, as applied in Stone-Hoyos-Varghese, teaches determining, based at least in part on the captured biometric information, that the user is alive. APPL-1003, ¶133.



APPL-1013, FIG. 1, annotated

Specifically, Hoyos describes that its authentication system 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]; APPL-1003, ¶134. Hoyos describes that "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]; APPL-1003, ¶135 (describing various liveness determination techniques based images

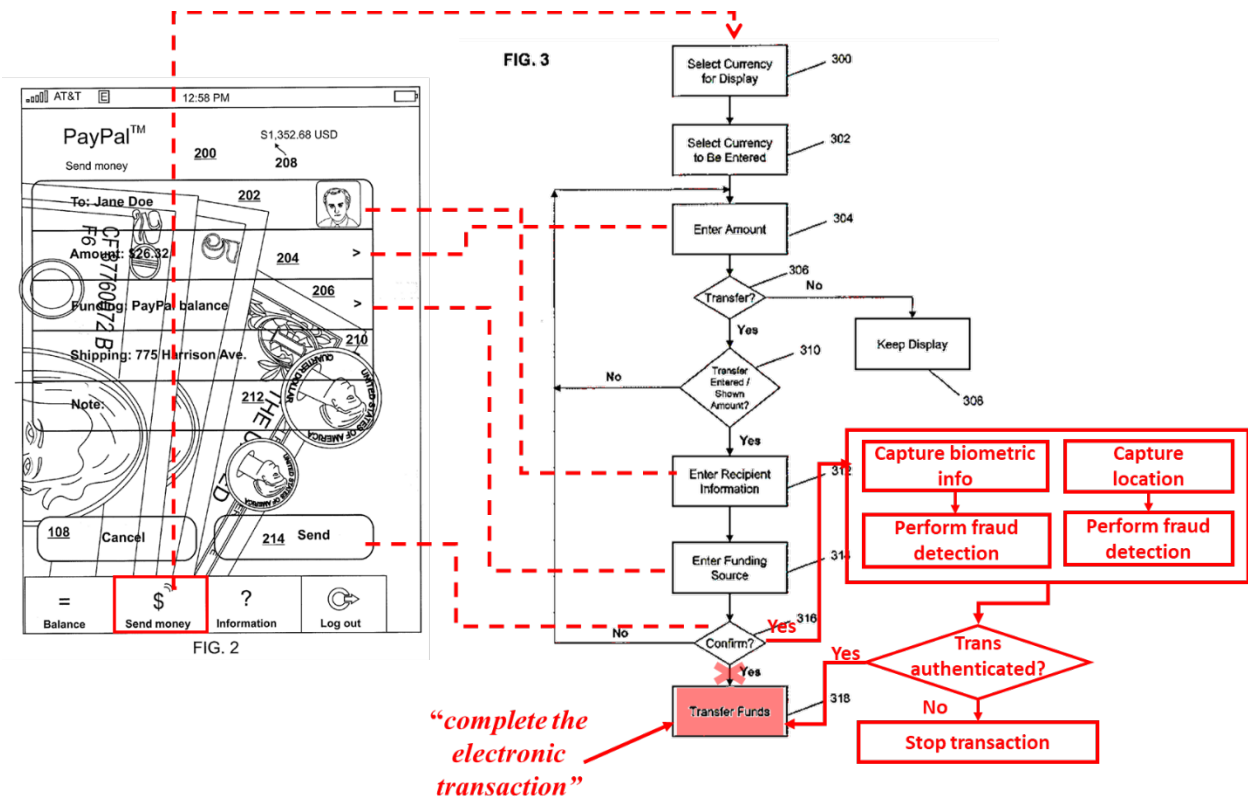
with eye/pupil analysis, finger or palm temperature, citing APPL-1013, [0011], [0018]-[0021], claims 5-8).

Therefore, Stone-Hoyos-Varghese renders obvious this element.

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

Stone-Hoyos-Varghese renders this element obvious. APPL-1003, ¶¶137-140.

Specifically, Stone-Hoyos-Varghese teaches completing the electronic transaction (e.g., performing transferring funds at 318 of FIG. 3 of Stone) based at least in part on both the user interaction with the transaction icon (see [1.6]) and performing the fraud detection analysis (*see* [1.7.1]-[1.7.3]), because the user interaction is the user's indication to continue/confirm the transaction request, and authorization of the transaction request is provided based on the fraud detection analysis, as taught by Hoyos and well-known in the art. APPL-1003, ¶¶138-139 (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-Hoyos-Varghese (annotated based on APPL-1008, FIGS. 2 and 3)

Therefore, Stone-Hoyos-Varghese renders this element obvious.

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

Stone alone or Stone-Hoyos-Varghese renders obvious this element. APPL-1003, ¶¶137-143.

Specifically, Stone discloses a memory (e.g., system memory component 506 of FIG. 5) coupled to a processor 504 in each device of the system, and the memory is configured to provide the processor with instructions for various processes for an electronic transaction. APPL-1003, ¶138; APPL-1008, [0050] (“system 500 performs specific operations by **processor 504** executing one or

more sequences of one or more instructions contained in system memory component 506"); FIG. 5; [0049].

Therefore, Stone alone or Stone-Hoyos-Varghese renders obvious this element, and Stone-Hoyos-Varghese renders obvious claim 1 in its entirety.

5. Claim 4

[4.0] The system of claim 1 wherein the virtual likeness of the face of the recipient was provided by the recipient.

Stone discloses or renders obvious this element. APPL-1003, ¶¶144-148.

First, as discussed at [1.3] above, Stone teaches rendering the virtual likeness of the face of the recipient in interface 200, e.g., using the photograph/icon information of user identifier 418 of recipient devices 406. APPL-1008, [0045]-[0046], [0020], [0036].

Second, Stone's electronic transaction system provides a social networking aspect for connecting people, which was well-known in the art. APPL-1008, FIG. 2, [0020], [0036]; APPL-1003, ¶146(citing APPL-1036, [0002]).

A POSITA would have been motivated to apply the well-known technique that an account holder (e.g., recipient) is provided the option to select the profile image for display (e.g., on a sender's display of FIG. 2 of Stone), for benefits including online identity expression and "increase[ing] a level of trust" between users. APPL-1003, ¶147 (citing APPL-1036, [0006], APPL-1009, 1:20-28; 15:15-27).

Accordingly, Stone-Hoyos-Varghese renders obvious claim 4.

6. Claim 5

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

Stone discloses or renders obvious this element. APPL-1003, ¶¶149-152.

First, Stone’s funding source box 206 of FIG. 2 discloses a transaction icon for selecting a fund source. APPL-1008, [0034], FIG. 2, [0024] (display including “a funding source box 206, indicating the source or account where the user’s funds will be transferred from.”); APPL-1003, ¶150.

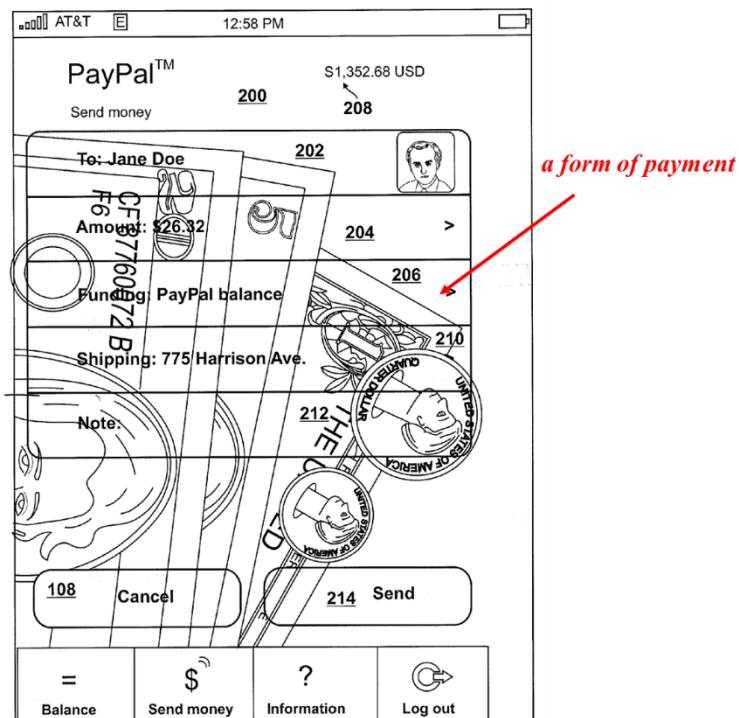


FIG. 2

APPL-1008, FIG. 2, annotated

Second, to the extent that Stone does not explicitly describe an icon representing a form of payment, a POSITA would have been motivated to

implement the funding source selection using a form of payment icon (e.g., “the specific card, such as a PayPal card, Visa, MC, AMEX”) for improved visual presentation, “**as contrasted to** a generic representation of a card or no visual at all.” APPL-1003, ¶151 (citing APPL-1008, [0004], [0038]).

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

7. Claim 6

[6.0] The system of claim 5 wherein the transaction icon comprises a graphical representation of money.

Stone discloses or renders obvious this element. APPL-1003, ¶¶153-156.

First, as shown in annotated FIG. 2 of Stone below, each of the transaction icons “\$ Send money,” “Send” 214, and the virtual currency discloses the transaction icon.

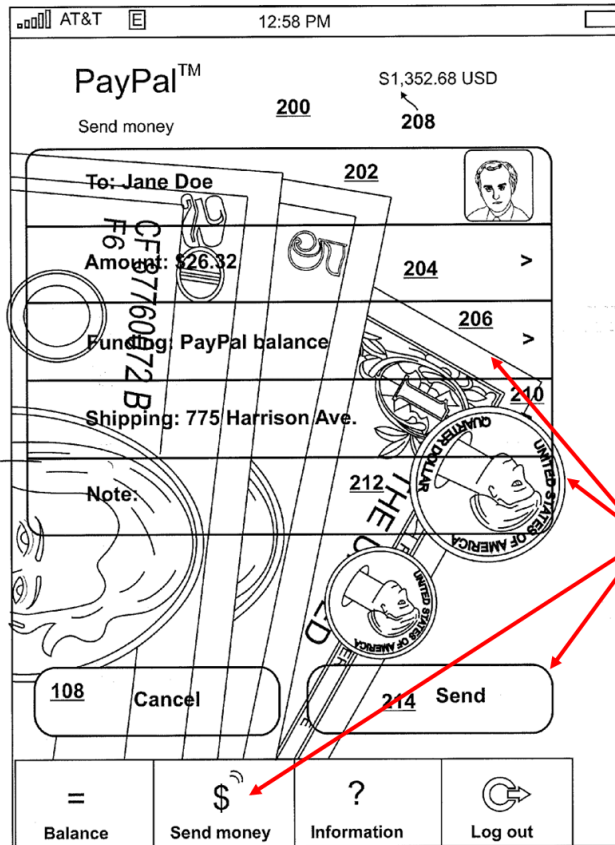


FIG. 2
APPL-1008, FIG. 2, annotated

Second, each transaction icon above discloses graphical representation of money, e.g., “\$ Send money” includes “\$;” the virtual currency icon include a group of one, five, and 20 dollar bills and coins. APPL-1003, ¶155. Furthermore, a POSITA would have been motivated to implement “Send” 214 of FIG. 2 and other transaction icons (e.g., “Send,” “Confirm,” “Proceed” as discussed at [1.5] for transferring funds) with a graphical representation of money (e.g., “\$”) for richer visual representaion.

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

8. Claim 7

[7.0] The system of claim 1 wherein the virtual likeness of the face of the recipient comprises a photograph of the recipient.

Stone discloses or renders obvious this element and claim for reasons discussed at [1.3]. APPL-1003, ¶98 (a POSITA would have understood Stone’s disclosure of “**photograph image**” as a user attribute applies to both user device and recipient device, which would be used as recipient icon, citing APPL-1008, [0045], [0046]); ¶157.

9. Claim 8

[8.0] The system of claim 1 wherein the virtual likeness of the face of the recipient comprises an avatar of the recipient.

Stone renders obvious this element. APPL-1003, ¶¶158-161.

First, Stone discloses “a recipient icon on the display, such as a picture of the recipient.” APPL-1008, [0036].

Second, Stone combined with a POSITA’s knowledge that avatar is a well-known alternative of a picture for a user icon renders this element obvious. APPL-1003, ¶160. Specifically, in Stone, a POSITA would have been motivated to provide the option to use an avatar as a recipient icon, because avatar was a well-known alternative design choice of pictures for user icon (regardless of whether it is for recipient or sender), where avatar has the benefits of providing an online identity that balances personal expression and privacy, and user picture has the benefits of enhanced personal recognition and trust. APPL-1003, ¶106 (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)). Accordingly, a POSITA would have been motivated to provide the option to use an avatar as a recipient icon in Stone for the benefits of flexibility and user options (regardless of recipient or sender) to use a picture or avatar as profile icon based on the individual needs.

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

10.Claim 9

[9.0] The system of claim 1 wherein a password is not required to initiate the electronic transaction.

Stone or Stone-Hoyos-Varghese renders obvious this element. APPL-1003, ¶¶162-167.

First, Sone describes initiating the electronic transaction, e.g., clicking on “\$Send money” of FIG. 2 without requiring a password. APPL-1003, ¶163.

Second, to the extent that Patent Owner argues that Stone (alone or in combination with Hoyos and Varghese) performs an authentication requiring a password (e.g., for login to view the interface of FIG. 2) to initiate the transaction, or does not explicitly describe that a password is not required to initiate the electronic transaction, it was well-known that a password is one of many alternative authentication techniques (e.g., biometrics, location, non-password based tokens). APPL-1003, ¶¶164-165 (citing APPL-1022, [0063] (biometric

verification “may be employed in addition to or **as an alternative** to passwords”); APPL-1037, 10; APPL-1016, [0036], [0044]). As such, a POSITA would have been motivated to implement a login authentication, even if it were required to initiate a transaction, using other authentication techniques (e.g., biometrics) without requiring a password based on design needs, because biometrics and password are known alternative authentication techniques and password is known to be vulnerable to brute force attacks or phishing and prone to being forgotten. APPL-1003, ¶165.

Third, in Stone-Hoyos-Varghese, the multifactor real-time transaction authentication does not affect Stone’s teaching that “a password is not required to initiate the electronic transaction” as claimed, because the transaction authentication (1) does **not** require a password, and (2) is performed **after** the transaction is initiated, as discussed above at [1.5]-[1.8]. APPL-1003, ¶166.

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

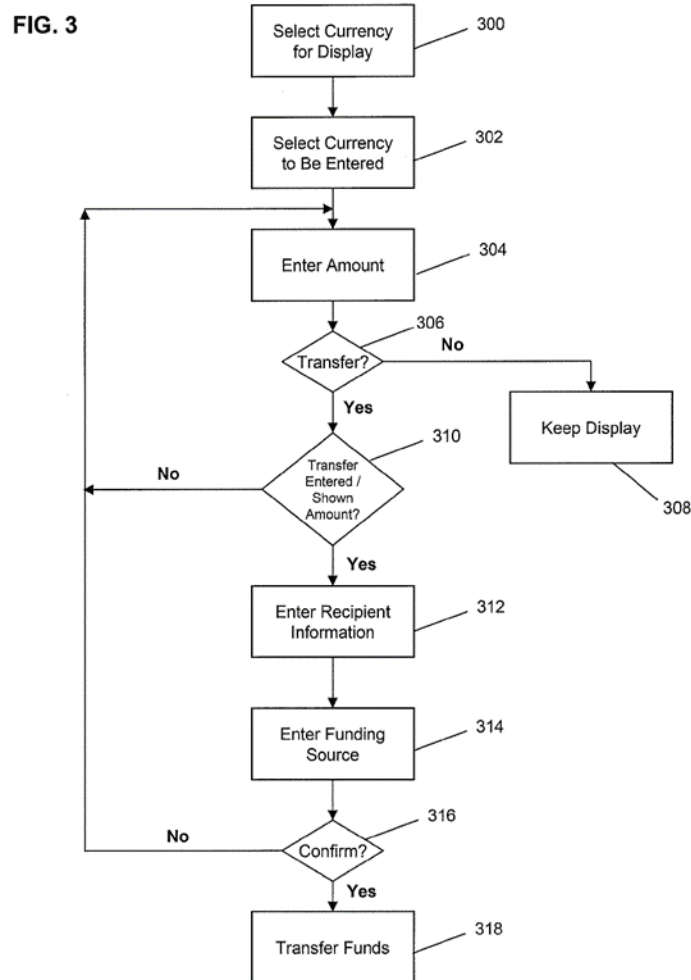
11. Claim 10

[10.0] A method, comprising:

Stone discloses or renders obvious the preamble to the extent that it is limiting. APPL-1003, ¶¶168-170.

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),

continuation confirmation steps (e.g., steps 306 and 316), and fund transfer step (step 318).



APPL-1008, FIG. 3

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

[10.1]-[10.4]

Stone alone or Stone-Hoyos-Varghese renders obvious these elements for reasons discussed at [1.2]-[1.5]. APPL-1003, ¶¶171-174.

[10.5]

Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [1.6]. APPL-1003, ¶¶175.

[10.6.1]

Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [1.1] and [1.7.1]. APPL-1003, ¶176.

[10.6.2]-[10.7]

Stone-Hoyos-Varghese renders obvious these elements for reasons discussed at [1.7.2]-[1.8]. APPL-1003, ¶¶177-179. Accordingly, Stone-Hoyos-Varghese renders obvious this claim.

12.Claims 13, 14, 15, 16, and 17

Stone discloses or renders obvious the elements of these claims for reasons discussed at Ground 1: Claims 4, 5, 6, 7, and 8 respectively. APPL-1003, ¶¶180-184. Accordingly, Stone-Hoyos-Varghese renders obvious these claims.

13.Claim 18

Stone-Hoyos-Varghese renders obvious this claim for reasons discussed at Ground 1: Claim 9. APPL-1003, ¶¶185.

14.Claim 19

[19.0] 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, ¶¶186-188.

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, ¶187; *see also* [1.0], [1.1], and [1.9].

Therefore, Stone discloses or renders obvious this element.

[19.1]

Stone alone or Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [1.2]. APPL-1003, ¶189.

[19.2]- [19.4]

Stone discloses or renders obvious these elements for reasons discussed at [1.3]-[1.6]. APPL-1003, ¶¶190-192.

[19.5]

Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [1.6]. APPL-1003, ¶193.

[19.6.1]

Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [1.1] and [1.7.1]. APPL-1003, ¶194.

[19.6.2]-[19.7]

Stone-Hoyos-Varghese renders obvious these elements for reasons discussed at [1.7.2]-[1.8]. APPL-1003, ¶¶195-197. Accordingly, Stone-Hoyos-Varghese renders obvious claim 19.

C. Ground 2: Claims 1, 4-10, and 13-19 are Rendered Obvious under §103(a) over Stone in view of FFIEC Guidance.

Ground 2 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 2 is substantially similar to the analysis of Stone as applied in Ground 1. APPL-1003, ¶198.

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, and the additional benefits of FFIEC compliance for federal supervised financial institutions. APPL-1003, ¶199.

First, as discussed at IX.A.5, Guidance is analogous art to the ’656 patent. APPL-1003, ¶200.

Second, Guidance addresses “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 whether or not regulated by FFIEC. APPL-1003, ¶201; 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), and because the Guidance was a recognized driver for implementing multi-factor authentication by a POSITA as shown in numerous articles and patent disclosures. APPL-1003, ¶201 (citing APPL-1013, [0009], [0011]; APPL-1010, [0148]; APPL-1016, FIG. 3, [0073]); APPL-1003, ¶50 (citing US 8,776,176 by Oracle, 17:61-67; US 8,239,677 by Equifax, 1:62-66; US 8,032,932 by Citibank, 1:6-9).

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, ¶202 (citing APPL-1039, 1; APPL-1008, [0041]-[0042] (describing user devices implemented with any appropriate computing devices (e.g., personal computer, wireless telephone, etc.))).

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, ¶203.

[1.1] a processor configured to:

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

¶¶204-208.

First, as discussed at Ground 1:[1.1], Stone discloses or renders this element obvious.

Second, to the extent that Patent Owner argues that “*a processor*” requires a **single** processor (contradictory to its own definition of “processor”), Stone alone or Stone-Guidance renders it obvious. APPL-1003, ¶206.

Specifically, as discussed at IX.C.1, a POSITA would have been motivated to implement various steps for initiating, authenticating and completing an electronic transaction (e.g., steps of [1.2]-[1.8] discussed below) **locally** (e.g., on the user device of Stone) or remotely (e.g., on the service provider of Stone). For example, a POSITA would have been motivated to implement the authentication steps locally for the benefits including reduced latency, offline analysis capabilities, enhanced privacy, efficient resource utilization, customization for device characteristics, improved security. APPL-1003, ¶207(citing APPL-1015, FIG. 3, 4:4-10; APPL-1016, [0040], [0042], APPL-1038, 64). As such, to the extent that Patent Owner argues that “*a processor*” requires a **single** processor, Stone alone or Stone-Guidance renders obvious using a single processor of the user device to perform the processes discussed at [1.2]-[1.8] below.

Therefore, Stone alone or Stone-Guidance renders obvious “*a processor*” configured to perform the processes as claimed.

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

Stone alone or Stone-Guidance renders obvious these elements. APPL-1003, ¶¶209-212.

First, Stone alone renders obvious these elements as discussed at Ground 1:[1.2].

Second, to the extent that Patent Owner argues that Stone’s “biometric id” does not explicitly describe using it for comparison in biometric authentication, Guidance, as applied in the combination, explicitly describes receiving and storing biometric information during enrollment, which is used later for comparison with biometric data captured using of a live scan. APPL-1003, ¶211 (citing APPL-1037, 11 (“The systems capture facial images from video cameras and generate templates that are stored and used for comparisons.”), 9-10).

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

[1.3]-[1.5]

Stone discloses or renders obvious these elements for the reasons discussed at Ground 1:[1.3]-[1.5]. APPL-1003, ¶¶209-212.

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

Stone-Guidance renders this element obvious. APPL-1003, ¶¶216-222.

First, Guidance describes multifactor real-time authentication for financial transactions, which uses a combination of authentication techniques of different factors including physical location authentication (“Something a person has”/“something you have”), along with biometric authenticating including face recognition (“Something a person is”/“something you are”) with testing for liveness, based on the risk of the transaction. APPL-1037, 3, 11-12; APPL-1003, ¶217 (citing APPL-1010, [0035]).

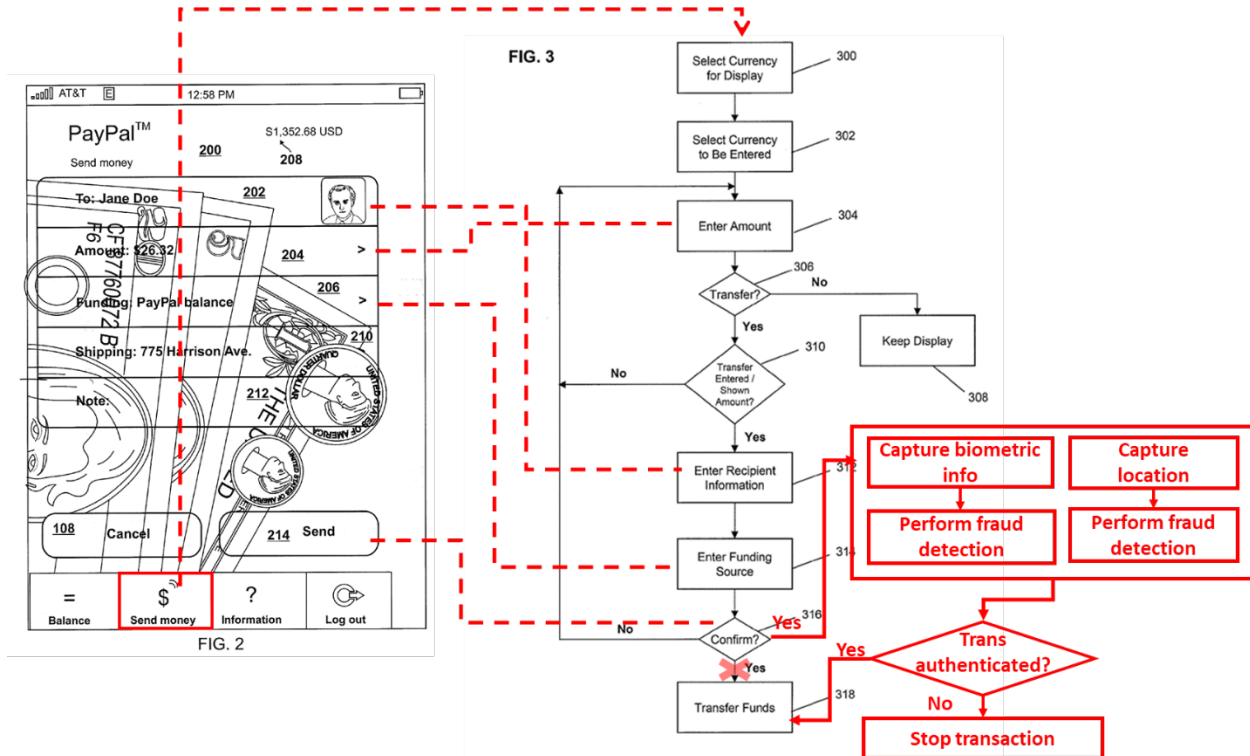
Guidance describes selecting from the various authentication techniques based on risk assessment of the transaction request, and a POSITA would have been motivated to perform transaction authentication for a transaction request using a combination of physical location authentication and biometrics authentication using facial recognition with liveness test. Specifically, physical location authentication would be selected 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, ¶218 (citing APPL-1010, [0012], [0035]; APPL-1016, [0043]). Furthermore, biometric authentication using facial recognition with liveness test would be selected along with the physical location authentication for the benefits of contactless and hygienic authentication using easy to acquire (e.g., using a

camera) facial images and spoof-proofing. APPL-1003, ¶218 (citing APPL-1013, [0007]; APPL-1037, 11).

The multifactor real-time risk-based authentication (using a combination of physical location authentication and biometrics authentication using facial recognition with liveness test) of Guidance teaches capturing real-time biometric information associated with the electronic transaction for biometric authentication, and capturing real-time location associated with the user. APPL-1037, 9-11 (capturing biometric information associated with the user using “live-scan process of the biometrics technology”), 12 (capturing and analyzing location data associated with the user including “IPA location” and “geo-location” “in a real-time environment”); APPL-1003, ¶219.

Second, as shown in example Stone-Guidance below, a POSITA would have been motivated to implement Guidance’s multifactor real-time authentication for transaction authentication (including the capturing the contextual information and fraud/authentication analysis based thereupon) “subsequent to receiving the indication of the action taken by the user” (e.g., after a user confirms a transaction request at 316, thereby subsequent to user interaction with any of the transaction icons associated with “\$Send money,” 202, 206, 214, personalized currency, 300, 302, 306, 312, 314, and 316) as claimed, for the benefit of providing real-time risk-based authentication for fraud analysis. APPL-1003, ¶220 (citing 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)

A POSITA would have been motivated to implement the multifactor real-time authentication as taught by Guidance (including capturing the contextual data including biometric data and location data and fraud analysis thereafter) 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., 300-

314) and confirm (e.g., 316) the transaction request. for the benefits of risk-based contextual authentication adaptive for the specific transaction based on transaction information, and more accurate real-time information for real-time authentication. APPL-1003, ¶221; APPL-1010, FIG. 14, [0091], [0097]-[0099], [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; *see also* IX.B.2-3; IX.C.1.

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, 300, 302, 306, 312, 314, and 316), contextual information comprising biometric information (e.g., facial images by video cameras for liveness detection) and location data associated with the user are captured as taught in Guidance, which renders obvious this element.

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

Stone-Guidance renders this element obvious. APPL-1003, ¶¶223-225.

Specifically, Guidance describes performing a fraud detection analysis of the captured contextual information, describing various techniques for fraud detection analysis where “selection and use of any technique should be based upon the assessed risk.” APPL-1003, ¶224; APPL-1037, 7, 9-10 (describing “Biometrics”

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” for fraud analysis and customer authentication), 12 (describing “Internet Protocol Address (IPA) Location and Geo-Location” technologies with fraud detection analysis of the captured location data, where “software analyzes [IP Intelligence including “**location**”] in a real-time environment and checks it against multiple data sources and profiles to prevent unauthorized access,” including detection of “out-of-character details of the access attempt”); *see also* detailed discussion at [1.7.2] and [1.7.3].

Accordingly, Stone-Guidance renders obvious this element.

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

Stone-Guidance renders this element obvious. APPL-1003, ¶¶226-228.

Specifically, Guidance describes, for biometric authentication as applied in Stone, the basic knowledge of performing a comparison based on the stored biometric information and the captured biometric information. APPL-1037, 9 (“The results of a live scan, such as a fingerprint, are compared with the registered templates stored in the system”), 10-11 (“The systems capture facial images from video cameras and generate templates that are stored and used **for comparisons.**”); APPL-1003, ¶227.

Accordingly, in Stone-Guidance, the fraud detection analysis includes comparing live scan biometric results with the registered stored sample, which renders obvious this element.

[1.7.3] 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, ¶¶229-232.

Specifically, Guidance describes that biometric authentication as applied in Stone, includes face recognition that uses facial images from “video cameras” with “tests for **liveness**, such as blinking eyes.” APPL-1037, 11. Techniques for liveness tests based on facial images from video cameras were wellknown. APPL-1003, ¶230 (citing APPL-1044).

A POSITA would have been motivated to apply the liveness test in the multifactor real-time authentication as applied in Stone-Guidance because “[t]esting for liveness reduces the chance that the person requesting access is using a photograph of an authorized individual.” APPL-1037, 11; APPL-1003, ¶231.

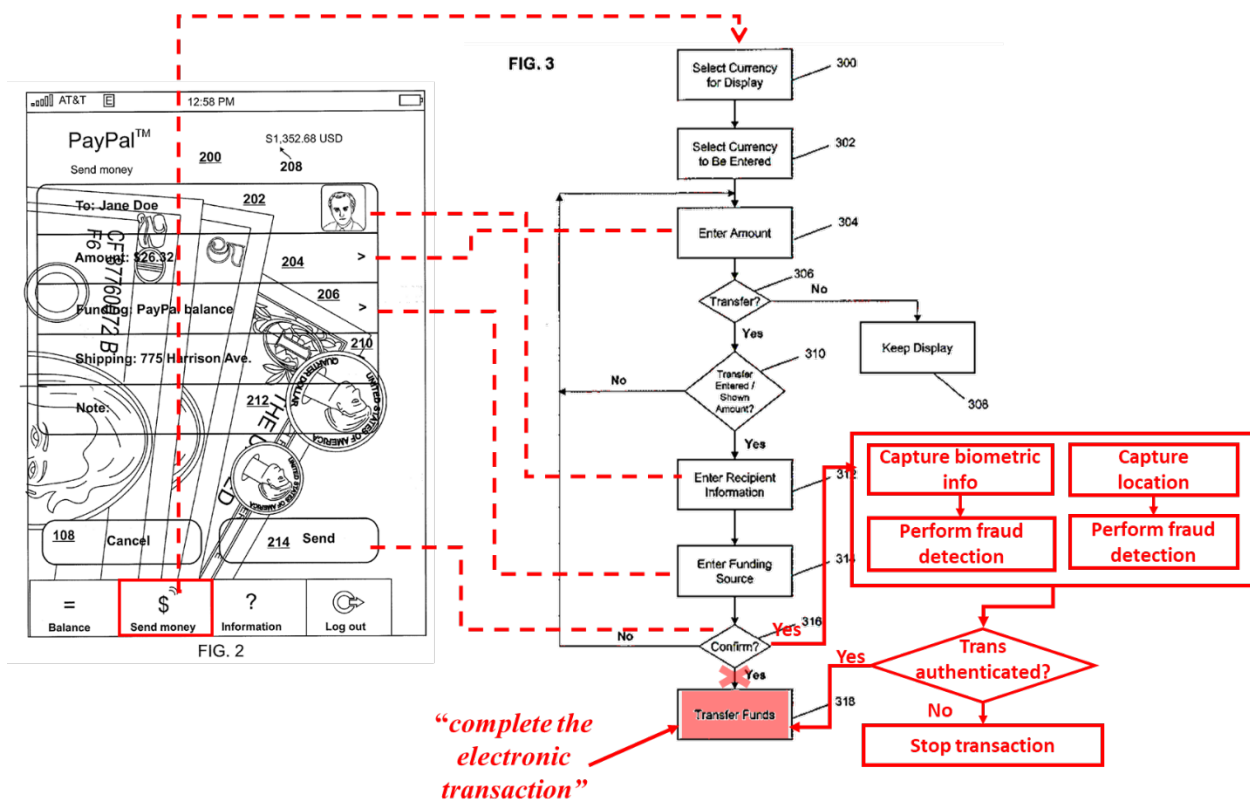
Accordingly, Stone-Guidance renders obvious this element.

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

Stone-Guidance renders this element obvious. APPL-1003, ¶¶233-236.

Stone-Guidance teaches completing the electronic transaction (e.g., performing transferring funds at 318 of FIG. 3 of Stone) based at least in part on

both the user interaction with the transaction icon (see [1.6]) and performing the fraud detection analysis (see [1.7.1]-[1.7.3]), because the user interaction is the user's indication of continuing/confirming the transaction request, and the transaction request is authorized based on the fraud detection analysis, as well-known in the art. APPL-1003, ¶¶234-235 (citing APPL-1008, [0035], APPL-1037, 12; parent patent 9,972,010, claim 23).



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 processor and configured to provide the processor with instructions.

Stone discloses or at least renders obvious this element for reasons discussed at Ground 1:[1.9]; and Stone-Guidance renders obvious claim 1 in its entirety. APPL-1003, ¶237.

3. Claims 4, 5, 6, 7, 8

Stone renders obvious the elements of these claims for the reasons discussed at Ground 1: Claims 4, 5, 6, 7, and 8 respectively. APPL-1003, ¶¶238-242.

Accordingly, Stone-Guidance renders obvious these claims.

4. Claim 9

[9.0] The system of claim 1 wherein a password is not required to initiate the electronic transaction.

Stone alone or Stone-Guidance renders obvious this element. APPL-1003, ¶¶243-246.

First, Stone renders obvious this element as discussed at Ground 1:[9.0].

Second, in Stone-Guidance, similar to Stone-Hoyos-Varghese, the multifactor real-time transaction authentication does not affect Stone's teaching that "a password is not required to initiate the electronic transaction" as claimed, because the transaction authentication (1) does **not** require a password, and (2) is performed **after** the transaction is initiated, as discussed above at Ground 2:[1.5]-[1.8]. APPL-1003, ¶245.

Accordingly, Stone-Guidance renders obvious this claim.

5. Claim 10

[10.0]

Stone discloses or renders obvious the preamble to the extent that it is limiting for the reasons discussed at Ground 1:[10.0]. APPL-1003, ¶247.

[10.1]-[10.4]

Stone alone or Stone-Guidance renders obvious these elements for the reasons discussed at Ground 2:[1.2]-[1.5]. APPL-1003, ¶¶248-251.

[10.5]

Stone-Guidance renders obvious this element for reasons discussed at Ground 2:[1.6]. APPL-1003, ¶252.

[10.6.1]

Stone-Guidance renders obvious this element for reasons discussed at Ground 2:[1.1] and [1.7.1]. APPL-1003, ¶253.

[10.6.2]-[10.7]

Stone-Guidance renders obvious these elements for reasons discussed at [1.7.2]-[1.8]. APPL-1003, ¶¶254-256. Accordingly, Stone-Guidance renders obvious claim 10.

6. Claims 13, 14, 15, 16, and 17

Stone renders obvious the elements of these claims for reasons discussed at Ground 2: Claims 4, 5, 6, 7, and 8. APPL-1003, ¶¶257-261. Accordingly, Stone-Guidance renders obvious these claims.

7. Claim 18

Stone-Guidance renders obvious this claim for reasons discussed at Ground 2: Claim 9. APPL-1003, ¶¶262.

8. Claim 19

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

To the extent that the preamble is limiting, Stone alone or in view of Guidance renders it obvious for reasons discussed at Ground 2:[1.0]-[1.1], and [1.9]. APPL-1003, ¶263.

[19.1]

Stone alone or Stone-Guidance renders obvious this element for reasons discussed at Ground 2:[1.2]. APPL-1003, ¶264.

[19.2]-[19.4]

Stone discloses or renders obvious these elements for reasons discussed at Ground 2:[1.2]-[1.5]. APPL-1003, ¶¶264-267.

[19.5]

Stone-Guidance renders obvious this element for reasons discussed at Ground 2:[1.6]. APPL-1003, ¶268.

[19.6.1]

Stone-Guidance renders obvious this element for reasons discussed at Ground 2:[1.1] and [1.7.1]. APPL-1003, ¶269.

[19.6.2]-[19.7]

Stone-Guidance renders obvious these elements for reasons discussed at

Ground 2:[1.7.2]-[1.8]. APPL-1003, ¶¶270-272. Accordingly, Stone-Guidance renders obvious claim 19.

D. Grounds 3 and 4: Combination of Stone, Hoyos, Varghese, and Borovsky (Ground 3, “Stone-Hoyos-Varghese-Borovsky”) and Combination of Stone, Guidance, and Borovsky (Ground 4, “Stone-Guidance-Borovsky”) render obvious Claims 2-3 and 11-12.

The claim analysis for Grounds 3 and 4 rely on the same analysis and evidence as provided for Ground 1 (Stone-Hoyos-Varghese) and Ground 2 (Stone-Guidance), respectively, except for where additional analysis is provided, as noted for respective limitations of the claims below. The additional analysis provided below applies for both Grounds 3 and 4. APPL-1003, ¶273.

1. Borovsky

Borovsky is directed at a system using a management system to “update configuration information for the mobile device” and “send the **configuration information** to the mobile device for **configuring the mobile device.**” APPL-1041, Title, Abstract, Claim 1. APPL-1003, ¶274.

As shown in FIG. 6 of Borovsky below, Borovsky describes obtaining “**photos corresponding to contacts of the user**” from “**social networking**” sites (e.g., “myspaceTM, facebookTM, twitterTM”), and sending these obtained photos, together with other configuration information to a client device “be displayed with a particular contact.” APPL-1041, claims 3-7; [0035], [0039], [0043], [0045], [0046], FIGS. 5, 6; APPL-1003, ¶275.

*“obtain the virtual likeness of
the face” of contacts
“from a social networking site”*

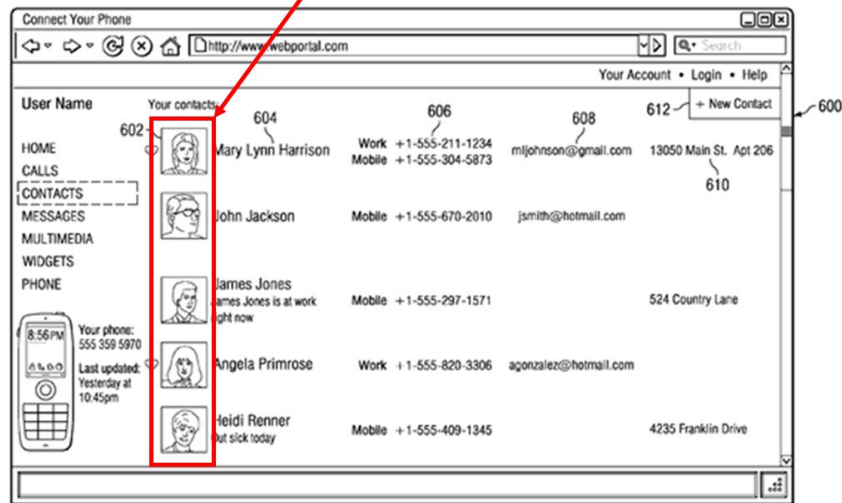


FIG. 6

APPL-1041, FIG. 6

2. Reasons to Combine Stone and Borovsky

A POSITA would have been motivated to apply in Stone, Borovsky’ s teaching of updating contact display on a user device with a photo from social networks, for the benefits of enhanced user experience with helpful visuals, increased transaction confidence (e.g., providing reassurance by seeing a recognizable photo), and efficient identification (e.g., easier identification of a recipient, esp. with common names). APPL-1003, ¶¶276-279 (citing APPL-1042, 1; APPL-1036, [0002]).

First, Borovsky is analogous art to the ’656 patent, because it is at least (1) in the same field of endeavor (computer network applications using a server-client system); or (2) reasonably pertinent to a problem with which the inventor of the

'656 patent was involved (e.g., improving display/identification of other users on a user device). APPL-1041, claims 1, 3, 6, 7; APPL-1003, ¶277.

Second, Stone has the need to obtain for display on the user device, pictures of other users connected to a network with the user. APPL-1003, ¶278 (citing APPL-1008, [0020], [0036]). Facing the need of Stone, a POSITA would have been motivated apply Borovsky's teaching of providing contact photo obtained from social network sites for user device contact display as icons for network-connected users on user device, especially in the case that the other user did not profile a profile icon, for the benefits of enhanced user experience with helpful visuals, increased transaction confidence and efficient identification. APPL-1003, ¶278 (It was well-known that profile images "can be created using a digital camera function of mobile device 504 or **downloaded from various servers** over a communications network," citing APPL-1009, 15:20-25; APPL-1042, 1 (well-known applications to synchronize contact information including contact images with social network servers)).

Third, while Borovsky describes "particular embodiments" where "the mobile device is a mobile phone having a simple and elegant user interface and, in particular example embodiments, a relatively limited display and means for providing input relative to a typical remote computer," a POSITA would have understood that such examples are "by way of example and not by way of

limitation,” and Borovsky’s teachings apply to various types of mobile devices including smart phones. APPL-1041, [0013]; APPL-1003, ¶279 (explaining the well-known need for synchronizing client device contacts with social networks applies to general mobile phones and mobile applications, citing APPL-1042, 1). Furthermore, Stone describes user devices implemented with any appropriate computing devices (e.g., personal computer, wireless telephone, etc.) with wired and/or wireless communication over network, and therefore, is not limited to any specific types of user devices. APPL-1008, [0041]-[0042]. Accordingly, a POSITA would have reasonably expected to succeed in configuring Stone to implement Borovsky’s teaching, 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, ¶279 (citing APPL-1042, 3-4; APPL-1009, 15:20-25).

3. Claims 2 and 11

[2.0/11.0] The system of claim 1/method of claim 10 wherein the processor is further configured to obtain the virtual likeness of the face of the recipient from a social networking site.

Stone-Borovsky renders obvious this element. APPL-1003, ¶¶280-283.

First, Borovsky describes obtaining photos of contacts from a social networking site. APPL-1003, ¶281. Specifically, as shown in FIG. 6 of Borovsky below, Borovsky describes collecting “**photos corresponding to contacts of the user**” from “**social networking**” sites and providing these photos, together with other configuration information to a client device “displayed with a particular

contact.” APPL-1041, claims 3-7; [0035], [0039], [0043], [0045], [0046] (“any and all of the afore mentioned aggregated contact information is pushed **to the mobile device 108 for display** and access via the mobile device 108”), FIGS. 5-6.

*“obtain the virtual likeness of
the face” of contacts
“from a social networking site”*

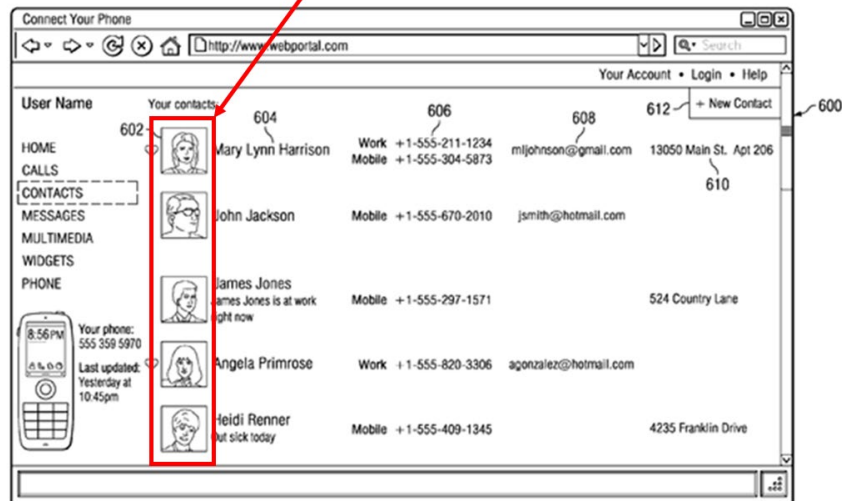


FIG. 6

APPL-1041, FIG. 6, annotated

Second, a POSITA would have understood that Stone has the need to obtain for display on the user device, pictures of other users connected to a network with the user. APPL-1003, ¶282 (citing APPL-1008, [0020], [0036]). As such, a POSITA would have been motivated to apply Borovsky’s teaching of providing contact photo obtained from social network sites as contact icons in user device in Stone, for the benefits of providing updated contact icon display on a user device for enhanced user experience and increased transaction confidence. APPL-1003, ¶282 (citing APPL-1009,15:20-25, APPL-1042, 1); IX.D.2.

Accordingly, Stone-Hoyos-Varghese-Borovsky and Stone-Guidance-

Borovsky each render obvious these claims.

4. Claims 3 and 12

[3.0/12.0] The system of claim 2/method of claim 11 wherein obtaining the virtual likeness of the face of the recipient from the social networking site comprises scraping the social networking site for the virtual likeness of the face of the recipient.

Stone-Borovsky renders obvious this element. APPL-1003, ¶¶284-287.

It was well-known that scraping was a basic technique for collecting information including contact photos from social network sites, e.g., as an alternative when no API level access was available. APPL-1003, ¶285 (citing APPL-1046, [0026], [0031]-[0033]; APPL-1045, 174; APPL-1043, 4:42-49).

In view of POSITA's fundamental and basic knowledge of scraping social network sites for collecting contact profile information including photos, a POSITA would have been motivated to apply scraping the social networking site to obtain the photo of the recipient in Stone-Borovsky. APPL-1003, ¶286.

Accordingly, Stone-Hoyos-Varghese-Borovsky and Stone-Guidance-Borovsky each render obvious these claims.

X. DISCRETIONARY DENIAL IS NOT WARRANTED

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

A. The *Fintiv*³ 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 '656 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

³ 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 2-3, 5-6, 11-12, 14-15, 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).

Related to the first prong of *Advanced Bionics*, none of the applied references were presented to the Office. The Examiner did not consider Stone, Hoyos, Varghese, Guidance, or Borovsky during the prosecution. Moreover, they are non-cumulative, because they teach the amended features resulting in the notice of allowance (APPL-1002, 99), as discussed at Section IX above.

XI. CONCLUSION

Petitioner has established a reasonable likelihood that Challenged Claims of the '656 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 and III–XI) has 13108 (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-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