

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

CARBYNE BIOMETRICS, LLC,

Patent Owner

IPR2024-00331

U.S. Patent No. 11,526,886

**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 '886 PATENT.....	2
	A. Summary of the '886 patent.....	2
	B. Prosecution History	3
V.	LEVEL OF ORDINARY SKILL IN THE ART.....	4
VI.	CLAIM CONSTRUCTION	4
VII.	REQUESTED RELIEF.....	5
VIII.	OVERVIEW OF CHALLENGES	5
	A. Challenged Claims	5
	B. Statutory Grounds for Challenges.....	5
IX.	IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE....	6
	A. Overview of Prior Art.....	6
	1. Stone.....	6
	2. Hoyos	8
	3. Varghese.....	10
	4. FFIEC Guidance (or “Guidance”)	11
	5. Campbell	12
	6. Analogous Art.....	13
	B. Ground 1: Claims 1-12, 14-18, and 20-23 are Rendered Obvious under §103(a) over Stone in view of Hoyos and Varghese.	14
	1. Combination of Disclosures/Embodiments of Stone.....	14
	2. Combination of Stone and Hoyos (“Stone-Hoyos”).....	16

3.	Combination of Stone, Hoyos, and Varghese.....	21
4.	Claim 1	23
5.	Claim 2	54
6.	Claim 3	55
7.	Claim 4	58
8.	Claim 5	59
9.	Claim 6	60
10.	Claims 7, 8, 9, 10	62
11.	Claim 11	62
12.	Claims 12 and 18.....	63
13.	Claims 14 and 20.....	64
14.	Claims 15 and 21.....	65
15.	Claims 16 and 22.....	66
16.	Claims 17 and 23.....	66
C.	Ground 2: Claims 1-12, 14-18, and 20-23 are Rendered Obvious under §103(a) over Stone-Guidance.	67
1.	Combination of Stone and FFIEC Guidance (“Stone- Guidance”)	68
2.	Claim 1	70
3.	Claims 2-3	81
4.	Claim 4	81
5.	Claim 5	82
6.	Claim 6	83
7.	Claims 7, 8, 9, 10	83
8.	Claim 11	83
9.	Claims 12 and 18.....	84
10.	Claims 14 and 20.....	84
11.	Claims 15 and 21.....	85
12.	Claims 16 and 22.....	86

13.	Claims 17 and 23.....	86
D.	Grounds 3 and 4: Combination of Stone, Hoyos, Varghese, and Campbell (Ground 3) and Combination of Stone, Guidance, and Campbell (Ground 4) Render Obvious Claims 15-17 and 21-23.	87
1.	Combination of Campbell with each of Grounds 1 and 2	87
2.	Claims 15 and 21.....	88
3.	Claims 16 and 22.....	89
4.	Claims 17 and 23.....	90
X.	DISCRETIONARY DENIAL IS NOT WARRANTED	91
A.	The <i>Fintiv</i> factors favor institution.	91
B.	<i>Advanced Bionics</i> Test Favors Institution.....	94
XI.	CONCLUSION.....	94
XII.	CERTIFICATE OF WORD COUNT	95
	CERTIFICATE OF SERVICE	96

PETITIONER’S EXHIBIT LIST

January 30, 2024

APPL-1001	U.S. Patent No. 11,526,886 to Jakobsson (“’886 patent”)
APPL-1002	Prosecution File History of U.S. App. No. 16/893,237 (issued as ’886 patent) (“’237 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	Prosecution File History of U.S. App. 15/948,744 (issued as U.S. Patent No. 10,713,656) (“’744 App”)
APPL-1031	U.S. Patent No. 8,160,877 to Nucci et al. (“Nucci”)
APPL-1032	U.S. Patent No. 7,516,074 to Bilobrov (“Bilobrov”)
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) (“FFIEC Guidance” or “Guidance”)
APPL-1038	Bhargav-Spantzel a 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- APPL-1043	RESERVED
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- APPL-1046	RESERVED
APPL-1047	Vasalou et al., “Avatars in Social Media: Balancing Accuracy, Playfulness and Embodied Messages,” International Journal of Human-Computer Studies Volume 66, Issue 11, November 2008, Pages 801-811 (“Vasalou”)

Listing of Challenged Claims

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

	on an analysis of the set of images captured using the camera; and
[1.5]	a memory coupled to the one or more processors and configured to provide the processor with instructions.
Claim 2	
[2.0]	The system recited in claim 1, wherein the account holder comprises a recipient of the electronic transaction, and wherein the electronic transaction comprises a payment from the user to the account holder.
Claim 3	
[3.0]	The system recited in claim 1, wherein the icon represents a form of payment.
Claim 4	
[4.0]	The system recited in claim 1, wherein the image comprises at least one of a photograph or an avatar.
Claim 5	
[5.0]	The system recited in claim 1, wherein the one or more interfaces are associated with at least one of a phone, a tablet device, or a laptop.
Claim 6	
[6.0]	A method, comprising:
[6.1.1]	rendering, in one or more interfaces, a virtual likeness of a face associated with an account holder,
[6.1.2]	wherein the virtual likeness of the face was selected by the account holder as part of an enrollment;
[6.2.1]	subsequent to an interaction by a user with an icon rendered in the one or more interfaces: capturing contextual information comprising location data usable to determine a physical location

	associated with the user; and
[6.2.2]	[subsequent to an interaction by a user with an icon rendered in the one or more interfaces:...] capturing a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images; and
[6.3.1]	facilitating a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed based at least in part on: the physical location associated with the user determined using the captured location data; and
[6.3.2]	[facilitating a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed based at least in part on:...] an analysis of the set of captured biometric information comprising a determination of whether the user is alive based at least in part on an analysis of the set of images captured using the camera.
Claim 7	
[7.0]	The method of claim 6, wherein the account holder comprises a recipient of the electronic transaction, and wherein the electronic transaction comprises a payment from the user to the account holder.
Claim 8	
[8.0]	The method of claim 6, wherein the icon represents a form of payment.
Claim 9	
[9.0]	The method of claim 6, wherein the image comprises at least one

	of a photograph or an avatar.
Claim 10	
[10.0]	The method of claim 6, wherein the one or more interfaces are associated with at least one of a phone, a tablet device, or a laptop.
Claim 11	
[11.0]	11. A computer program product embodied in a non-transitory computer readable storage medium and comprising computer instructions for:
[11.1.1]	rendering, in one or more interfaces, a virtual likeness of a face associated with an account holder,
[11.1.2]	wherein the virtual likeness of the face was selected by the account holder as part of an enrollment;
[11.2.1]	subsequent to an interaction by a user with an icon rendered in the one or more interfaces: capturing contextual information comprising location data usable to determine a physical location associated with the user; and
[11.2.2]	[subsequent to an interaction by a user with an icon rendered in the one or more interfaces:...] capturing a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images; and
[11.3.1]	facilitating a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed based at least in part on: the physical location associated with the user determined using the captured location data; and
[11.3.2]	[facilitating a fraud detection analysis to determine whether to

	allow an electronic transaction associated with the account holder to proceed based at least in part on:... an analysis of the set of captured biometric information comprising a determination of whether the user is alive based at least in part on an analysis of the set of images captured using the camera.
Claim 12	
[12.0]	The system recited in claim 1, wherein the analysis of the set of images captured using the camera further comprises determining whether a face is detected in the captured set of images.
Claim 14	
[14.0]	The system recited in claim 1, wherein the set of images comprises a plurality of images successively captured using the camera.
Claim 15	
[15.0]	The system recited in claim 1, wherein the set of captured biometric information further comprises an audio sample.
Claim 16	
[16.0]	The system recited in claim 15, wherein facilitating the fraud detection analysis to determine whether the electronic transaction associated with the account holder is allowed to proceed is further based at least in part on a determination of whether the audio sample matches a previously recorded voice sample.
Claim 17	
[17.0]	The system recited in claim 16, wherein the determination of whether the audio sample matches the previously recorded voice sample is based at least in part on performing a Fast Fourier Transform.
Claim 18	

[18.0]	The method of claim 6, wherein the analysis of the set of images captured using the camera further comprises determining whether a face is detected in the captured set of images.
Claim 20	
[20.0]	The method of claim 6, wherein the set of images comprises a plurality of images successively captured using the camera.
Claim 21	
[21.0]	The method of claim 6, wherein the set of captured biometric information further comprises an audio sample.
Claim 22	
[22.0]	The method of claim 21, wherein facilitating the fraud detection analysis to determine whether the electronic transaction associated with the account holder is allowed to proceed is further based at least in part on a determination of whether the audio sample matches a previously recorded voice sample.
Claim 23	
[23.0]	The method of claim 22, wherein the determination of whether the audio sample matches the previously recorded voice sample is based at least in part on performing a Fast Fourier Transform.

I. INTRODUCTION

U.S. Patent No. 11,526,886 (the “’886 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 1-12, 14-18, and 20-23 (“Challenged Claims”) of the ’886 patent.

II. MANDATORY NOTICES

A. Real Party-in-Interest

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

B. Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), the ’886 patent is or was involved in the following cases, which may affect, or be affected by, this proceeding:

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

Apple is not aware of any disclaimers, reexamination certificates, or IPR petitions addressing the ’886 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 '886 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 '886 PATENT

A. Summary of the '886 patent

The '886 patent is directed at electronic transactions, and specifically financial transaction systems. APPL-1001, Abstract. APPL-1003, ¶¶28-33.

As shown in FIG. 7 below, the '886 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.

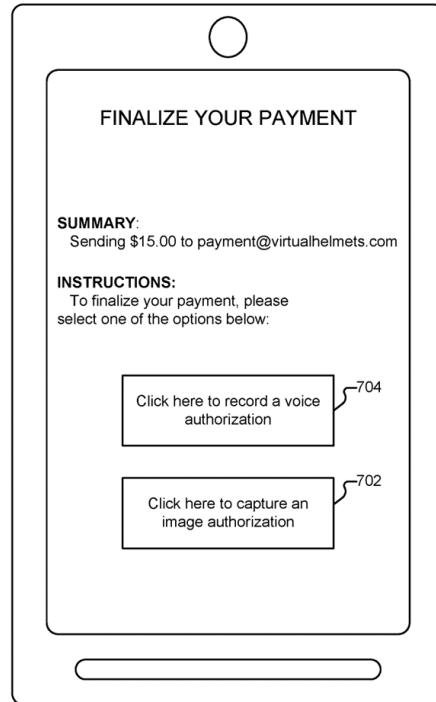


FIG. 7

APPL-1001, FIG. 7

Specifically, the '886 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, 8:65-9:4.

B. Prosecution History

After Applicant filed terminal disclaimer over 9,972,010 and 10,713,656, multiple rejections under §§101 and 115 and an RCE, a Notice of Allowance issued, with an Examiner amendment, apparently negotiated by the Applicant during an interview to address the §101 rejection. APPL-1002, 138-146, 171-182, 184-198; APPL-1003, ¶¶34-38.

V. LEVEL OF ORDINARY SKILL IN THE ART

The level of ordinary skill in the art may be reflected by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). Here, a Person of Ordinary Skill in the Art (“POSITA”) at the time of the claimed invention would have had a bachelor’s degree in electrical engineering, computer engineering, computer science, or a related field, and at least two years of experience in the research, design, development, and/or testing of biometric authentication techniques, and related firmware and software, or the equivalent, with additional education substituting for experience and vice versa. APPL-1003, ¶20. Furthermore, a person with less formal education but more experience, or more formal education but less experience, could have also met the relevant standard for POSITA. *Id.* However, Petitioner does not imply that a person having an extraordinary level of skill should be regarded as POSITA.

VI. CLAIM CONSTRUCTION

During IPR, claims are construed according to the standard as set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). 37 C.F.R. §42.100(b) (Nov. 13, 2018). Petitioner believes that, for the purposes of this proceeding and the analysis presented herein, no claim term requires express construction. *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (“only those terms need be construed that are in controversy, and only

to the extent necessary to resolve the controversy”). Accordingly, this Petition analyzes the claims consistent with ordinary and customary meaning as would be understood by POSITA in light of the specification.¹ *Phillips*, 415 F.3d at 1314-17; APPL-1003, ¶¶39-40.

VII. REQUESTED RELIEF

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

VIII. OVERVIEW OF CHALLENGES

A. Challenged Claims

Claims 1-12, 14-18, and 20-23 (“Challenged Claims”) of the ’886 patent are challenged.

B. Statutory Grounds² for Challenges

Ground	Claims	Basis
#1	1-12, 14-18, and 20-23	§103(a) over Stone in view of Hoyos and Varghese
#2	1-12, 14-18, and 20-23	§103(a) over Stone in view of FFIEC Guidance
#3	15-17 and 21-23	§103(a) over Stone in view of Hoyos,

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

² Pre-AIA §§102 and 103(a) apply.

		Varghese, and Campbell
#4	15-17 and 21-23	§103(a) over Stone in view of FFIEC Guidance and Campbell

Stone was filed Aug. 15, 2008 and published Feb. 18, 2010. Hoyos was filed Oct. 2, 2007 and published Jan. 21, 2010. Stone and Hoyos each are prior art under at least §§102(a) and 102(e). Varghese was filed Apr. 28, 2006 and published Dec. 14, 2006. Varghese is prior art under §102(b). FFIEC Guidance (also referred to as “Guidance”) was published October 12, 2005, and was prior art under at least §102(b). Dr. Jones testifies that the Guidance was publicly accessible to a POSITA, and was widely referenced by numerous articles and patent disclosures before 2010 as an important driver for implementing multifactor authentication for electronic transaction including financial transactions. APPL-1003, ¶¶52-54 (citing APPL-1039, APPL-1040, archive.org links, Google Scholar cites, patent disclosures).

Campbell was published Sep. 1997, and is prior art under §102(b).

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 ’886 patent, because it is directed to electronic transactions,

and specifically, financial transaction applications. APPL-1008, [0001]-[0005]; APPL-1003, ¶¶39-40.

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. APPL-1008, [0016]; FIGS. 1-3. Stone’s system includes user devices of different types (“mobile phone, laptop computer, PDA, or personal computer,” etc.) and various communication connections (“the Internet and/or one or more intranets, landline networks, wireless networks” etc.). APPL-1008, [0022], [0024], [0041], [0044], [0046].

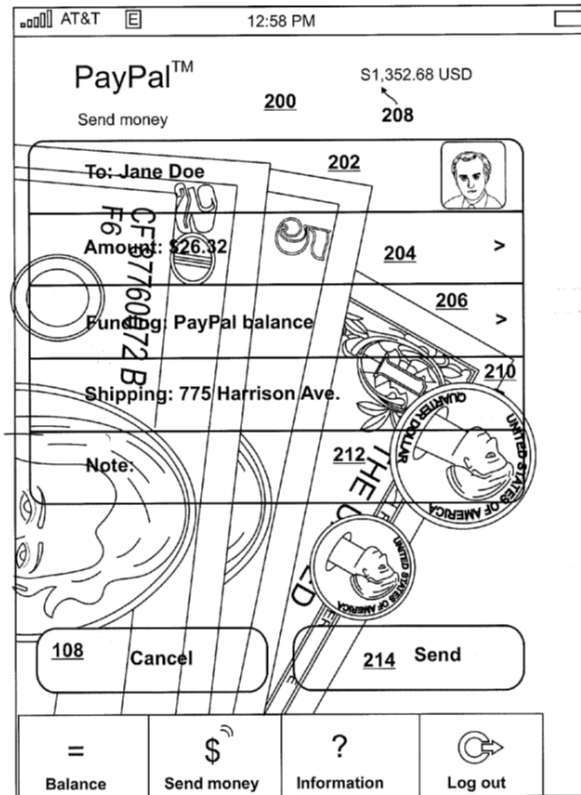


FIG. 2

APPL-1008, FIG. 2

2. Hoyos

Hoyos is directed at fraud detection with “authentication for financial transactions using biometrics.” APPL-1013, Abstract, [0002]; APPL-1003, ¶¶41-45.

Hoyos identifies a “spoofing” problem (e.g., using “a life-sized, high-resolution photograph” instead of a live person) “in the field of authentication of financial transactions,” where “high levels of accuracy and speed are critical.” APPL-1013, [0009], [0011]. To address these issues, as illustrated in FIG. 1 of Hoyos below, Hoyos describes an authentication method based on a combination

of biometric match and liveness analysis. APPL-1013, [0017], [0012], [0011], [0018]-[0021], claims 5-8 (describing liveness determination based on a plurality of images).

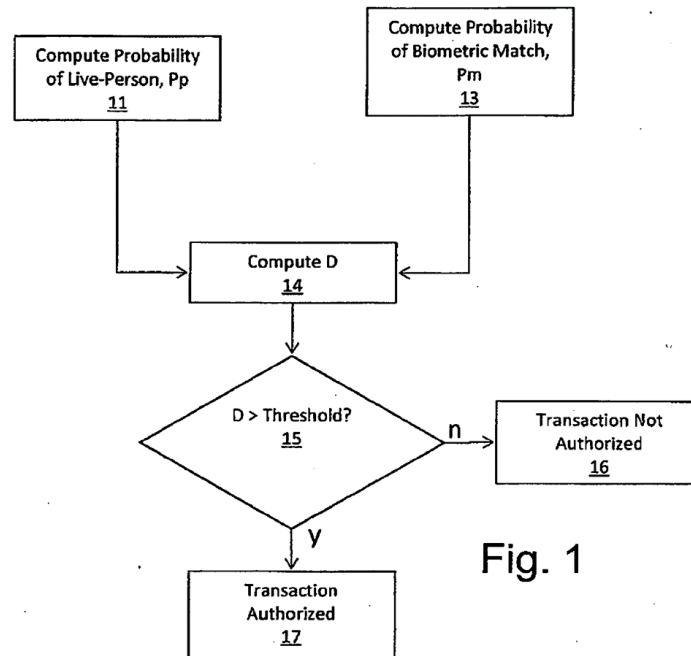


Fig. 1

APPL-1013, FIG. 1

Hoyos provides its biometric authentication system achieves various benefits, including protection against spoofing; “making it much more difficult for an attempted fraudster to refine fraudulent methods” by using a combination of liveness and comparison; greatly reducing “the reject rate of true authentic” by using the liveness probability; providing “an enormous deterrent to criminals;” and 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, ¶¶46-48.

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

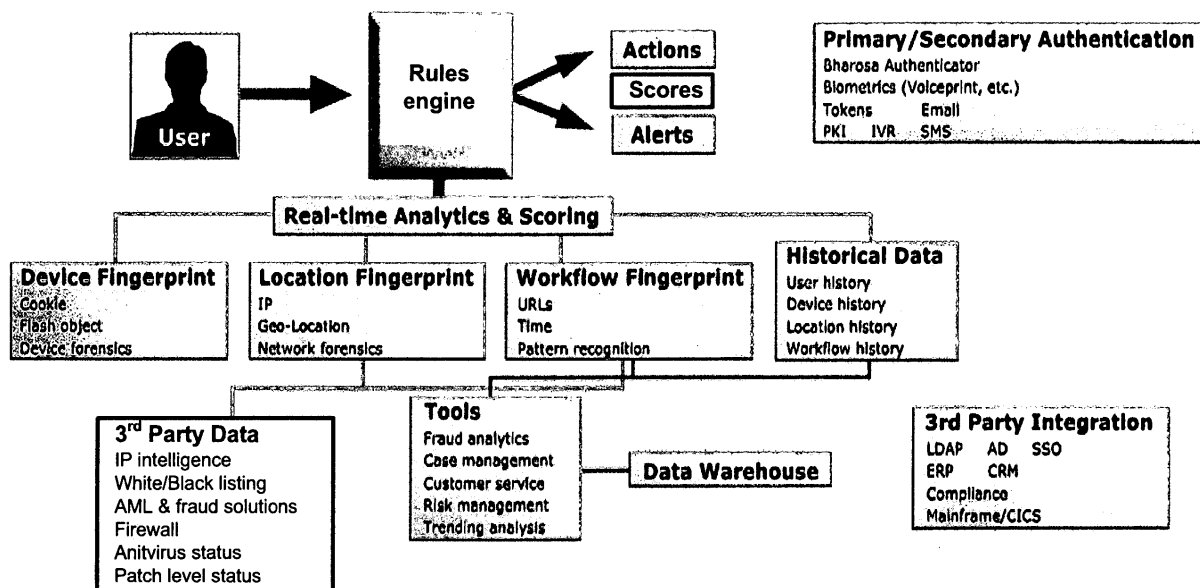


FIG. 14

APPL-1010, FIG. 14

Varghese describes performing multifactor real-time authentication (including location authentication (e.g., using “Geo-Location”) and voice authentication (e.g., using “Biometrics (Voiceprint, etc.)”) for improved fraud analysis. APPL-1010, FIG. 14. Varghese describes transaction authentication

(“post-authentication”) for transaction requests, which is 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 (or “Guidance”)

The Federal Financial Institutions Examination Council (FFIEC) is a formal U.S. government interagency body composed of five banking regulators (including FDIC) and is “empowered to prescribe uniform principles, standards, and report forms...to promote uniformity in the supervision of financial institutions.”³ On Oct. 12, 2005, FFIEC issued its guidance titled “Authentication in an Internet Banking Environment” that describes “enhanced authentication methods that regulators expect banks to use.” APPL-1037; APPL-1039, 1. The Guidance was publically available to a POSITA interested in the security electronic transactions. APPL-1039; APPL-1003, ¶¶50-52 (citing APPL-1039, APPL-1040, Google

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

Scholar cites, archive.org links, and patent disclosures referencing Guidance as the driver for multifactor authentication in financial transactions).

The Guidance explains that that “single-factor (e.g., ID/password) authentication” may not be sufficient, 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 (“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. Campbell

Campbell is titled “Speaker Recognition: A Tutorial,” and is directed at technologies that “could substantially reduce this [high-tech computer thieves] crime by reducing these fraudulent transactions.” APPL-1033, 1439; APPL-1003, ¶¶55-57.

As shown in FIG. 3 of Campbell, Campbell describes that the general approach to automatic speaker verification includes five steps: “digital speech data acquisition, feature extraction, pattern matching, making an accept/reject decision, and enrollment to generate speaker reference models.” APPL-1033, 1438. Campbell describes that a feature extraction technique (mel-warped cepstrum) using Fast Fourier transform (FFT) “is very popular” and “has been demonstrated to work well in speaker-recognition systems.” APPL-1033, 1445.

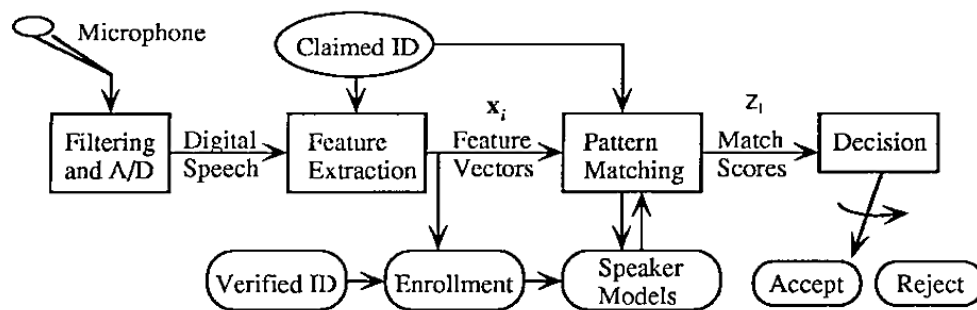


Fig. 3. Generic speaker-verification system.

APPL-1033, FIG. 3

6. Analogous Art

Stone, Hoyos, Varghese, Guidance, and Campbell are analogous art to the '886 patent, because each is at least (1) in the same field of endeavor (electronic financial transactions); or (2) reasonably pertinent to a problem with which the inventor of the '886 patent was involved (e.g., fraud detection in electronic financial transactions). APPL-1003, ¶58; compare APPL-1001, Title (“Method, Medium, and System for Reducing Fraud”), Background of the Invention; APPL-

1008, Title, [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”), [0145]; APPL-1033, 1437-1439 (“Automatic speaker-recognition technology could substantially reduce this [high-tech computer thieves] crime by reducing these fraudulent transactions.”); APPL-1037, Title (“Authentication in an Internet Banking Environment”).

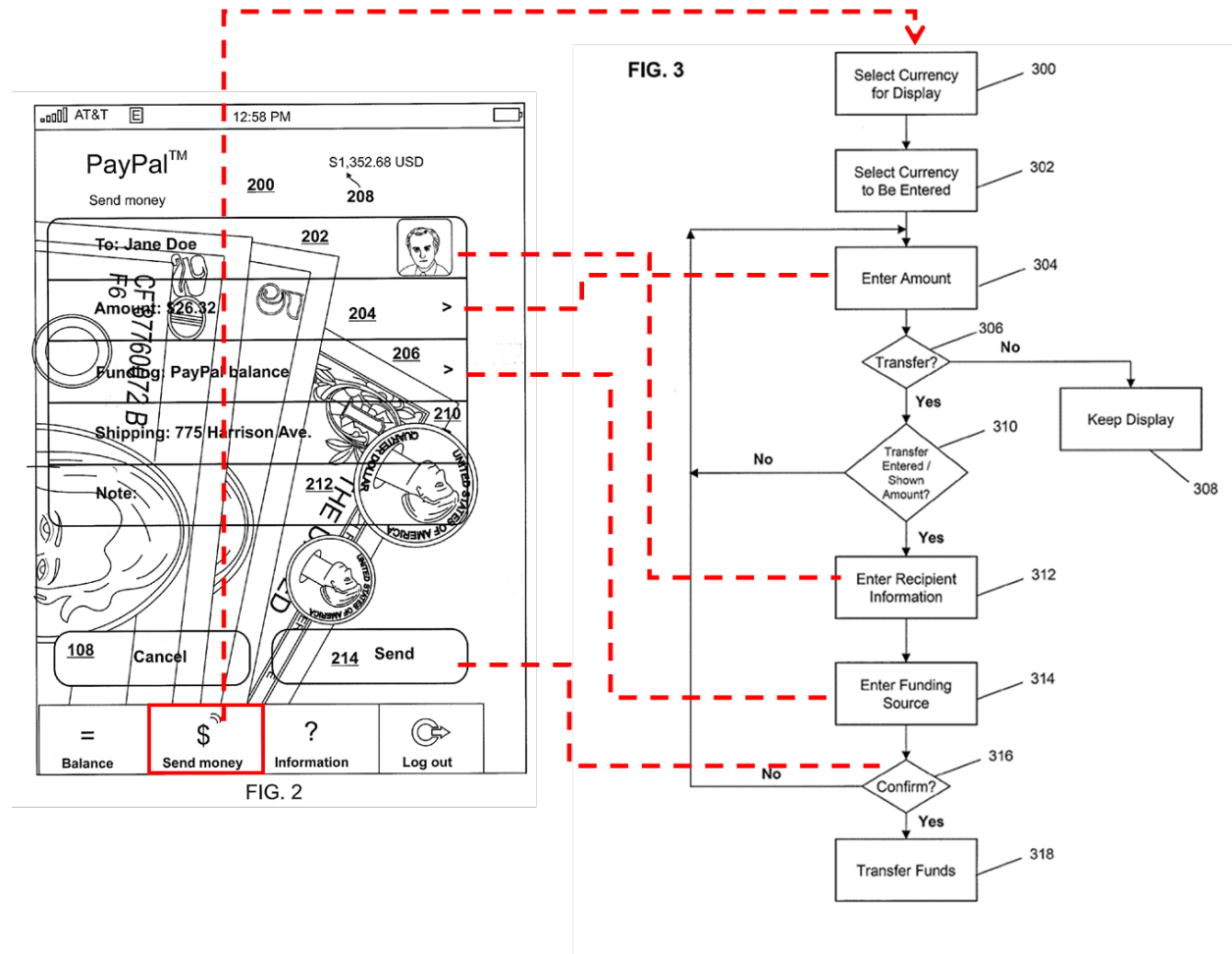
B. Ground 1: Claims 1-12, 14-18, and 20-23 are Rendered Obvious under §103(a) over Stone in view of Hoyos and Varghese.

1. Combination of Disclosures/Embodiments of Stone

A POSITA would have been motivated to combine disclosures or embodiments of Stone, e.g., FIG. 2 and 3, to provide a transaction system using user interfaces (e.g., as taught by FIG. 2) for performing an electronic transaction (e.g., as taught by FIG. 3). *Boston Scientific Scimed, Inc. v. Cordis Corp.*, 554 F.3d 982, 991 (“Combining two embodiments disclosed adjacent to each other in a prior art patent does not require a leap of inventiveness.”); APPL-1003, ¶¶59-63.

A POSITA would have understood that the display of FIG. 2 and modification thereof could be used to implement FIG. 3, e.g., by adding, removing, modifying components, or by using alternative design choices of buttons and icons.

APPL-1003, ¶¶60; APPL-1008, [0055]-[0056]. An example implementation relationship with FIGS. 2 and 3 of Stone is provided below.



APPL-1008, FIGS. 2 and 3, annotated

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, ¶¶62-53. For example, 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.

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, for the benefits of improved fraud resistancy by addressing spoofing and “improved deterrent against attempted fraudulent transactions, and decreased rejection of valid customers.” APPL-1013, [0015], [0017]-[0022]; APPL-1003, ¶¶64-73.

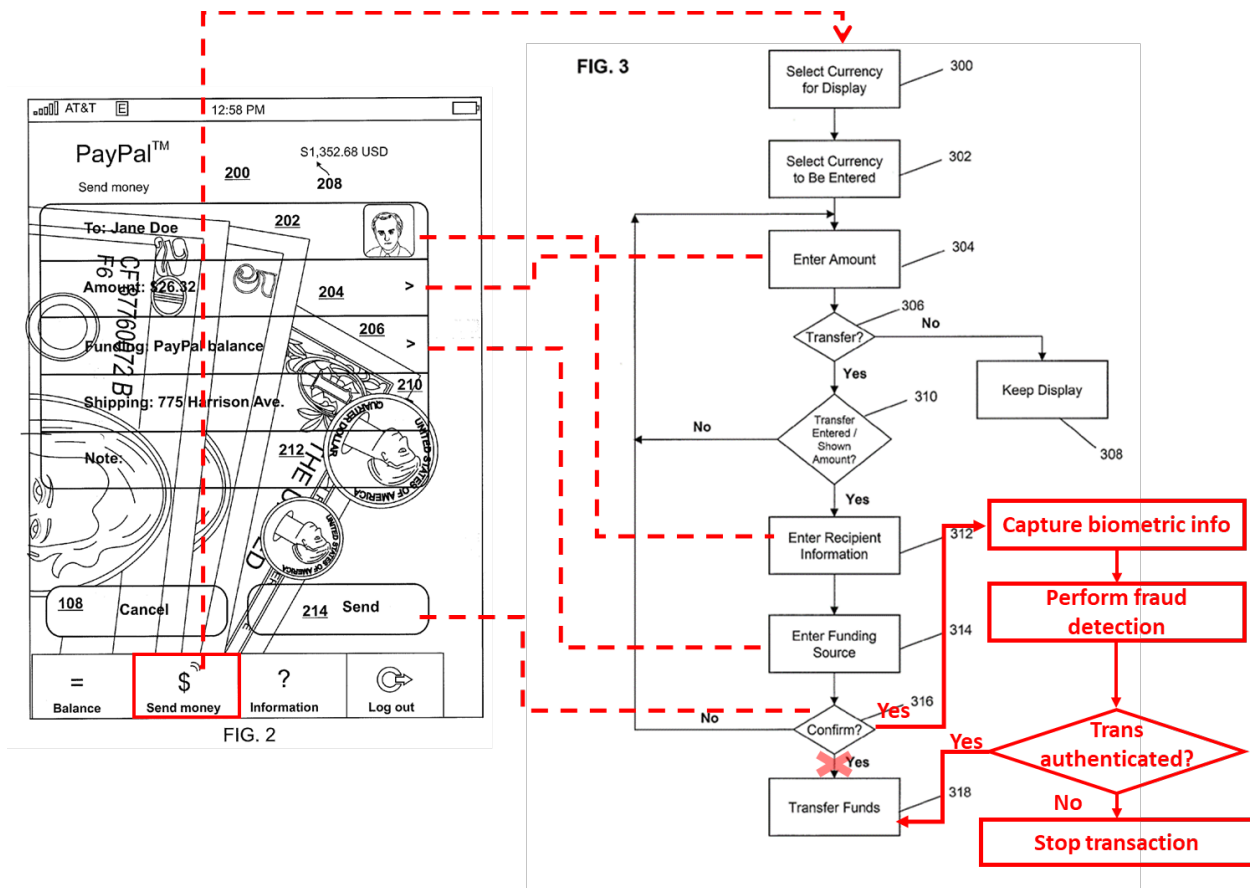
As discussed at IX.A.5, Stone and Hoyos each are analogous art to the ’886 patent. APPL-1003, ¶65 (citing APPL-1010, [0079]; APPL-1013, Title, Abstract, [0002]).

Further, it was well-known that financial transaction systems of Stone had a need for authentication for fraud detection (e.g., with higher levels of security for higher-risk transactions). APPL-1003, ¶66; APPL-1013, [0009], [0011]; APPL-1010, [0148]; APPL-1016, FIG. 3, [0073]; APPL-1037, 1; APPL-1022, 1 (describing increased online fraud impacts consumer confidence and business, and “pressure to proactively detect and prevent fraud” by regulatory mandates such as FFIEC).

A POSITA would have been motivated to implement Hoyos’ spoofing-resistant biometric authentication in the system of Stone for “improved deterrent

against attempted fraudulent transactions, and decreased rejection of valid customers.” APPL-1003, ¶67. 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”; providing “an enormous deterrent to criminals;” and providing “a means to perform customer redress.” APPL-1013, [0024], [0026], [0027], [0029].

To achieve such an improved financial transaction system with biometric authentication, a POSITA would have been motivated to incorporating Hoyos’ biometric authentication teachings in Stone according to the following Stone-Hoyos example. APPL-1003, ¶68; 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 of the transaction authentication process (e.g., including capturing input data for liveness analysis and biometric comparison) after a user confirms a user transaction request (e.g., at block 316). APPL-1003, ¶69.

A POSITA would have understood that performing transaction (including capturing input data e.g., biometric information) after and in response to user transaction request confirmation had various benefits over the alternative design

choice of using only previously captured input data before user transaction request confirmation. APPL-1003, ¶70.

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 specific transaction and assessed risk thereof for improved fraud detection, where Hoyos already describes setting a higher decision threshold for a transaction with a higher amount/security type. APPL-1003, ¶70 (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]). 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, ¶70 (citing APPL-1010, FIG. 14, [0097]-[0099], TABLE 10; APPL-1015, FIG. 4; APPL-1035, 4:60-62, 4:66-67).

A POSITA would have reasonably expected to succeed in configuring Stone-Hoyos, 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, ¶¶71-73 (citing APPL-1008, [0004]; APPL-1009, 15:22-23; APPL-1013, Title, claims 13 and 14, [0007], [0040]; APPL-1016, [0040], [0042], [0076]; APPL-1015, FIG. 3, 4:4-10; APPL-1016, [0040], [0042]; APPL-1038, 64).

3. Combination of Stone, Hoyos, and Varghese

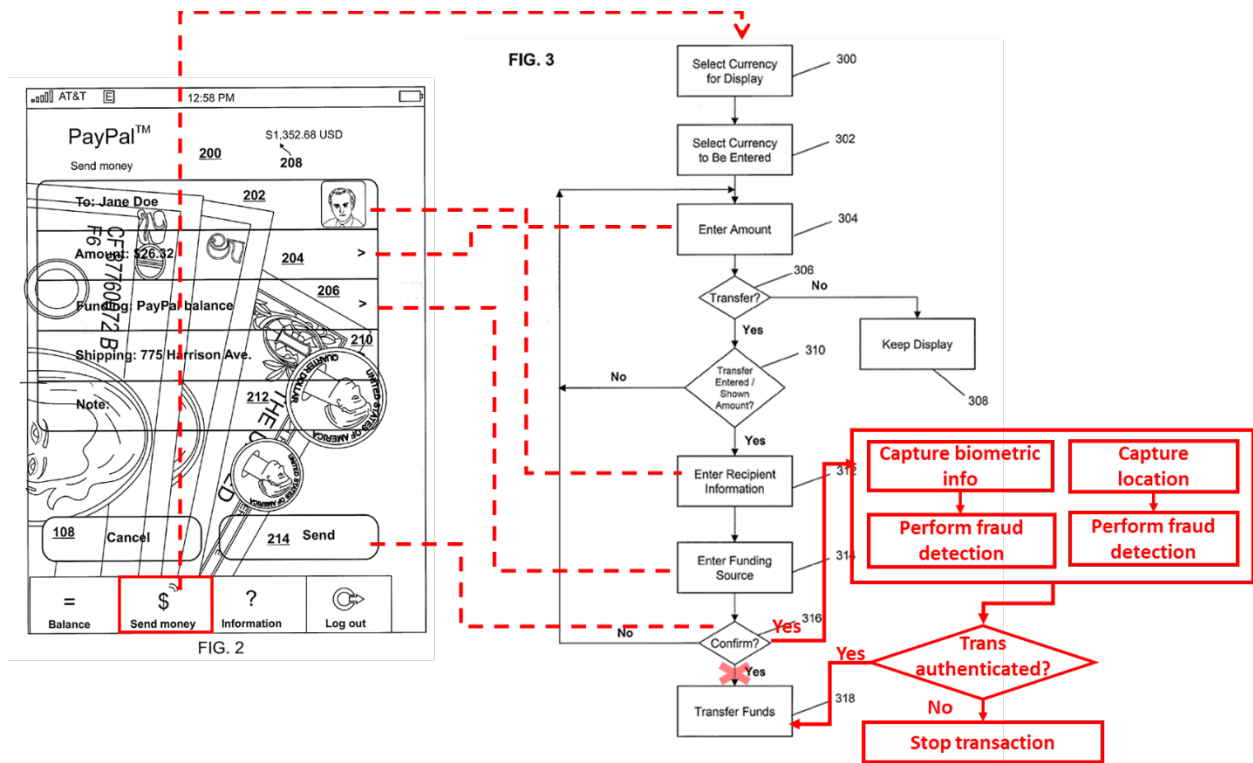
A POSITA would have been motivated to apply Varghese's teaching of real-time multifactor authentication (including location authentication combined with biometrics (e.g., voice, fingerprints, retinal scans, etc.)) for user transaction requests, in Stone-Hoyos for improved security for financial transactions. APPL-1003, ¶¶74-84; APPL-1010, [0079].

As discussed at IX.A.5, Varghese is analogous art to the '886 patent. APPL-1010, [0145]; APPL-1003, ¶75.

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 real-time multifactor authentication for user transaction requests for improved security. APPL-1003, ¶76 (citing APPL-1016, [0036]; APPL-1022, 1).

Techniques using multifactor authentication (e.g., location authentication combined with biometrics) to provide additional security for financial transactions, as taught in Varghese, were well-known. APPL-1003, ¶77 (citing APPL-1016, [0043]).

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, ¶78.



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 real-time multifactor authentication (including capturing input data and performing fraud detection thereupon) for user transaction request (also referred to as “post-authentication”) **after** a user confirms a user transaction request (e.g., at block 316). APPL-1003, ¶¶79-81; 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.

A POSITA would have reasonably expected to succeed in configuring Stone-Hoyos-Varghese since implementing Varghese’s multifactor real-time

authentication functionality would have required only routine knowledge well within the skill of a POSITA prior to the earliest effective filing date. APPL-1003, ¶¶82-84 (citing APPL-1008, [0026]; APPL-1010, [0093]; APPL-1016, [0040], [0042], [0076]; APPL-1015, FIG. 3, 4:4-10; APPL-1038, 64).

4. Claim 1

[1.0] A system, comprising:

Stone discloses or renders obvious the preamble to the extent that it's limiting. APPL-1003, ¶¶85-88.

Specifically, as shown in FIG. 4 of Stone below, Stone describes “**a system 400** configured to utilize the currency display over a network 402,” which “includes at least a user device 404, one or more recipient 406 devices, and at least one payment provider server 408 in communication over the network 402.” APPL-1008, [0040].

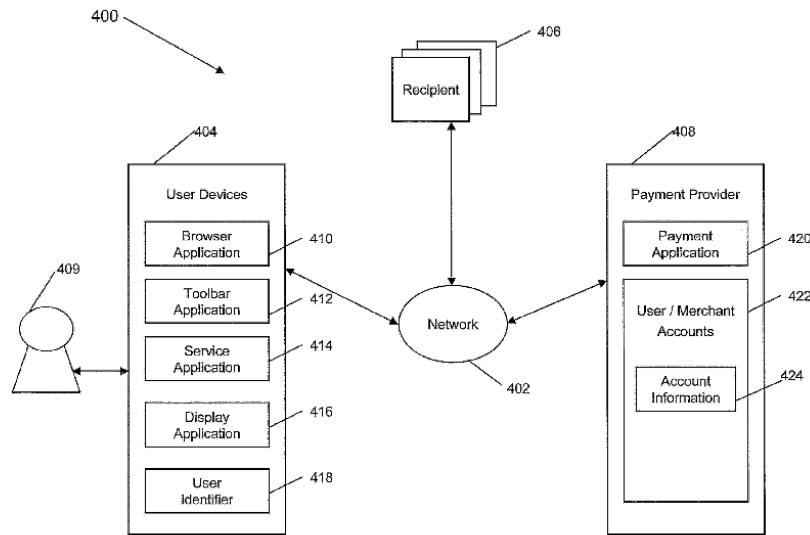


FIG. 4

APPL-1008, FIG. 4

Stone describes that “recipient devices 406 **may be the same** or have the same basic features as user device 404,” and may be implemented as various types of devices, including “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], [0054]

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

[1.1] one or more processors configured to:

Stone alone or Stone-Hoyos-Varghese renders obvious this element. APPL-1003, ¶¶89-94.

First, Stone describes a system (e.g., system 400 of FIG. 4) including one or more processors (e.g., processor 504 in user device 404 alone, or in combination with processors 504 of over devices in the system) configured to perform processes for a transaction. APPL-1008, [0049] (examples of processing component 504 include “**processor, micro-controller, digital signal processor (DSP), etc.**”); claim 1 (“A device comprising:...a **processor**...”).

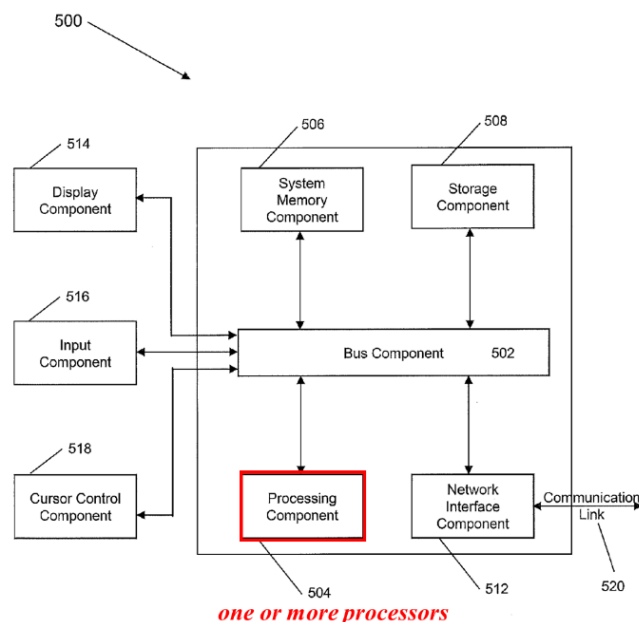


FIG. 5

APPL-1008, FIG. 5, annotated

As shown in FIG. 4 of Stone below, the one or more processors of the system 400 are configured to process data, such as computer program instructions, for perform processes for a transaction. *See also* APPL-1001, 2:21-23 (the '886 patent provides, “[a]s used herein, the term ‘processor’ refers to one or more devices, circuits, and/or processing cores configured to process data, such as

computer program instructions.”).

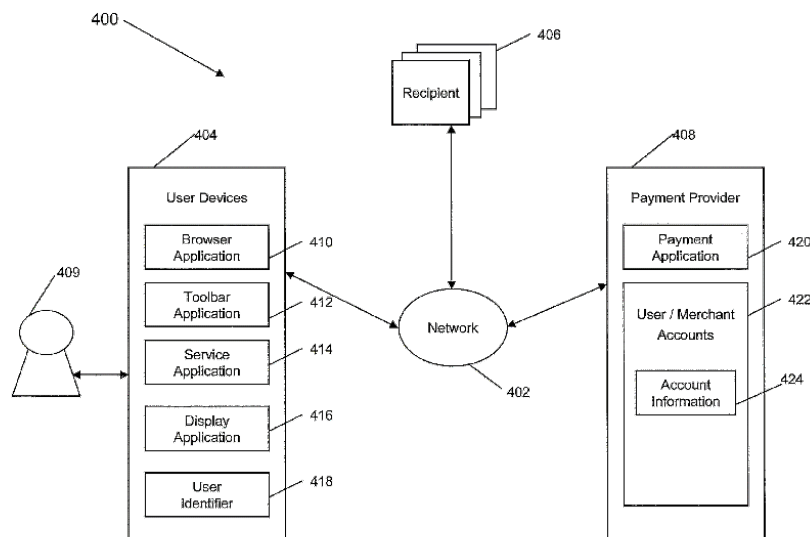


FIG. 4

APPL-1008, FIG. 4

Second, as discussed below at Ground 1:[1.2]-[1.4.2], Stone alone or Stone-Hoyos-Varghese teaches [1.2]-[1.4.2], and a POSTA would have understood to modify Stone such that the one or more processors are configured to perform the processes including [1.2]-[1.4.2] for processes including initiating, authenticating, and completing the electronic transaction. APPL-1003, ¶93.

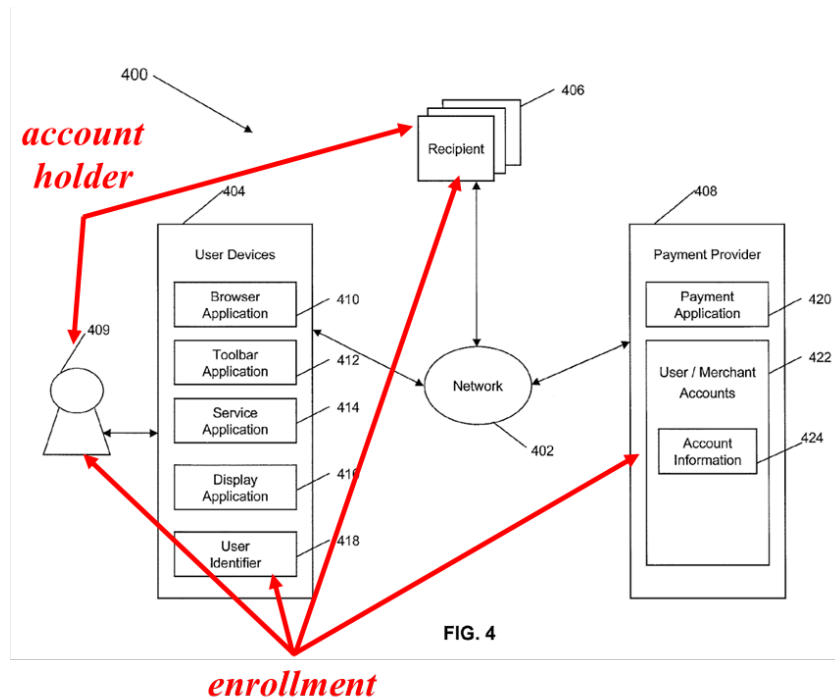
Therefore, Stone alone or Stone-Hoyos-Varghese renders obvious “*one or more processors*” as claimed.

[1.2.1] render, in one or more interfaces, a virtual likeness of a face associated with an account holder,

Stone discloses or renders obvious this element. APPL-1003, ¶¶95-99.

Specifically, Stone discloses one or more processors (e.g., of devices of system 400) configured to *render, in one or more interfaces* (e.g., interface 200 of

FIG. 2), *a virtual likeness of a face* (e.g., a photo of the user/sender on the personalized currency or a photo of recipient of the electronic transaction each disclosed by Stone) *associated with an account holder* (user 409/sender or recipient each having a user account 422). APPL-1003, ¶96; APPL-1008, [0048].



APPL-1008, FIG. 4, annotated

First, as shown in annotated FIG. 2 below, a photograph of a user's face on the personalized currency on interface 200 corresponds to *a virtual likeness of a face associated with an account holder* (user/sender) as claimed. APPL-1008, claim 1, [0007] ("the user may select or create his own currency for display, such as...**personalized currency with the user's photo**, etc."); *see also* APPL-1001, 5:45-51 (describing virtual likeness of a user including "a photograph, an avatar, or other representation of Bob").

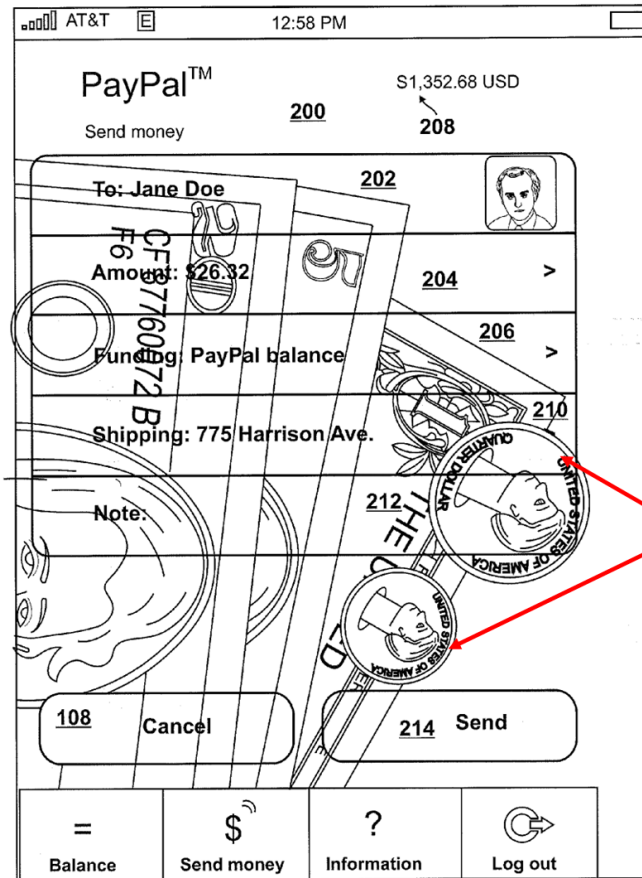


FIG. 2

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

Second, and additionally, claim 2 of '886 patent recites that “the account holder comprises a **recipient of the electronic transaction**.” Accordingly, a virtual likeness of a face of the recipient must also be within the scope of claim 1, from which claim 2 depends. As such, Stone’s photo of recipient (as shown in FIG. 2 below next to the name box 202) also discloses the limitation. APPL-1008, [0024] (“display 200 has... **a picture of the recipient**”). See also APPL-1008, [0020], [0036] (describing “a recipient icon on the display, such as a **picture of the recipient**”).

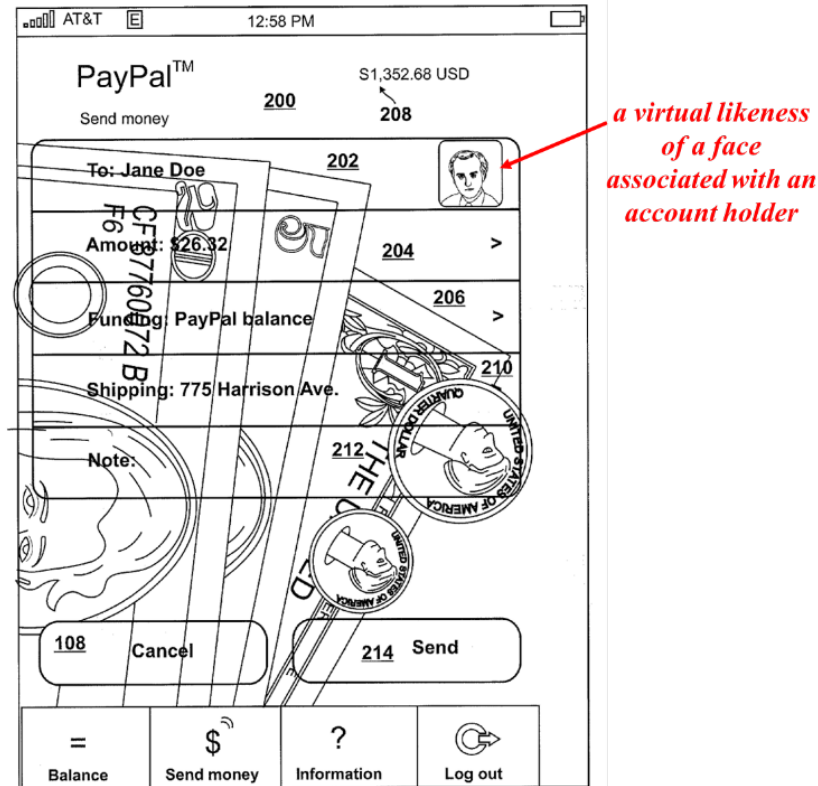


FIG. 2

APPL-1008, FIG. 2, annotated

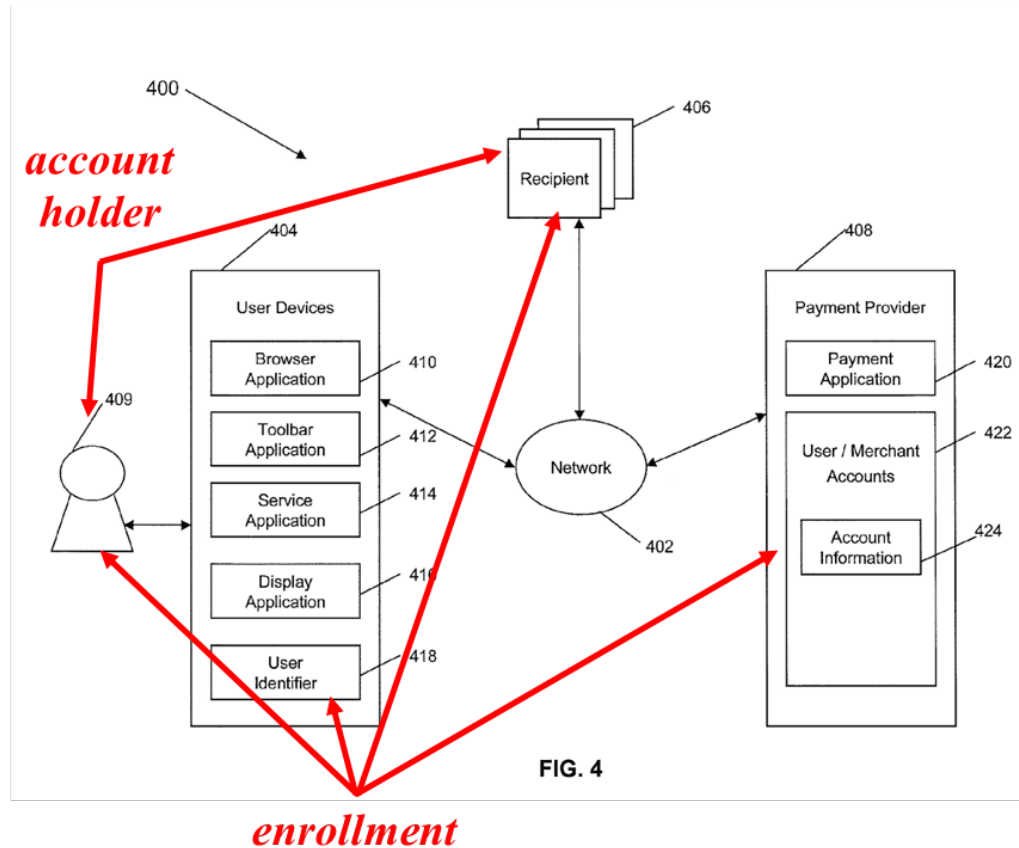
Therefore, Stone discloses or renders obvious this element.

[1.2.2] wherein the virtual likeness of the face was selected by the account holder as part of an enrollment;

Stone discloses or renders obvious this element. APPL-1003, ¶¶100-107.

Stone discloses that the virtual likeness of the face (displayed photograph of the account holder, either user/sender or recipient) was selected by the account holder as part of an enrollment/registration. Specifically, during enrollment/registration, the account holder (user 409) registers using user device 404 with the payment provider 408 with a user account 422, where the user identifier 418 (including “**photograph image**” selected by the user for display on

virtual currency, profile icon, etc.) is generated and stored on user device 418. Similar features apply to recipient account holder using recipient device 406. APPL-1003, ¶¶101-102; APPL-1008, [0045]-[0046], [0048].



APPL-1008, FIG. 4, annotated

A POSITA would have understood that Stone's user account registration/enrollment teaches the "enrollment" as claimed, where the user selects its photograph as a user profile icon during user registration/enrollment. Furthermore, Stone's user registration/enrollment includes biometric enrollment, because it was well-known that "**biometric id**" of its user identifier 418 was captured and stored during biometric enrollment, where the stored biometric id is

used (and as such referred to) as “enrollment data” for comparison with the later captured data for authentication. APPL-1003, ¶104 (explaining that “biometric id” means “biometric identification information”); APPL-1013, [0079] (“obtaining **biometric identification information**,” APPL-1014, [0009]; APPL-1021, Abstract; APPL-1023, 8:3-9:39; APPL-1013, [0003]; APPL-1024, 3:6-11; APPL-1037, 9-10.

Stone’s disclosure is consistent with, and reinforced by, a POSITA’s knowledge that, in practice, a user image (the *virtual likeness of the face*) is routinely selected by the account holder as part of user registration/enrollment with a service provider, and the selected user image is then used for display representing the user online. It would have been obvious to a POSITA that 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] (describing the social media aspect of the transaction application, “[w]hen the user is connected to a network with other users, the user display may **visually show other users**”), [0036]; APPL-1003, ¶105 (citing APPL-1036, [0002] (application from eBay providing user created social networks within a distributed commerce system including payment transactions to provide an improved level of trust between users)).

As such, a POSITA would have been motivated to provide a user the

selection option to choose images to use as the profile image for display both on its own display and on other users' display, which allows the user to select an online identity to connect with others, where increasing “a level of trust between [buyers and sellers to] increase online sales and corresponding profits”). APPL-1009, 1:20-28; 15:15-27 (“Profile image 504 can include a picture that a user of mobile device 500 **designates** as available to other users for purposes of presenting the user”); APPL-1003, ¶105 (citing APPL-1036, [0006], APPL-1009, 1:20-28; 15:15-27).

Furthermore, Stone's disclosure of enrollment/registration is consistent with the description of the '886 patent, where it uses “enrollment” and “registration” interchangeably. APPL-1003, ¶106; APPL-1001, 5:39-41, 7:64-8:1 (“as part of an **enrollment** process, Alice was asked to photograph herself... Alice is shown the image she provided at **registration** (502)”).

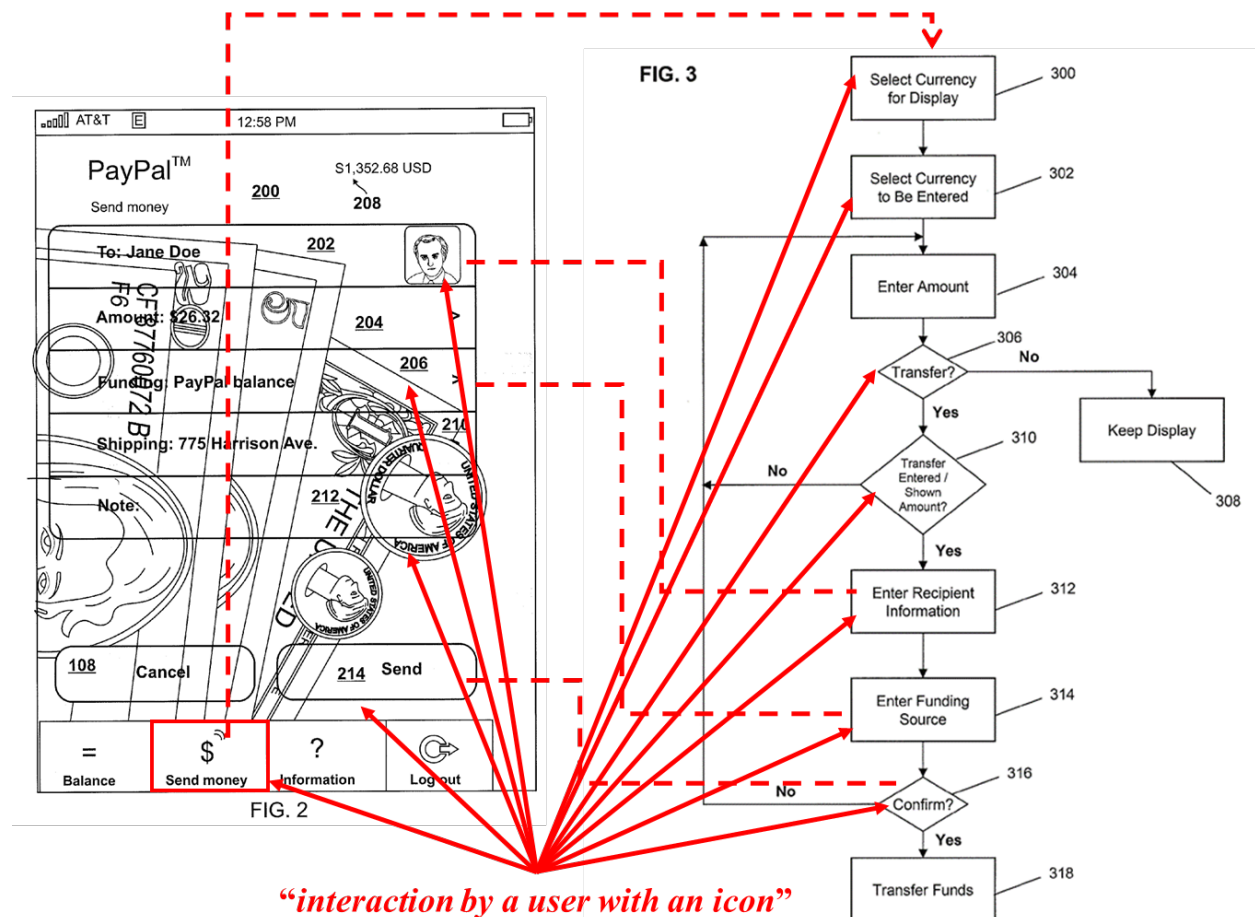
Therefore, Stone-Hoyos-Varghese renders obvious this claim.

[1.3.1] subsequent to an interaction by a user with an icon rendered in the one or more interfaces: capture contextual information comprising location data usable to determine a physical location associated with the user; and

Stone in view of Hoyos and Varghese renders this element obvious. APPL-1003, ¶¶108-120.

First, as shown in annotated FIGS. 2 and 3 of Stone below, each of the annotated control elements/blocks and other control elements (e.g., (“Send,” “Confirm,” or “Proceed” described in Stone) teaches an interaction by a user with

an icon rendered in the one or more interfaces (e.g., interface 200) as claimed, because each of these control elements/blocks is implemented (or would have been obvious for a POSITA to implement) using an icon in the interfaces of the user device for better visual presentation, and the user interaction with the icon (e.g., clicking, tapping on, dragging/sliding, dragging/sliding to/from) provides an indication that the user initiates, continues, or confirms a transaction request associated with the electronic transaction. APPL-1003, ¶109.



APPL-1008, FIGS. 2 and 3, annotated

For example, a POSITA would have understood that as shown in FIG. 2 of Stone above, “\$Send Money” at the bottom is implemented using an icon including “\$”, a user interacting with (e.g., by clicking/tapping on) the “\$Send Money” icon provides a user indication for initiating a send money transaction request, and in response, a corresponding interface 200 for a send money transaction is displayed for starting a send money method (e.g. FIG. 3 of Stone). APPL-1003, ¶110.

Similarly, a POSITA would have implemented each of the annotated blocks of FIG. 3 with an icon as claimed, serving as a visual indicator to the user for various user interactions to continue/confirm the transaction. APPL-1003, ¶111; APPL-1008, [0024] (“a send button 214”), [0025] (“Sending can be the user tapping on an appropriate button on the display, such as “Send,” “Confirm,” or “Proceed.”). For further example, the personalized virtual currency of Stone teaches a transaction icon associated with an electronic transaction, because Stone describes examples where the user drags or slides the virtual currency to the recipient icon to transfer funds. APPL-1008, [0020], [0036].

To the extent that any of the control items/blocks described above is not explicitly described as an icon in Stone, a POSITA would have been motivated to implement the control items/blocks using an icon, because icon and button are alternative design choices for control elements/blocks, and using icons provides “a more visually rich interface.” APPL-1008, [0016], [0004] (recognizing that “icon”

and “button” are alternative design choices, stating that “[t]he consumer typically clicks on **an icon or button** to make the transfer.”), [0038], [0035],

Stone’s icons as discussed above together with user interactions therewith (e.g., clicking/tapping on/sliding/dragging (including from/to)) each teach an “*an interaction by a user with an icon*” as claimed, because it was well-known that clicking/tapping on/sliding/dragging (including from/to) an icon by a user discloses user interaction. APPL-1003, ¶112 (citing APPL-1020, 27, 34-36; APPL-1019, 6:24-26).

Second, as shown in annotated FIG. 14 of Varghese below, Varghese describes, after the user confirms user transaction requests (referred to as “post-authentication”), capturing real-time contextual information including capturing real-time location data usable to determine a user physical location for fraud analysis, where the “**Real-time** Analytics & Scoring” for authentication uses “**Location** Fingerprint” including “IP, **Geo-Location**, Network Forensics.” APPL-1010, [0097]-[0099] (describing that these authentication/fraud detection techniques “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.”), [0074] (“requests usually handled by **post-authentication** services include, e.g., transaction requests involving large amounts of money”), [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, while especially so in the pre-authentication period. APPL-1010, [0093], [0109] (describing business policies applied during post-authentication where an example rule using location based on IP address is “don’t allow (or challenge user for) money transfer request from an international IP address”); APPL-1003, ¶113.

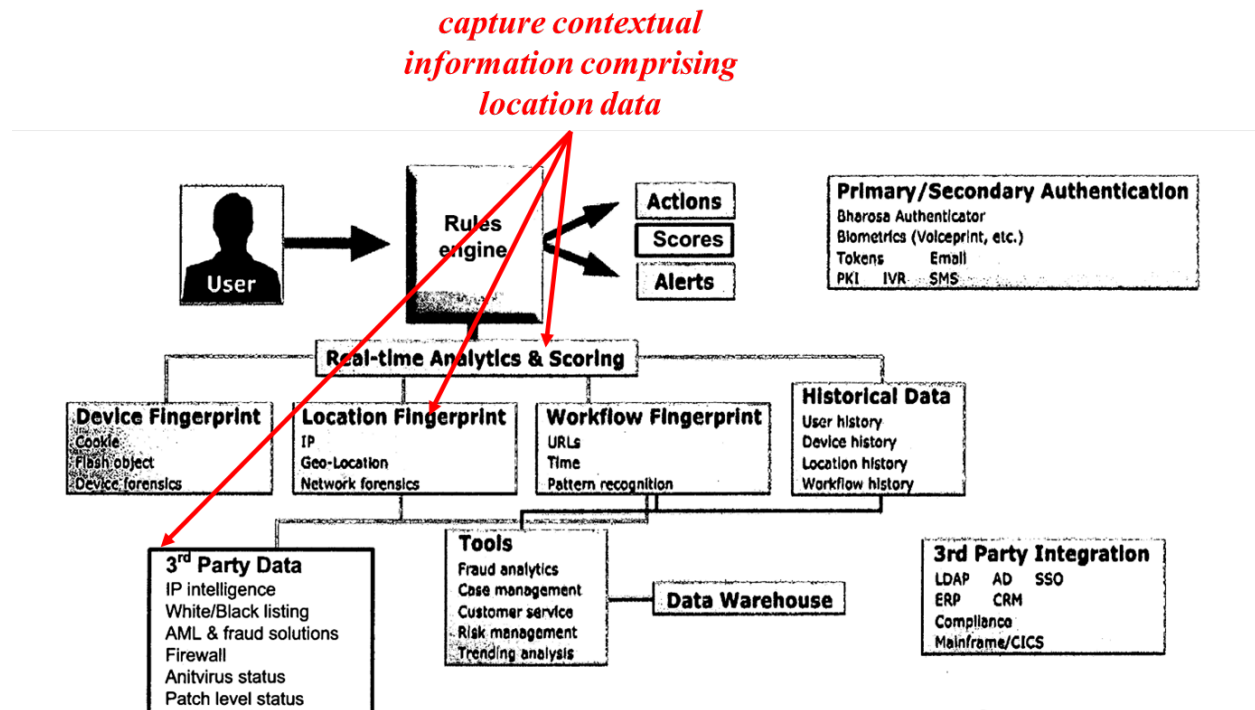


FIG. 14

APPL-1010, FIG. 14, annotated

A POSITA would have understood “real-time” authentication as described in Varghese includes both real-time capture and real-time analysis of input authentication data for transaction authentication, which provides more accurate

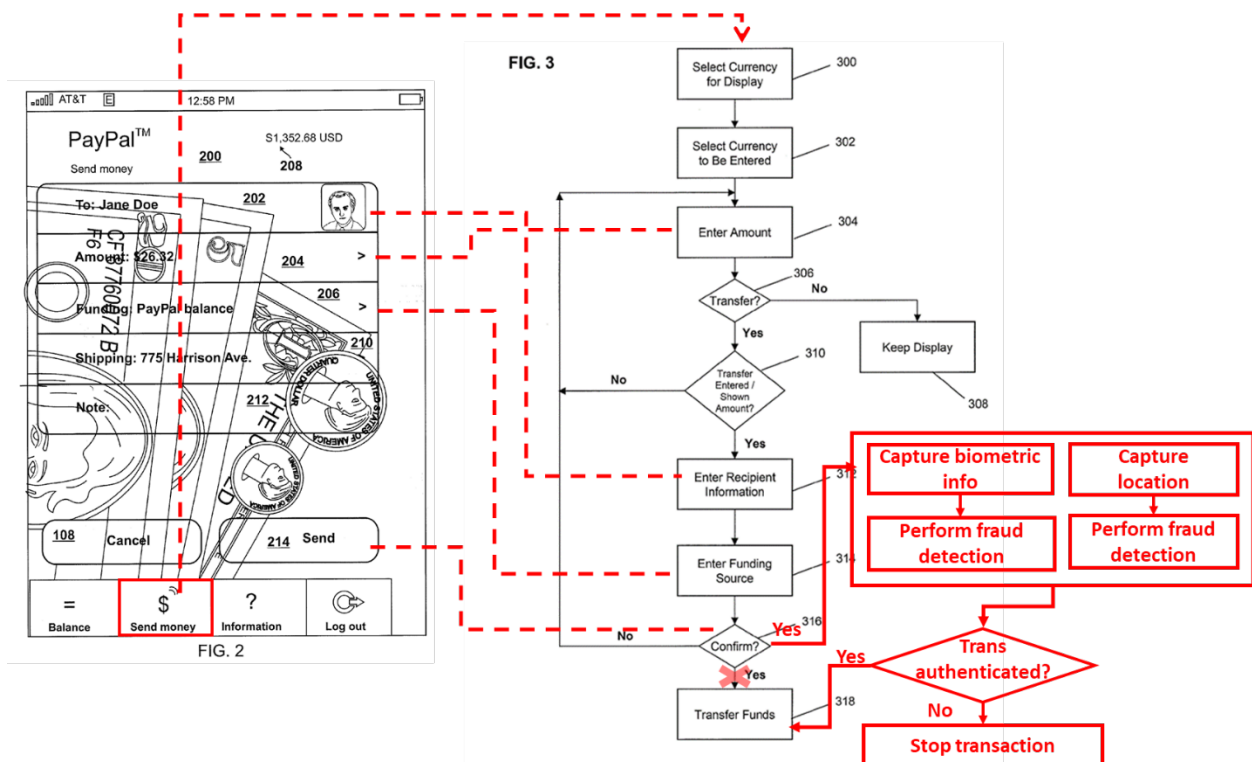
fraud analysis by using more accurate, real-time input data. APPL-1003, ¶114; APPL-1016, [0043] (describing real-time GPS capture for GPS location authentication, where “[a high value] transaction will be prevented unless the person is identified to be a specific location); [0044]; APPL-1035, 4:60-62 (describing real-time authentication data capture with the benefit to “avoid imposters from communicating based on stolen biometric data”), 4:66-67.

Varghese’s location data captured for “post-authentication”/transaction authentication is contextual information of the transaction, e.g., a user location from which the transaction request originates. APPL-1003, ¶115; APPL-1010, [0081], [0140] (describing using “external third-party data providers” including [a] **geolocation service 612**” which “provides **approximate geographic latitude and longitude** corresponding to **the user device IP address**”), [0142] (describing providing more security against a possible fraudulent transaction for a user transaction request “**where the device resides in a location, determined by geolocation information**, known for a[] larger than normal volume of fraudulent activity”), claim 31.

Third, as discussed at IX.B.3, a POSITA would have been motivated to apply Varghese’s teaching of real-time multifactor authentication (location authentication (capturing location data and performing fraud analysis based thereupon) together with biometrics) after user transaction request confirmation in

the electronic financial transaction system of Stone, which is performed **subsequent to** user transaction confirmation (block 316 of FIG. 3 of Stone) for improved security. APPL-1003, ¶116.

Based on the combined functionality of the improved financial transaction system with real-time multifactor authentication (including location authentication with biometrics), a POSITA would have been motivated to implement the following example Stone-Hoyos-Varghese for performing a financial transaction: APPL-1003, ¶117.

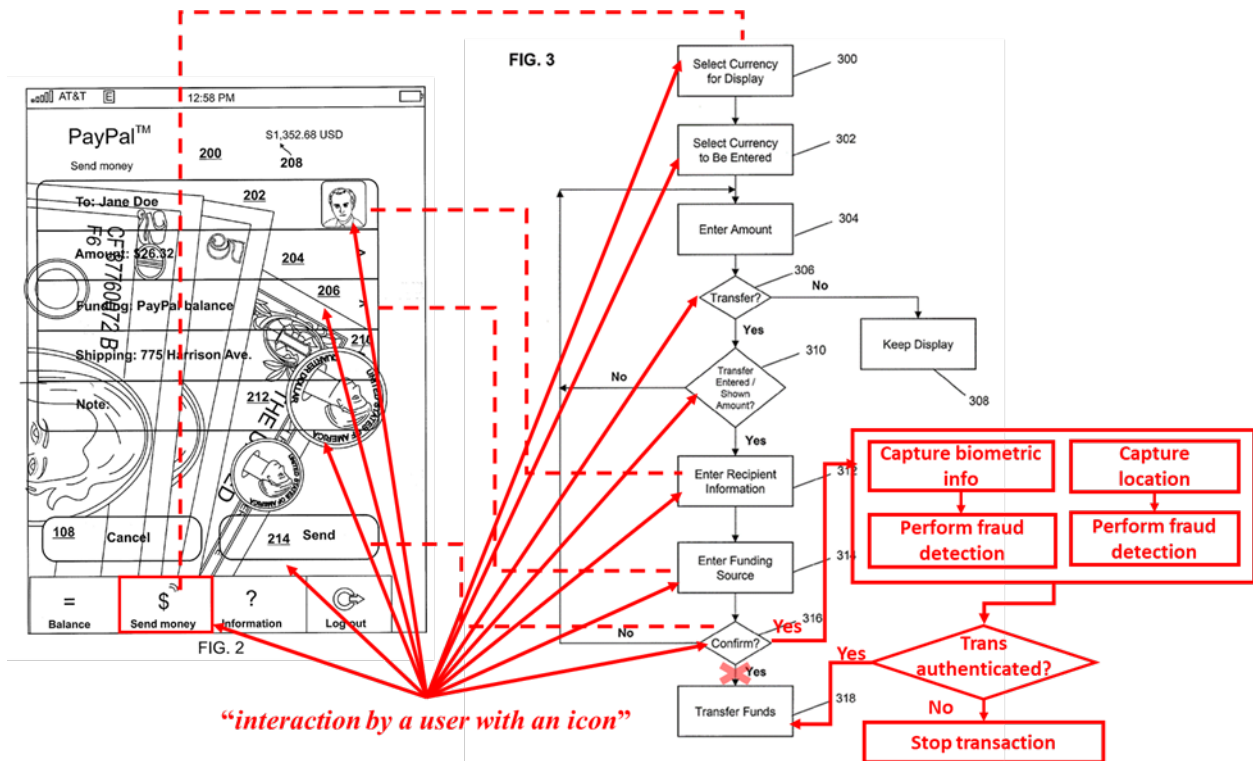


**Example of Stone-Hoyos-Varghese
(annotated based on APPL-1008, FIGS. 2 and 3)**

A POSITA would have been motivated to implement the multifactor real-time authentication as taught by Varghese (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, ¶118; 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.

In example Stone-Hoyos-Varghese below, various examples of user interaction with an icon as claimed are illustrated, which precede user transaction request confirmation and subsequent real-time multifactor authentication (including biometric authentication and location authentication). User interaction with each of these icons/buttons teaches the “*interaction by a user with an icon*” as recited in the claim.



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

Accordingly, in Stone-Hoyos-Varghese, subsequent to a user interaction with an icon (which indicates any of the initiation, continuation, and confirmation of the user transaction request), and after user transaction request confirmation, contextual information comprising location data usable to determine a physical location associated with the user (e.g., determined through device IP address, GPS, or any other location-determining method) for fraud detection is captured, which renders obvious this element.

[1.3.2] [subsequent to an interaction...] capture a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images; and

Stone in view of Hoyos and Varghese renders this element obvious. APPL-1003, ¶¶121-131.

First, as discussed at [1.3.1], Stone teaches an interaction by a user with an icon rendered in the one or more interfaces.

Second, as shown in FIG. 1 of Hoyos below, Hoyos discloses capturing a set of biometric information for performing biometric authentication including fraud detection (including blocks 11 and 13 of FIG. 1) based thereupon. APPL-1003, ¶123; APPL-1013, [0017] (“a method of authenticating financial transactions comprising **acquiring biometric data from a person**, calculating probability of liveness, Pp. of the person and probability of a match, Pm. between the person and known biometric information...”).

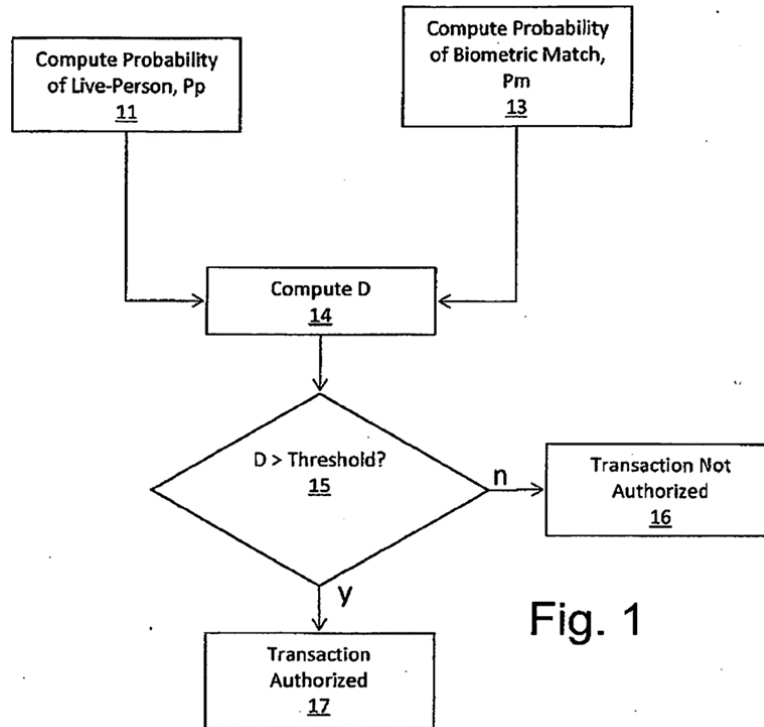


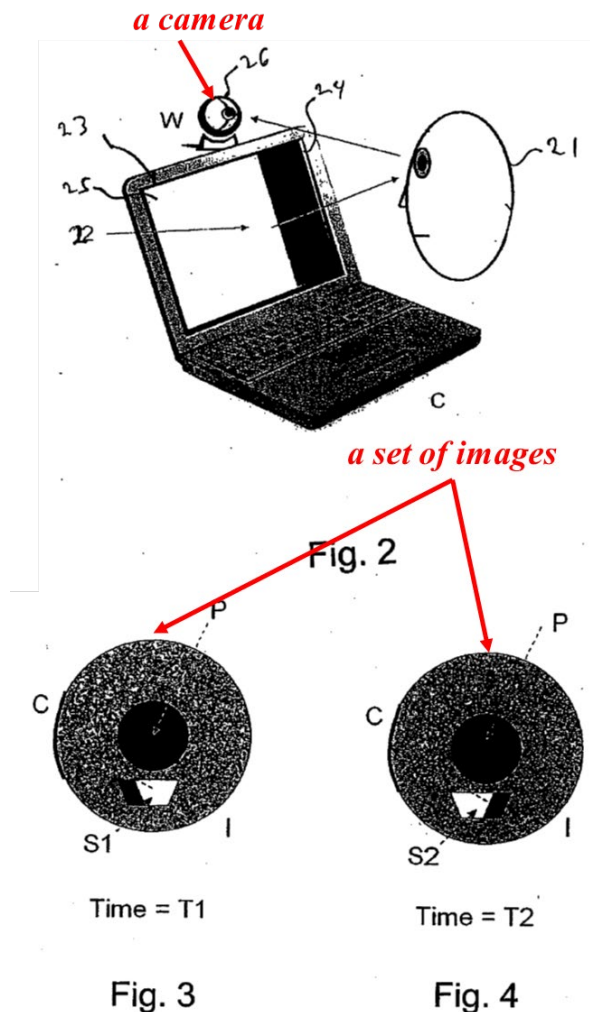
Fig. 1

APPL-1013, FIG. 1

Hoyos describes the biometric information include 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). APPL-1013, [0003], [0012], [0018]-[0022], [0040]; APPL-1003, ¶124 (it was well-known to capture a sequence of images (e.g., still or video) and use adjacent (successively captured) images/frames of a human face for liveness analysis); APPL-1011, Abstract; APPL-1012, Abstract.

As an example, and shown in annotated FIGS. 2, 3, and 4 of Hoyos below, Hoyos describes capturing the set of biometric information comprises capturing, using a camera (web-camera 26), a set of images (“obtaining first image of a user positioned in front of a computer screen from a first perspective; obtaining a

second image of the user positioned in front of the computer screen from a second perspective”). APPL-1013, claim 7; [0034] (referring to FIG. 2, describing capturing multiple images for calculating the probability of a live person); claims 5-8. While FIGS. 3 and 4 of Hoyos below illustrate only the eye portions, a POSITA would have understood that Hoyos captures images of a user’s face which includes the eye portions. APPL-1003, ¶125; APPL-1013, [0018]-[0020], claim 7.



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

Third, as shown in example Stone-Hoyos-Varghese below, a POSITA would have applied Hoyos’ teachings of biometric authentication including capturing biometric information (including capturing, using a camera, a set of images) in Stone for authenticating a user transaction request to provide improved authentication and fraud prevention for a user transaction request, with benefits of “improved deterrent against attempted fraudulent transactions, and decreased rejection of valid customers” as described in Hoyos, and together with applying Varghese’s multifactor authentication, Stone-Hoyos-Varghese provides multifactor authentication including location authentication (“something a person has”) and biometrics authentication. APPL-1003, ¶126; APPL-1013, [0015]; APPL-1010, [0035]; APPL-1008, [0004] (Stone describing user devices well-known to be easily connected to/include a camera for obtain photographs); APPL-1009, 15:22-23; APPL-1037, 10 (“Biometric identifiers are most commonly used as part of a multifactor authentication system” combined with “something a person knows” or “something a person has.”)

1013, Title, claim 1; APPL-1010, [0079]; APPL-1013, [0011]; *see also* IX.B.2: Combination of Stone and Hoyos.

For the reasons discussed at IX.B.2 and 3 and [1.3.1] above and shown in the example combination figure below, in Stone-Hoyos-Varghese, a POSITA would have been motivated to implement Hoyos' authentication process (capturing input images for liveness analysis and biometric comparison) after user transaction request confirmation, which is **at least after** a user interaction with an icon (e.g., user clicking the "\$Send money" icon of FIG. 2) to initiate the transaction request, and **after user interactions** with icons to continue (e.g., blocks 300-314) and confirm (e.g., block 316) the transaction request. APPL-1003, ¶129.

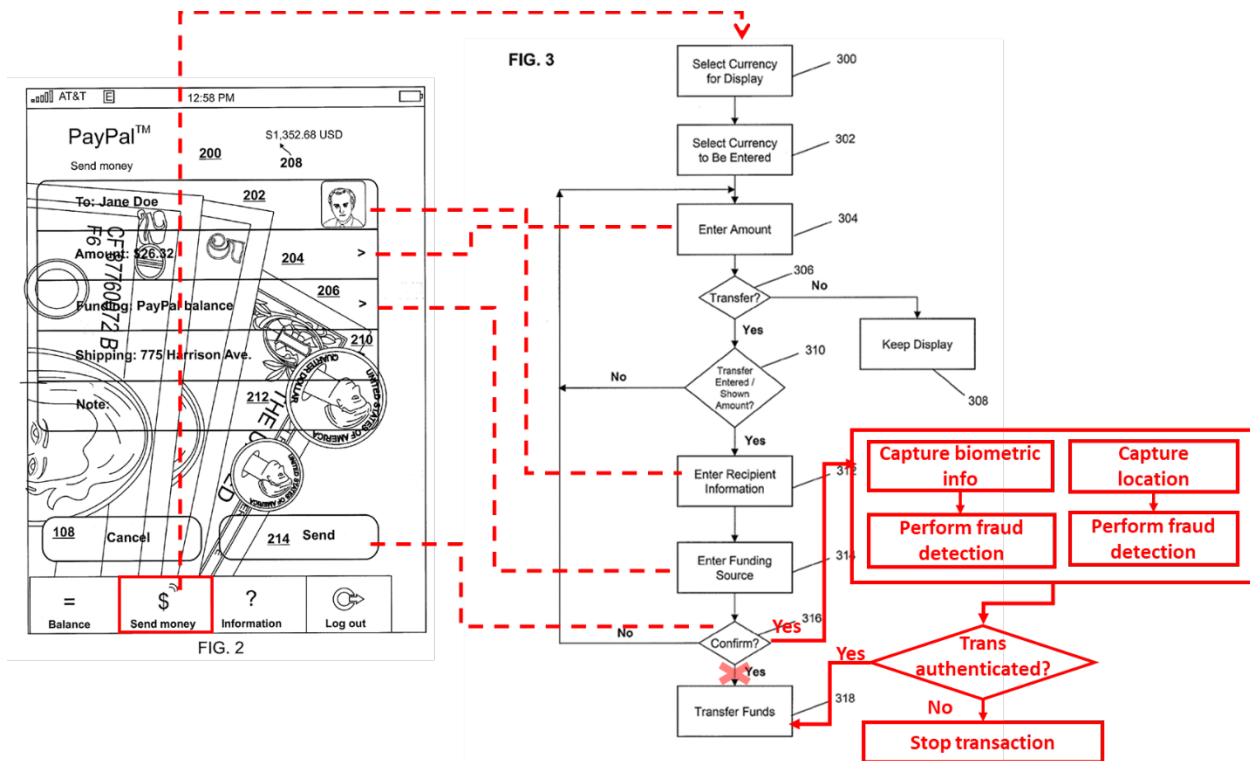
A POSITA would have understood that performing authentication including capturing authentication data (e.g., biometric information) after user transaction request confirmation had various benefits over the alternative design choice of using only previously captured authentication information before user transaction request confirmation, including enabling contextual authentication (e.g., capturing specific type of biometric/contextual data) for the specific transaction based on transaction information (e.g., type, amount) for improved fraud detection (APPL-1012, [0028]), capturing real-time, more accurate data that leads to more accurate and improved fraud detection and security (APPL-1010, FIG. 14, [0097]-[0099], TABLE 10), APPL-1015, FIG. 4). APPL-1003, ¶130.

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

[1.4.1] *facilitate a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed based at least in part on: the physical location associated with the user determined using the captured location data; and*

Stone in view of Hoyos and Varghese renders this element obvious. APPL-1003, ¶¶132-135.

First, in the combination, the user devices 404 capture information including location information and biometric information, and these captured information (e.g., location data usable to determine a physical location associated with the user, the set of biometric information including a set of images) are provided to facilitate a fraud detection analysis. As shown in the example Stone-Hoyos-Varghese below, the fraud detection analysis provides a decision regarding whether the transaction is authenticated/authorized, which teaches “*determine[ing] whether to allow an electronic transaction associated with the account holder to proceed*” as claimed. APPL-1003, ¶133; APPL-1013, FIG. 1, block 17 (“Transaction Authorized”); APPL-1016, FIG. 4, block 211 (“Transaction authenticated?”).



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

Second, as discussed at [1.3.1] and shown in annotated FIG. 14 of Varghese below, Varghese discloses facilitating and performing fraud detection analysis based at least in part on the physical location associated with the user determined using the captured location data. APPL-1010, [0088] (“More specifically, the risk scores output are **products of a number fraud detection inputs which are weighted and analyzed in real-time** using analytic processes customizable for **individual service providers**. **Fraud detection inputs** describe the user, the user’s device, **the location of the user’s device**,....”), [0012] (“certain geographic locations are known to contain an inordinate number of identity thieves.”).

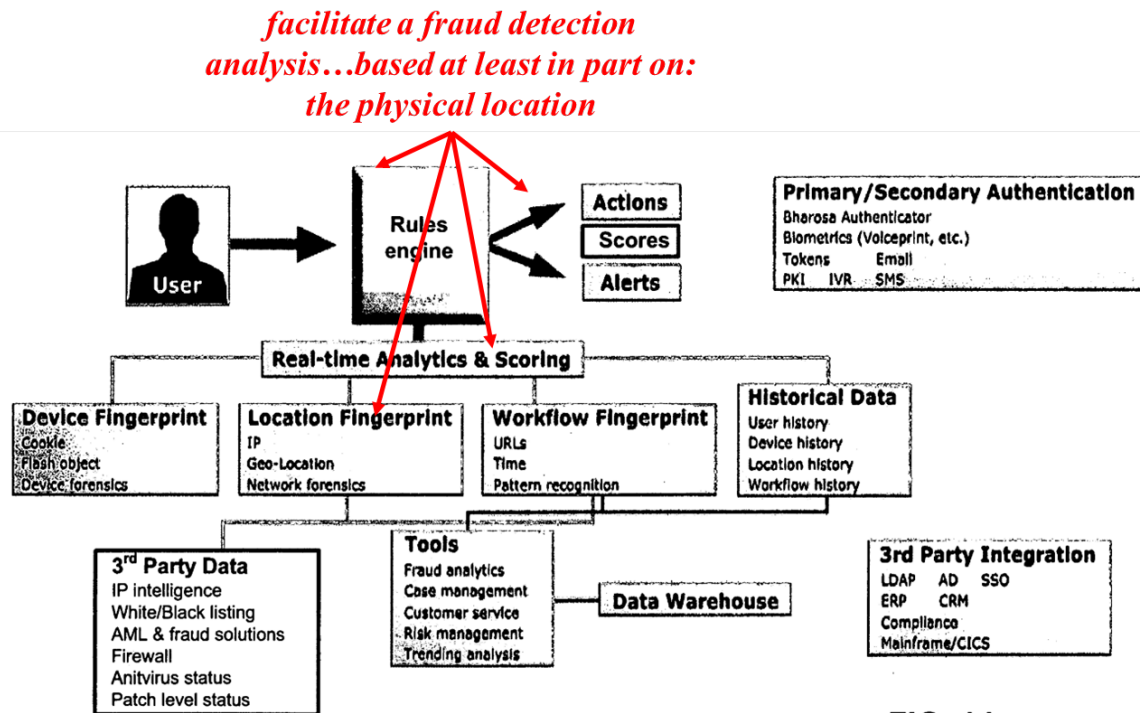


FIG. 14

APPL-1010, FIG. 14, annotated

As discussed at [1.3.1], in Stone-Hoyos-Varghese, a POSITA would have been motivated to apply Varghese’s teachings of real-time multifactor authentication including location authentication (e.g., evaluating fraud risk based on physical location determined from location data) in Stone for improved and more secure financial transactions. APPL-1003, ¶135 (citing APPL-1016, [0036], [0043] for the well-known knowledge to implement multifactor authentications, which “allows for increased authentication requirements” for increased security requirements, for example, “as the value of the transaction increases,” where location authentication is used for transactions with a large amount); IX.B.3.

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

***[1.4.2] [facilitate a fraud detection analysis...based at least in part on:...]
an analysis of the set of captured biometric information comprising a
determination of whether the user is alive based at least in part on an analysis of
the set of images captured using the camera; and***

Stone in view of Hoyos and Varghese renders this element obvious. APPL-1003, ¶¶136-142.

First, as discussed at [1.3.1], [1.3.2], and [1.4.1], Stone-Hoyos-Varghese teaches capturing contextual information and a set of captured biometric information, and facilitating a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed.

Second, as shown in FIG. 1 of Hoyos below, Hoyos discloses facilitating and performing fraud detection by performing an analysis of the set of captured biometric information. APPL-1003, ¶138; APPL-1013, [0017]-[0022] (describing fraud detection analysis (liveness based on images, finger or palm temperatures) and biometric match (biometric match including facial features, iris, fingerprint, finger vein, palm vein, etc.)), [0040], claims 1, 5-8.

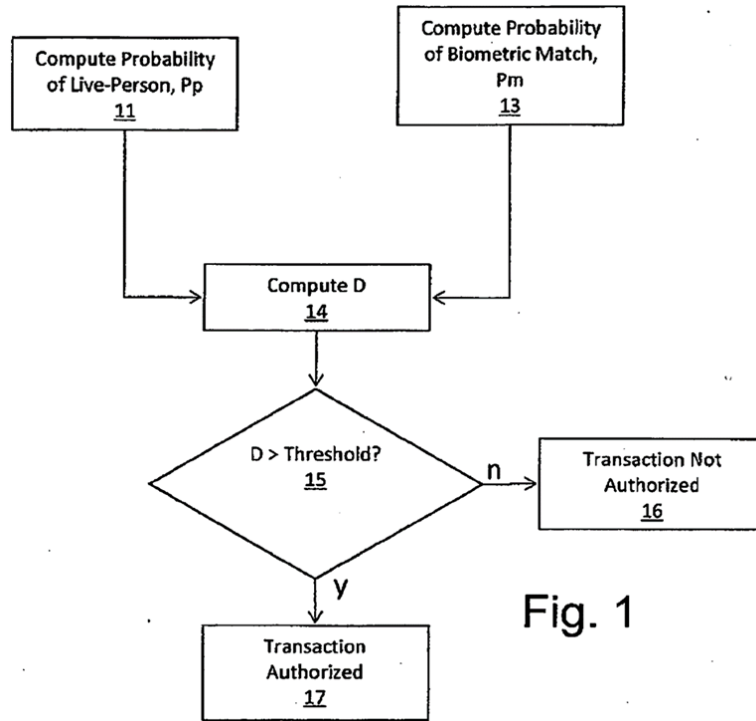
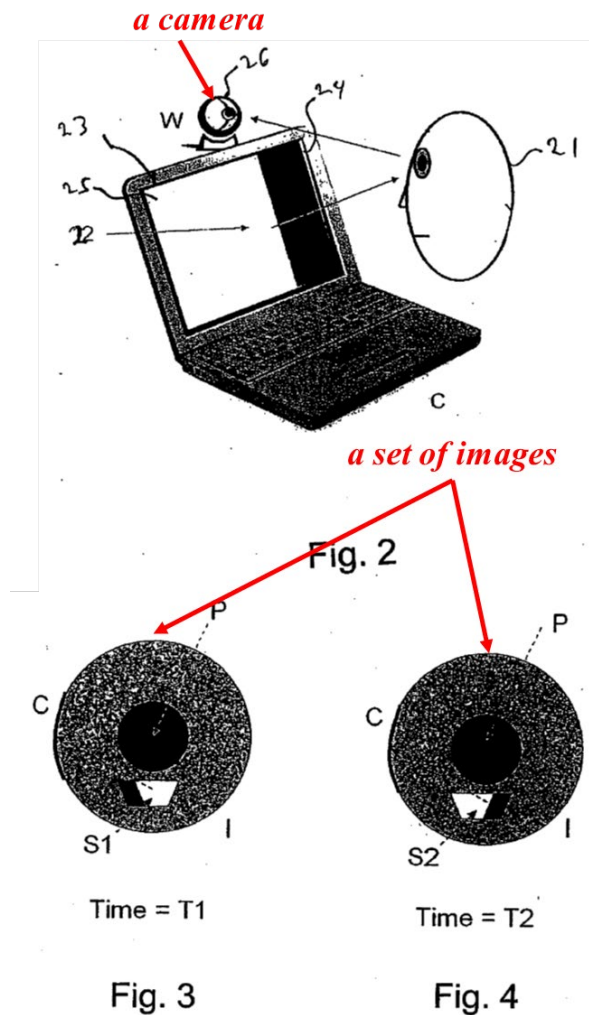


Fig. 1

APPL-1013, FIG. 1

Third, Hoyos describes that biometric authentication analysis (e.g., of FIG. 1) includes a determination of whether the user is alive based at least in part on an analysis of the set of images, including computing the probability, P_p of a live person being presented (e.g., block 11 of FIG. 1) based on analysis of the set of captured images (e.g., as described with reference to FIGS. 2-4). APPL-1003, ¶139; APPL-1013, FIG. 1. For example, [0019] and [0020] of Hoyos describe alternative techniques for determining whether a person is alive based on first and second user images captured by a computer. APPL-1013, [0019]-[0020]; APPL-1003, ¶139 (it was well-known to capture a sequence of images (e.g., still or video) and use adjacent (successively captured) images/frames of a human face for liveness analysis); APPL-1011, Abstract; APPL-1012, Abstract.

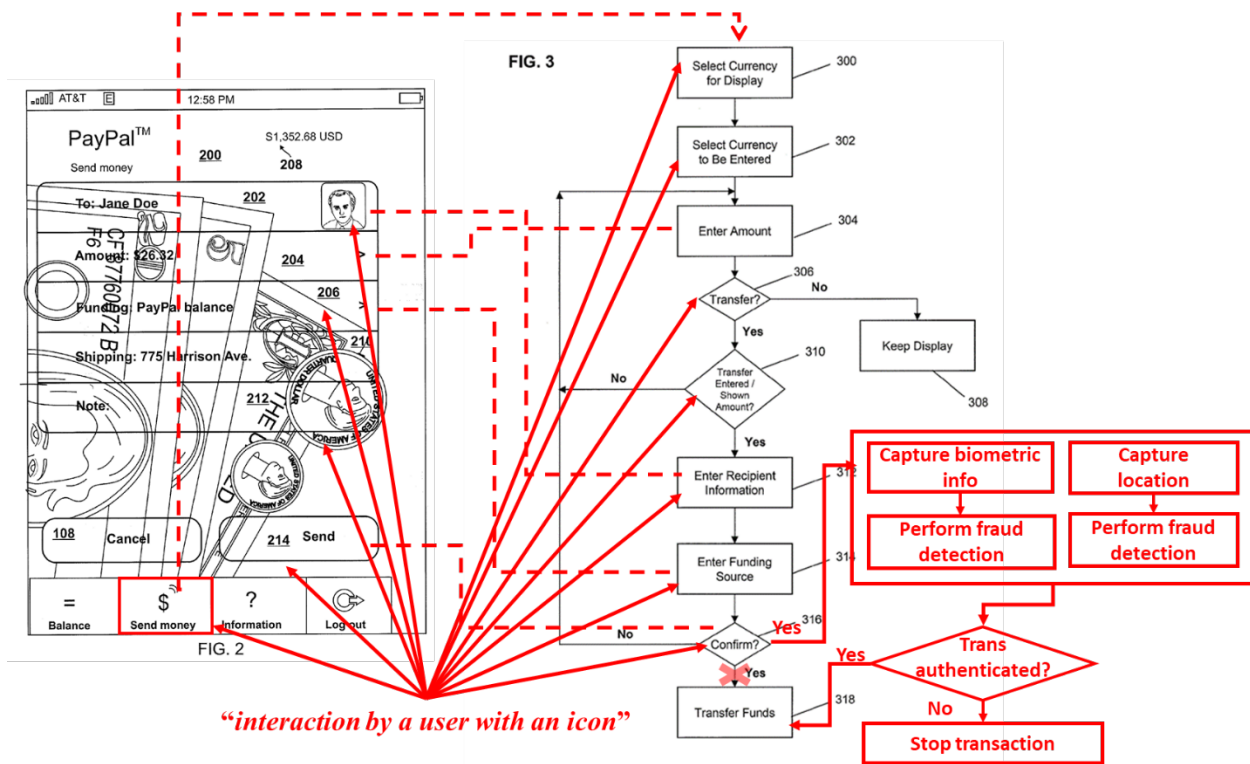
Referring to FIGS. 2, 3, and 4 below, Hoyos describes yet another example of determining whether a user is alive based on a set of captured images of the captured biometric information. APPL-1003, ¶140; APPL-1013, [0035]-[0037].



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

A POSITA would have applied Hoyos’ teachings of biometric authentication with fraud detection including liveness analysis based on the set of captured images in Stone-Hoyos-Varghese for improved authentication and fraud prevention, including the benefits of providing “biometric authentication systems

and methods for financial transactions for improved deterrent against attempted fraudulent transactions, and decreased rejection of valid customers” as described in Hoyos and multifactor authentication (with location authentication). APPL-1003, ¶141; APPL-1013, [0015]; APPL-1037, 9-10; *see also* IX.B.2-3, APPL-1008, [0045]; APPL-1010, [0079].



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

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

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

Stone discloses or renders obvious this element. APPL-1003, ¶¶143-146.

As discussed at [1.1], Stone discloses one or more processors (e.g., processor 504 in user device 404 alone, or in combination with other processors including the processor 504 of payment provider device 408) configured to perform processes for a transaction.

Stone further discloses a memory (memory component 506 of FIG. 5) coupled to a processor 504 in each device of the system including e.g., user devices 404, and the memory is configured to provide the processor with instructions (e.g., “instructions to create and display the proper currencies, convert currency, display various types of graphics showing transfer of currency, etc.”). APPL-1008, [0050] (“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-Hoyos-Varghese renders obvious claim 1.

5. Claim 2

[2.0] The system recited in claim 1, wherein the account holder comprises a recipient of the electronic transaction, and wherein the electronic transaction comprises a payment from the user to the account holder.

Stone discloses or renders obvious this element. APPL-1003, ¶¶147-149.

Specifically, as shown in annotated FIG. 2 of Stone below, Stone teaches that the account holder comprises a recipient of the electronic transaction, and wherein the electronic transaction comprises a payment from the user to the account holder. APPL-1008, [0024] (“display 200 has a **name box 202** indicating

the recipient of funds as well as a picture of the recipient,... and a send button 214 to transfer the funds in noted in box 204.”), see also APPL-1008, FIG. 3, [0035] (“the user confirms the transaction, such as by **tapping** an appropriate button, and the shown funds are **transferred to the desired recipient** in step 318”).

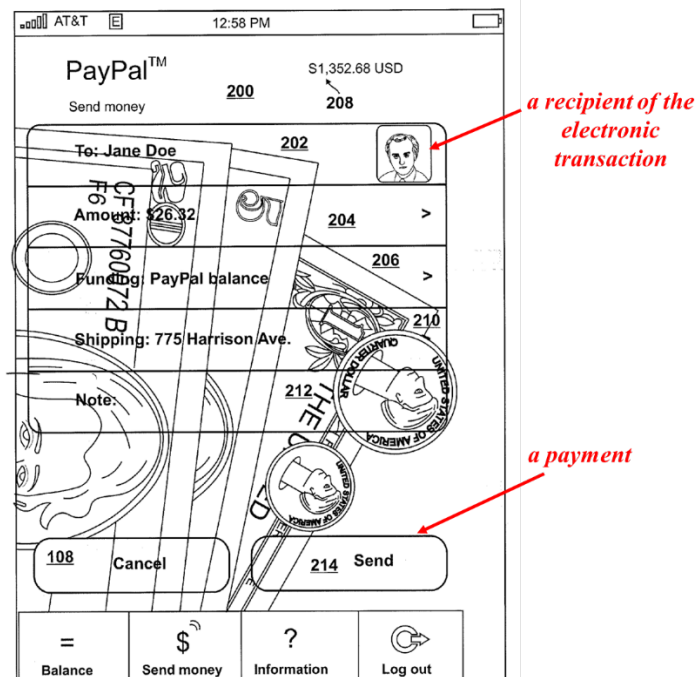


FIG. 2

APPL-1008, FIG. 2, annotated

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

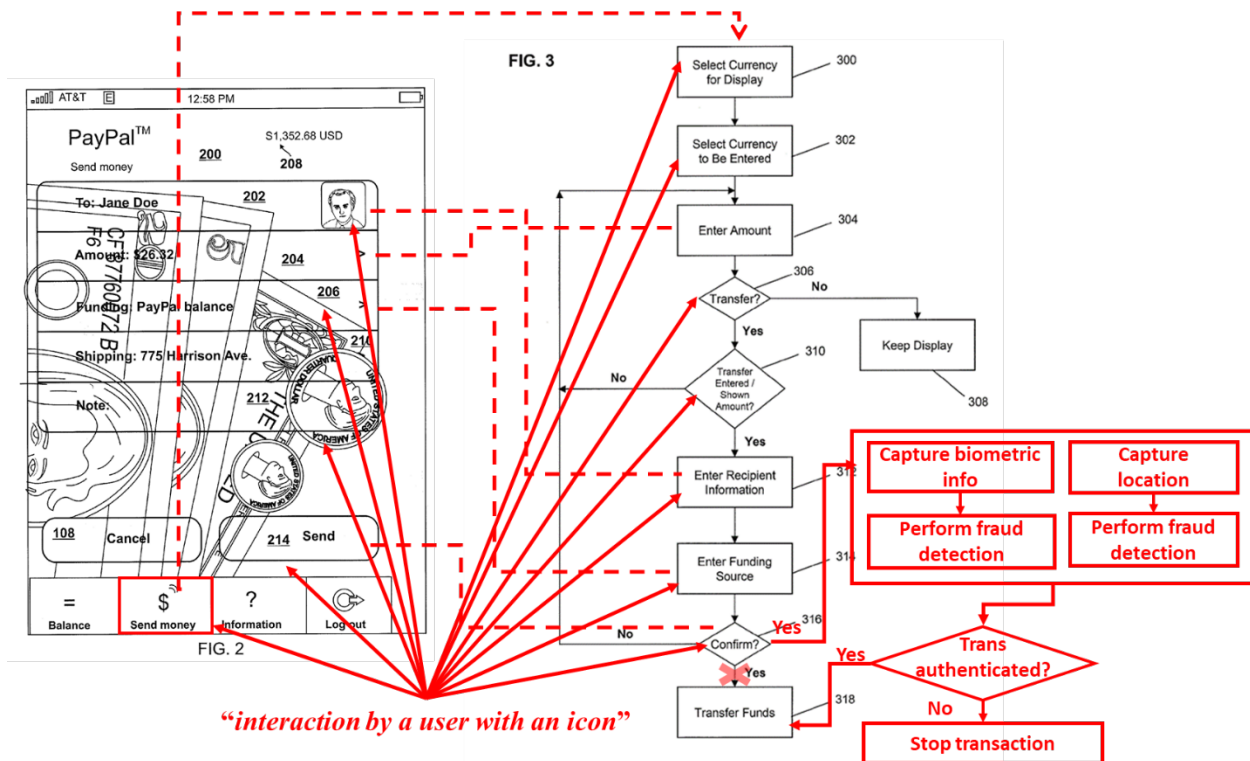
6. Claim 3

[3.0] The system recited in claim 1, wherein the icon represents a form of payment.

Stone discloses or renders obvious. APPL-1003, ¶¶150-154.

First, as discussed at [1.3.1] and shown in annotated example of Stone-Hoyos-Varghese, where each icon associated with user interaction blocks 300, 302,

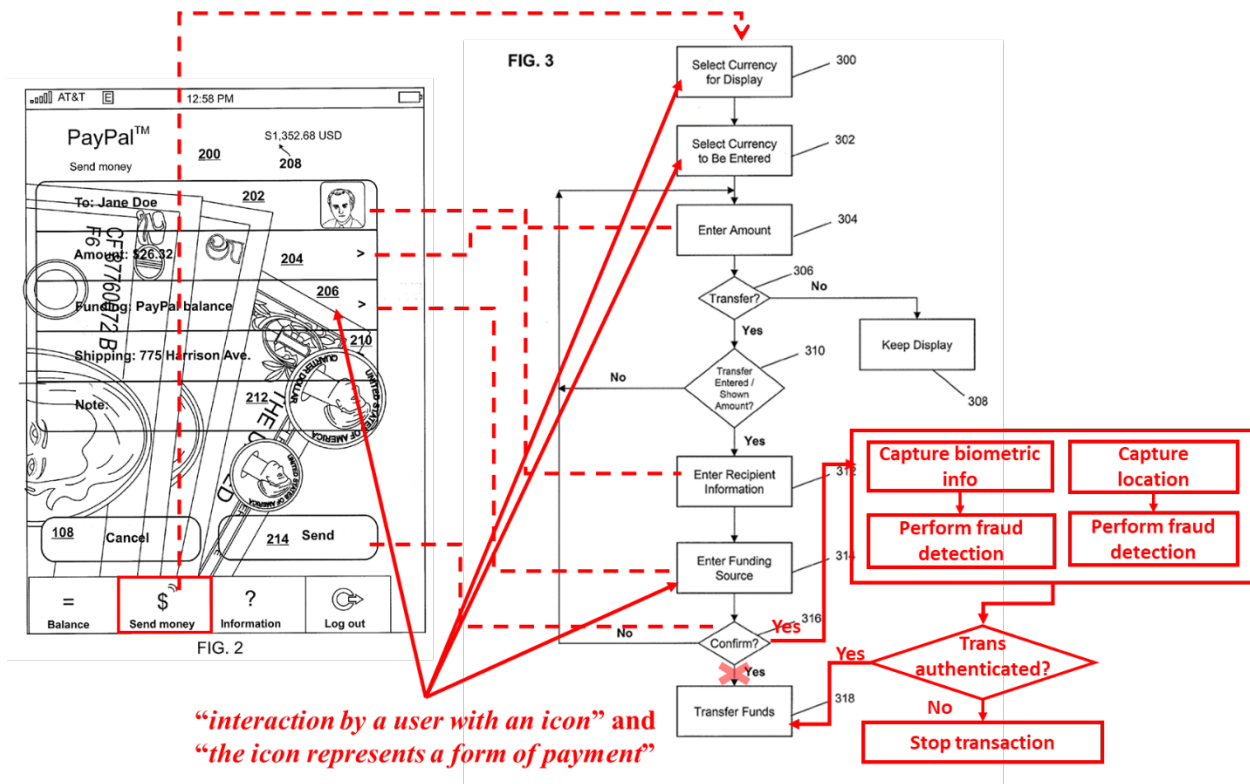
306, 312, 314, and 316) teaches the “*interaction by a user with an icon*,” as recited in [1.3.1].



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

Second, as shown in example of Stone-Hoyos-Varghese below, the icon “funding source box 206”/block 314 teaches that the icon represents a form of payment (“such as PayPal, a bank, a credit card, a debit card, etc.”), because Stone discloses clicking on that icon to make a transfer from a selected funding source. APPL-1008, [0034]; *see also* APPL-1008, [0004] (“The consumer typically clicks on **an icon or button** to make the transfer.”); APPL-1008, FIG. 2, [0024] (display including “a funding source box 206, indicating the source or account where the

user's funds will be transferred from.”). Furthermore, Stone describes that after the funding source is selected at step 314, “if the user still wants to proceed with the transfer, the user confirms the transaction, such as by **tapping** an appropriate button, and the shown funds are transferred to the desired recipient in step 318.” APPL-1008, [0035]. Further, Stone itself describes using a visual image to present the selected funding source in the display. APPL-1008, [0038] (“the display may show the specific card, such as a PayPal card, Visa, MC, AMEX, etc., **as contrasted to** a generic representation of a card or no visual at all.”). It would have been obvious to a POSITA to implement the funding source selection using an icon with the visual representation of the payment for improved visual presentation. APPL-1008, [0004] (recognizing that “icon” and “button” are alternative design choices); APPL-1003, ¶152.



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

Third, additionally, each icon associated with user action for blocks 300 (“Select Currency for Display”) and 302 (“Select Currency to be Entered”) teaches that the icon represents a form of payment, because a POSITA would have been motivated to use an icon of a form of payment (e.g., type of currency) to provide a visual indication to assist the user to select a currency at block 300 and/or 302.

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

7. Claim 4

[4.0] *The system recited in claim 1, wherein the image comprises at least one of a photograph or an avatar.*

Stone-Hoyos-Varghese renders obvious this element. APPL-1003, ¶¶155-

160.

The term “*the image*” in claim 4 lacks antecedent basis. Regardless of the lack of antecedent basis, the claim is rendered obvious by Stone-Hoyos-Varghese.

First, to the extent that “*the image*” is of “a set of images” of [1.3.2], Guidance describes that the set of captured images include a photograph of the user. APPL-1013, FIG. 2, [0034] (“an image from a web-camera 26 that the person 21 looks at is recorded”). APPL-1003, ¶157.

Second, to the extent that “*the image*” is “*a virtual likeness of a face*” of [1.2.1], Stone teaches that the image (e.g., shown on the currency or recipient icon) includes a photograph, as discussed in [1.2.1]. APPL-1008, [0007], [0024], [0020], [0036]; APPL-1003, ¶158.

Additionally, a POSITA would have been motivated to implement the virtual likeness in Stone-Hoyos-Varghese using an avatar, because an avatar and a photo were well-known alternative choices for the profile image. APPL-1003, ¶159; APPL-1009, 9:30-35.

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

8. Claim 5

[5.0] The system recited in claim 1, wherein the one or more interfaces are associated with at least one of a phone, a tablet device, or a laptop.

Stone discloses or renders obvious this element. APPL-1003, ¶¶161-163.

Specifically, Stone describes its system implementing user devices of different types (“mobile phone, laptop computer, PDA, or personal computer,” or “other suitable device”) for displaying the interfaces. APPL-1008, [0022], [0024], [0041], [0044], [0046].

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

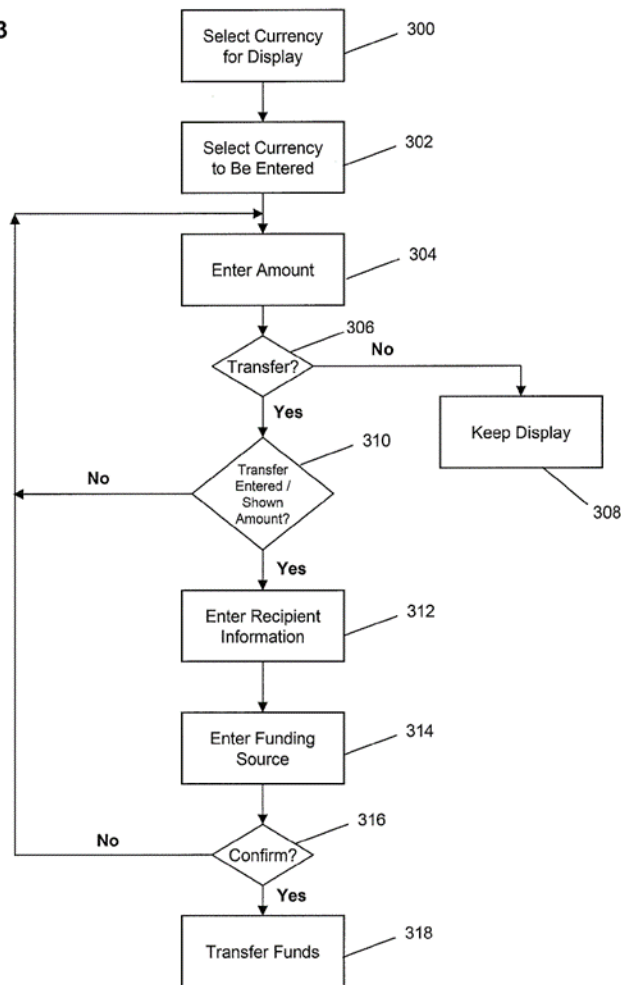
9. Claim 6

[6.0] A method, comprising:

Stone discloses or renders obvious the preamble to the extent that it is limiting. APPL-1003, ¶¶164-166.

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).

FIG. 3



APPL-1008, FIG. 3

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

[6.1.1]-[6.1.2]

Stone discloses or renders obvious these elements for reasons discussed at Ground 1: [1.2.1]-[1.2.2]. APPL-1003, ¶¶167-168.

[6.2.1]-[6.3.2]

Stone-Hoyos-Varghese renders obvious these elements for reasons discussed at Ground 1:[1.3.1]-[1.4.2]. APPL-1003, ¶¶169-172.

10. Claims 7, 8, 9, 10

Stone discloses or renders obvious the elements of these claims for reasons discussed at Ground 1: [2.0], [3.0], [4.0], [5.0] respectively. APPL-1003, ¶¶173-176. Accordingly, Stone-Hoyos-Varghese renders obvious these claims.

11. Claim 11

[11.0] 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, ¶¶117-119.

As discussed at [1.0], [1.1], and [1.5], Stone describes a system including one or more processors and a memory (*a non-transitory computer readable storage medium*) configured to provide the processors with instructions. In Stone, a computer program product is embodied in the memory and includes these instructions. APPL-1008, [0054] (“Software...such as program code and/or data, may be stored on one or more computer readable mediums”); APPL-1003, ¶178.

Therefore, Stone discloses or renders obvious this element.

[11.1.1]-[11.1.2]

Stone discloses or renders obvious these elements for reasons discussed at Ground 1:[1.2.1]-[1.2.2]. APPL-1003, ¶¶180-181.

[11.2.1]-[11.3.2]

Stone-Hoyos-Varghese renders obvious these elements for reasons discussed at Ground 1:[1.3.1]-[1.4.2]. APPL-1003, ¶¶182-185.

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

12. Claims 12 and 18

[12.0/18.0]...wherein the analysis of the set of images captured using the camera further comprises determining whether a face is detected in the captured set of images.

Stone-Hoyos-Varghese renders obvious this element. APPL-1003, ¶¶186-190.

Hoyos as applied in Stone-Hoyos-Varghese discloses that the analysis of the set of images includes determining whether a face is detected therein, because its authentication uses a face recognition match score. APPL-1003, ¶¶187-188 (citing APPL-1013, [0022], [0038] (“[u]sing the method described in Turk, et al., U.S. Pat. No. 5,164,992, **a face recognition match score, Pm**, is calculated”), claim 7; APPL-1017.

Additionally, to the extent that Patent Owner argues that Hoyos does not disclose face recognition, it would have been obvious to a POSITA to implement face recognition as an additional authentication technique in Stone-Hoyos-Varghese for improved security, where “the face biometric is easy to acquire (a web camera for example).” APPL-1003, ¶189; APPL-1013, [0007]; [0003]; APPL-1010, [0145]; APPL-1016, FIG. 4, [0042]; APPL-1037, 11.

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

13. Claims 14 and 20

[14.0/20.0] ...wherein the set of images comprises a plurality of images successively captured using the camera.

Stone-Hoyos-Varghese renders obvious this element. APPL-1003, ¶¶191-193.

As shown in FIGS. 3 and 4 of Hoyos below, Hoyos as applied in the combination describes that the set of images are successively captured using the camera at successive times T1 and T2, because a POSITA would have implemented the image captures to continue one after the other for improved spoofing, accuracy, and reduced delay in user experience. APPL-1013, [0036]; claims 5-8; [0018]-[0020]; APPL-1003, ¶192 (citing APPL-1011, Abstract; APPL-1012, Abstract).

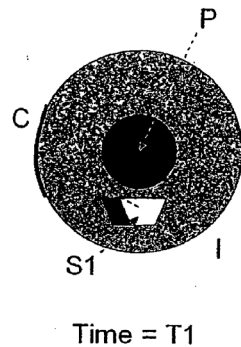


Fig. 3

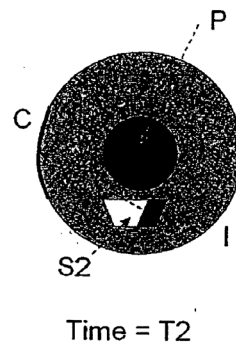


Fig. 4

APPL-1013, FIGS. 3 and 4

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

14. Claims 15 and 21

[15.0/21.0] ...wherein the set of captured biometric information further comprises an audio sample.

Stone-Hoyos-Varghese renders obvious this element. APPL-1003, ¶¶194-197.

First, as shown in annotated FIG. 14 of Varghese below, Varghese describes multifactor authentication including voice authentication, which includes capturing an audio sample. APPL-1010, FIG. 14, [0078]-[0079], [0084]; APPL-1033, FIG. 3.

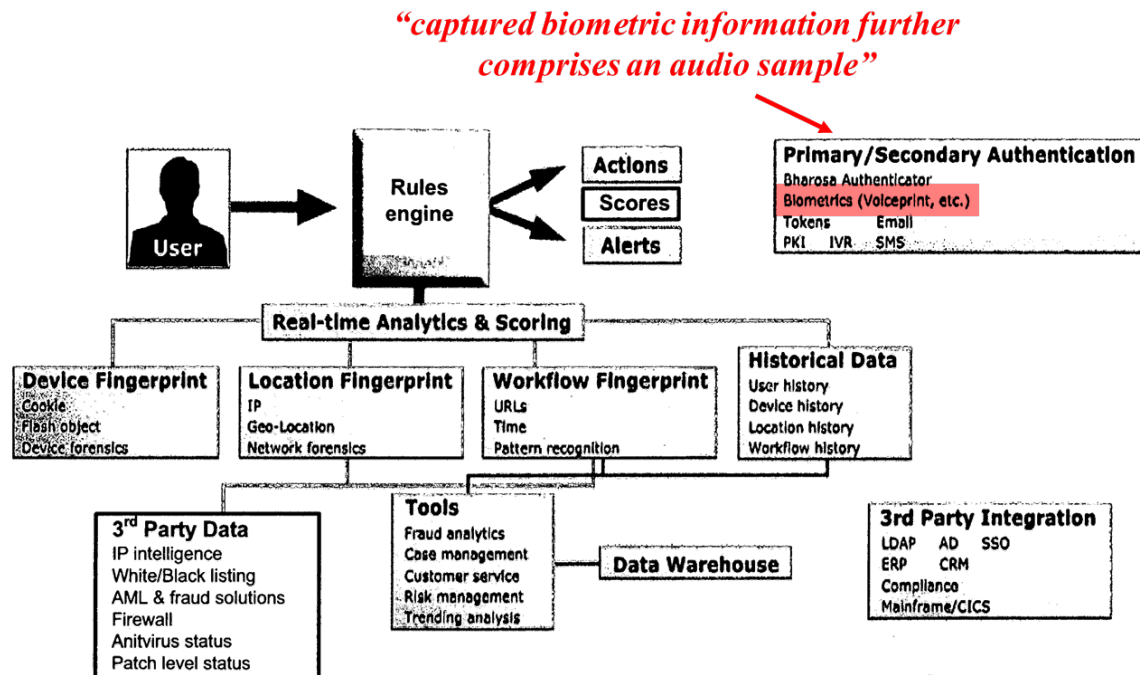


FIG. 14

APPL-1010, FIG. 14, annotated

Second, a POSITA would have been motivated to implement the multifactor authentications with an additional voice authentication for improved security based on assessed risk of a transaction. APPL-1003, ¶196; APPL-1010, [0145]; APPL-

1018, 51:12-15, 52:20-24; APPL-1016, FIG. 4, [0036], [0040]-[0041]; IX.B.3.

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

15. Claims 16 and 22

[16.0/22.0] ...wherein facilitating the fraud detection analysis...is further based at least in part on a determination of whether the audio sample matches a previously recorded voice sample.

Stone-Hoyos-Varghese renders obvious this element. APPL-1003, ¶¶198-201.

It is fundamental and basic knowledge that biometric authentication (including voice authentication) makes an accept/reject decision based on a determination of whether there is a match between a captured sample (e.g., a voice sample) and a previously captured reference (e.g., a previously recorded voice sample), and thus Stone-Hoyos-Varghese's voice authentication renders obvious this limitation. APPL-1003, ¶¶199-200; APPL-1010, [0145], APPL-1016, [0036], [0040]-[0041]; APPL-1018, 51:12-15; APPL-1033, FIG. 3.

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

16. Claims 17 and 23

[17.0/23.0] ...wherein the determination of whether the audio sample matches the previously recorded voice sample is based at least in part on performing a Fast Fourier Transform.

Stone-Hoyos-Varghese renders obvious this element. APPL-1003, ¶¶202-204.

It is fundamental and basic knowledge that a well-known technique for matching audio samples voice authentication determines whether audio samples match based on performing FFT, because FFT is a fundamental, highly efficient tool for converting the time-domain audio signal into the frequency domain for comparing frequency domain features of the audio samples. APPL-1003, ¶203; APPL-1033, 1445 (describing using FFT for frequency feature extraction for speaker recognition); APPL-1031, 12:15-19 (describing using FFT for feature extraction for speaker recognition); (Bilobrov) APPL-1032, FIG. 2 (illustrating using FFT for voice fingerprint).

Accordingly, building on Stone-Hoyos-Varghese analysis for claims 16/22, and in view of POSITA's fundamental and basic knowledge of using FFT for speaker recognition, it would have been obvious to determine whether the audio samples match based on performing an FFT, which renders obvious claims 17/23. APPL-1010, [0145]; APPL-1003, ¶204.

C. Ground 2: Claims 1-12, 14-18, and 20-23 are Rendered Obvious under §103(a) over Stone-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, ¶205.

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 regardless of whether they are subject to FFIEC supervision, and the additional benefits of FFIEC compliance for federal supervised financial institutions. APPL-1003, ¶¶206-209.

First, as discussed at IX.A.5, Guidance is analogous art to the ’886 patent. APPL-1003, ¶207.

Second, Guidance “addresses why financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services,” and provides “improved authentication technologies” for reducing fraud and identity theft and improving customer protection, even for service providers of financial transactions not regulated by FFIEC. APPL-1037, 1; APPL-1003, ¶208 (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 multifactor authentication by a POSITA as shown in numerous articles and patent disclosures. *See, e.g.*, APPL-1013, [0009], [0011]; APPL-1010, [0148]; APPL-1016, FIG. 3, [0073]); APPL-1003, ¶52 (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).

Third, 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, ¶209 (citing APPL-1039, 1; APPL-1008, [0041]-[0042]). It was with a POSITA's level of skill in the art to select from various authentication factors/techniques for the multifactor real-time authentication based the assessed risk associated with a particular electronic transaction. APPL-1003, ¶209; APPL-1037, 8; APPL-1016, [0036]. Additionally, a POSITA would have understood to implement the enrollment phase during user registration in Stone to capture high-confidence enrollment data, and implement the authentication phase of transaction authentication (e.g., for authenticating a specific transaction request, capturing biometric data and location and performing fraud analysis thereupon) after user initiates and confirms a transaction request in Stone (e.g., by selecting transaction icons), for providing risk-based authentication adaptive to the risk of

the transaction (e.g., based on transaction type and/or amount). APPL-1003, ¶209.

2. Claim 1

[1.0]

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, ¶210.

[1.1] *one or more processors configured to:*

Stone alone or Stone-Guidance renders obvious this element. APPL-1003, ¶¶211-214.

First, Stone renders obvious this element for the reasons discussed at Ground 1:[1.1].

Second, as discussed below at Ground 2:[1.2.1]-[1.4.2], Stone alone or in combination with Guidance teaches [1.2.1]-[1.4.2], and a POSTA would have understood to modify Stone such that the one or more processors are configured to perform the processes including [1.2.1]-[1.4.2], for initiating, authenticating, and completing the electronic transaction. APPL-1003, ¶213.

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

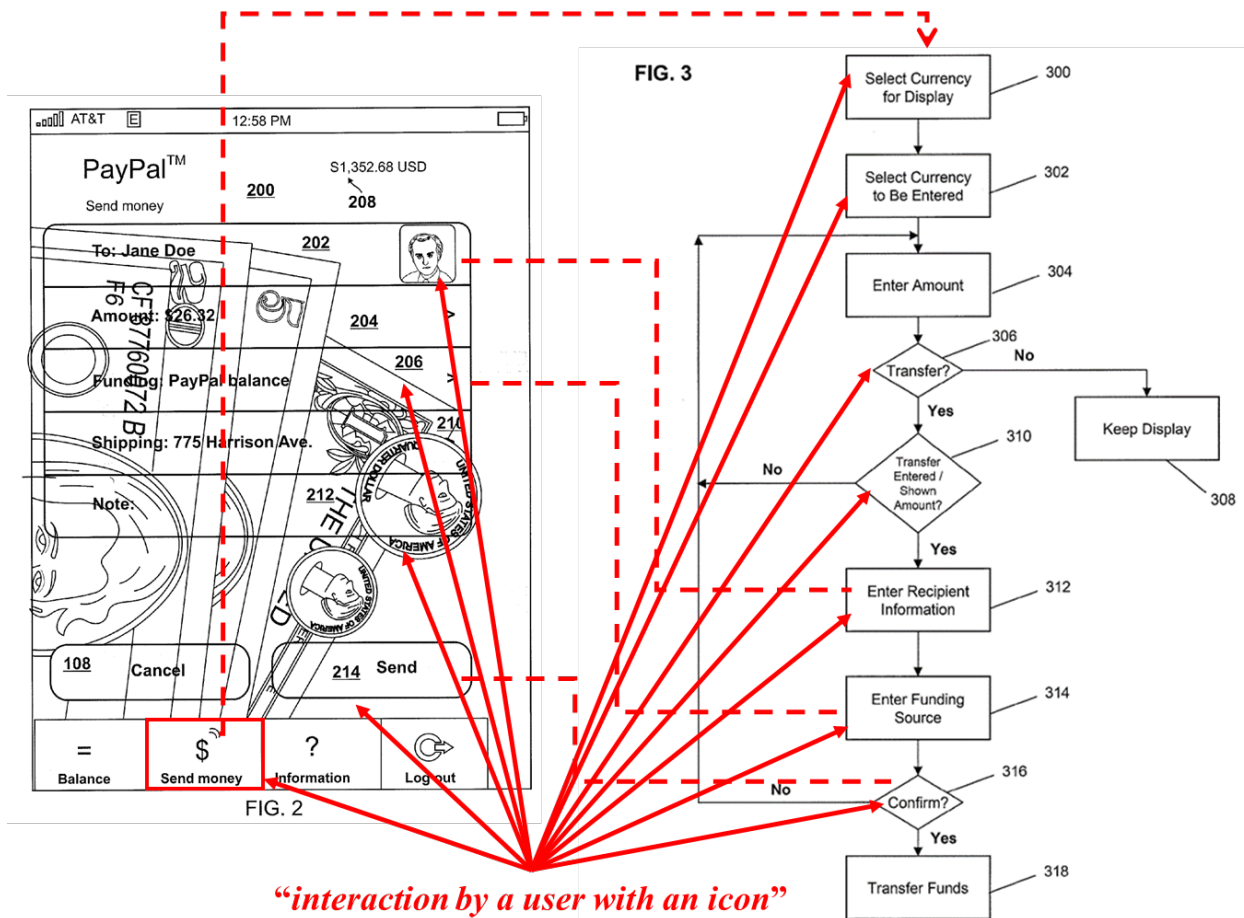
[1.2.1]-[1.2.2]

Stone discloses or renders obvious this element for the reasons discussed at Ground 1:[1.2.1]-[1.2.2]. APPL-1003, ¶¶215-216.

[1.3.1] subsequent to an interaction by a user with an icon rendered in the one or more interfaces: capture contextual information comprising location data usable to determine a physical location associated with the user; and

Stone-Guidance renders this element obvious. APPL-1003, ¶¶217-226.

First, as discussed at Ground 1:[1.3.1], and shown in annotated FIGs. 2 and 3 of Stone below, in Stone, each of the annotated control elements/blocks (e.g., “\$Send money,” 202, 206, 214, personalized currency, blocks 300, 302, 306, 312, 314, and 316) and other control elements (e.g., “Send,” “Confirm,” or “Proceed” described in Stone) teaches an interaction by a user with an icon rendered in the one or more interfaces (e.g., interface 200) as claimed.



APPL-1008, FIGS. 2 and 3, annotated

Second, Guidance describes multifactor real-time authentication including location authentication and biometric authentication, and location authentication teaches capturing contextual information including location data usable to determine a physical location associated with the user. APPL-1003, ¶219.

Specifically, 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

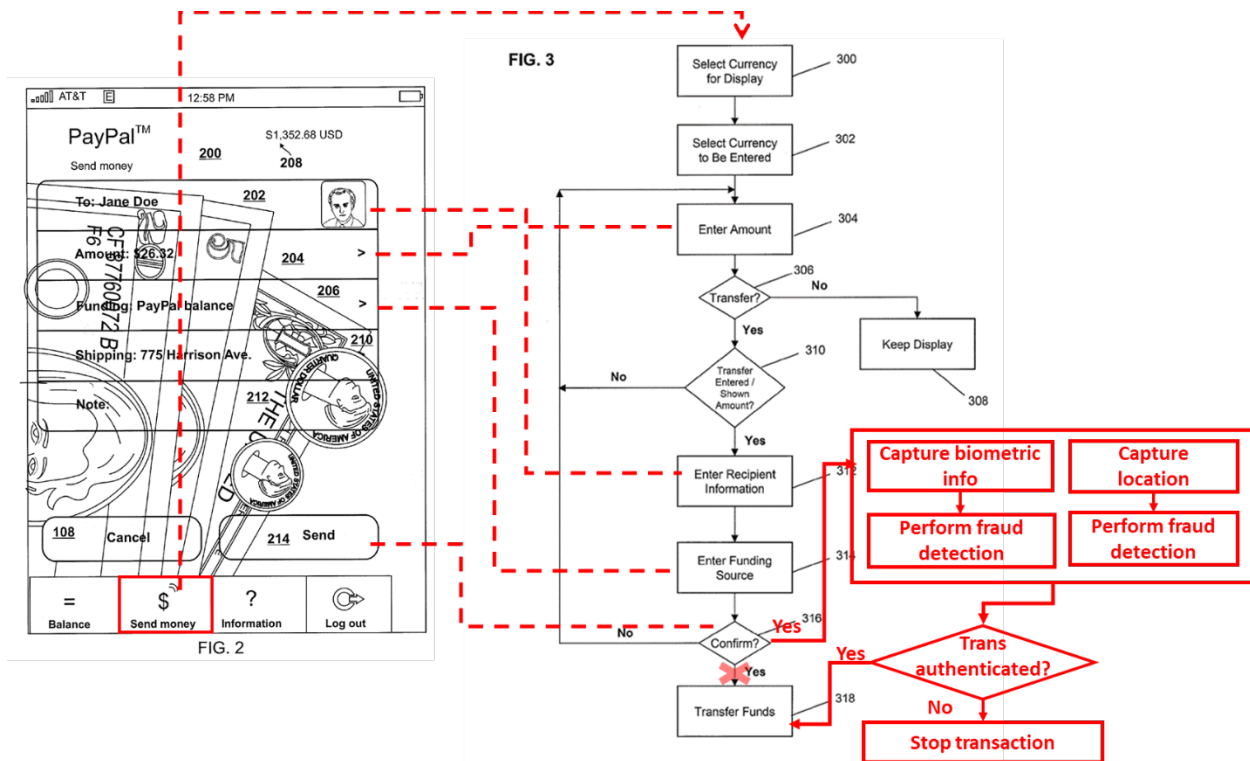
recognition (“Something a person is”/“something you are”) with testing for liveness, based on the risk of the transaction. APPL-1003, ¶220; APPL-1037, 3, 11-12; (Varghese), APPL-1010, [0035].

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, ¶221; APPL-1010, [0012], [0035]; APPL-1016, [0043]). Furthermore, biometrics 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-1013, [0007]; APPL-1037, 11.

Guidance’s physical location authentication teaches capturing real-time location data usable to determine a physical location associated with the user. APPL-1037, 12. In Stone-Guidance, a POSITA would have been motivated to

apply suitable well-known techniques (e.g., Geolocation by IP address, GPS for mobile phone, etc.) for capturing location data for various user devices using various communication networks. APPL-1003, ¶222 (citing APPL-1037, 12-13; APPL-1010, [0140]; APPL-1016, [0036]; APPL-1008, [0026]).

Third, 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-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. This has various benefits over the alternative design choice of using a previously captured and stored data (e.g., for liveness analysis or for comparison with the enrollment data), including enabling contextual authentication adaptive for the specific transaction based on

transaction information (e.g., type, amount) for improved fraud detection (APPL-1010, FIG. 14, [0091], TABLE 10, APPL-1016 [0043]), providing more accurate and updated real-time information for real-time authentication (APPL-1010, [0148]; APPL-1015, FIG. 4), and performing fraud analysis based on location match (e.g., between locations captured before and after confirmation at 316) for improved security. It was well-known to provide higher level authentication for higher risk transactions (e.g., a \$10,000 transfer request with a higher risk than a \$10 transfer request. APPL-1037, 3-4 (describing risk-based authentication including evaluating risks in light of customer transaction capabilities, transaction types (e.g., bill payment, wire transfer, loan origination)).

Accordingly, in Stone-Guidance, subsequent to an interaction by a user 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 including location data usable to determine a physical location associated with the user as taught in Guidance.

Accordingly, Stone-Guidance renders obvious this element.

[1.3.2] [subsequent to an interaction...] capture a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images; and

Stone-Guidance renders this element obvious. APPL-1003, ¶¶227-230.

First, as discussed at Ground 2:[1.3.1], Stone-Guidance teaches performing multifactor real-time authentication including both physical location authentication and biometric authentication using face recognition with liveness tests subsequent to an interaction by a user with an icon.

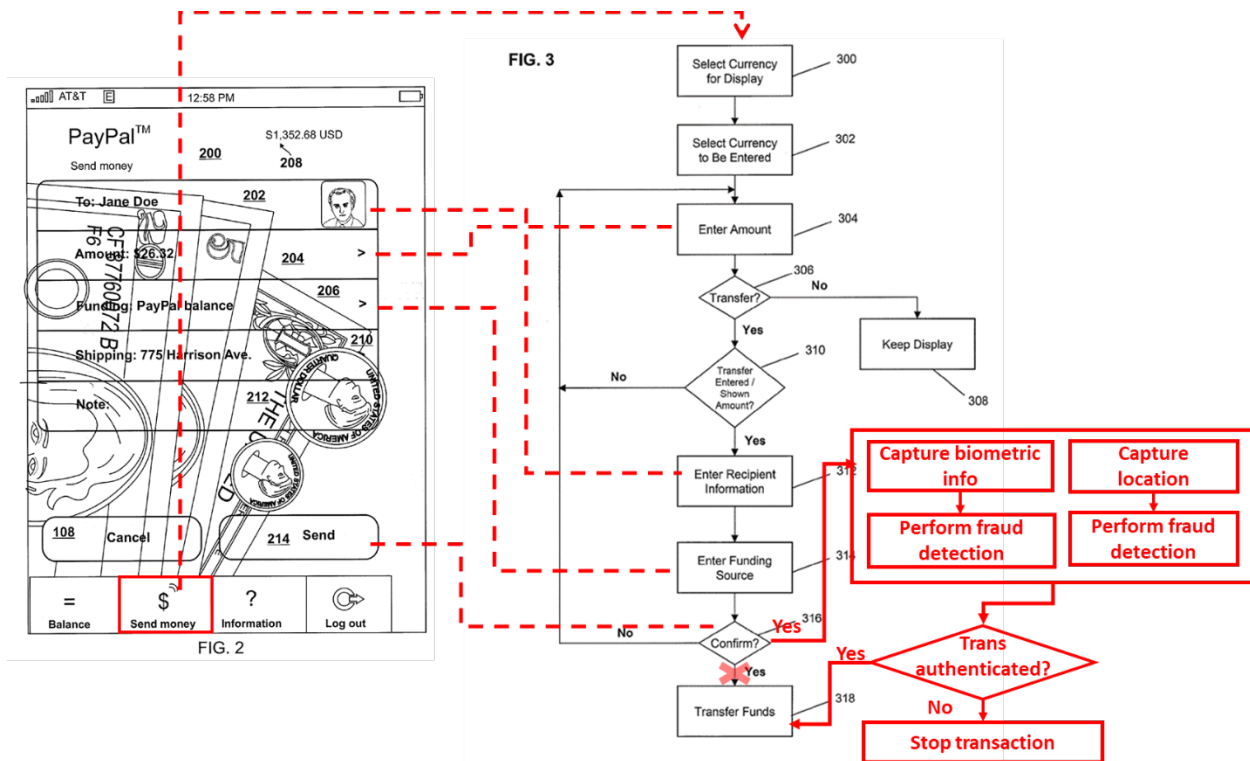
Second, Guidance's face recognition with liveness tests teaches capturing the set of biometric information comprises capturing, using a camera, a set of images. Specifically, Guidance describes that biometric authentication using face recognition with liveness tests using facial scans captured by a camera (e.g., a still camera to capture a sequence of images at different times, a video camera to capture a video with subsequent frames, each frame being an image), and the facial scans are analyzed for "**tests for liveness**, such as blinking eyes." APPL-1037, 11. Indeed, it was well-known in the art to use a plurality of images captured using a camera (still or video) to perform liveness test (e.g., based on blinking eyes or other liveness tests). APPL-1003, ¶229; APPL-1044, 2; APPL-1013, FIGs. 2-4, claims 5-6; APPL-1011, Abstract; APPL-1012, Abstract.

Therefore, Stone-Guidance renders obvious this element.

[1.4.1] *facilitate a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed based at least in part on: the physical location associated with the user determined using the captured location data; and*

Stone-Guidance renders this element obvious. APPL-1003, ¶¶231-235.

First, Stone-Guidance teaches facilitating a fraud detection analysis to determine whether to allow an electronic transaction associated with the account holder to proceed, by providing a decision based on the fraud detection analysis about whether to complete the electronic transaction by performing transferring funds at 318 of FIG. 3 of Stone. APPL-1037, 4-6 (describing transaction authentication for an electronic transaction including “movement of funds” and “bill payment”). As shown in the example Stone-Guidance below, the fraud detection analysis provides a decision regarding whether the electronic transaction is authenticated/authorized, which teaches “*to determine whether to allow an electronic transaction associated with the account holder to proceed*” as claimed. APPL-1003; APPL-1016, FIG. 4, block 211 (“Transaction authenticated?”); see also APPL-1013, FIG. 1, block 17 (“Transaction Authorized”).



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

Second, Guidance’s physical location authentication further describes facilitating a fraud detection analysis based on the determined physical location associated with the user (where the physical location is determined using the captured location data as discussed at Ground 2:[1.3.1]).

For location authentication, Guidance describes authentication based on “geo-location technology” to “limit Internet users by determining where they are.” APPL-1037, 12. It was well-known that geo-location technology captures location data (e.g., IP address and other associated network information) for determining the physical location of the user. *See, e.g.*, APPL-1010, [0140] (“Geolocation by IP address is a technique of determining the geographic latitude and longitude

corresponding to a user by comparing the user's IP address with known locations of other nearby servers and routers.”). Furthermore, various technologies for capturing location data were well-known, including e.g., geo-location using IP address and network data, “GPS” location data. APPL-1003, ¶234 (citing APPL-1016, [0036]; APPL-1008, [0026] (describing that detection of the location of the user “may be determined through GPS or any other location-determining method” by using GPS location data)).

Therefore, Stone-Guidance renders obvious this element.

[1.4.2] [facilitate...based at least in part on:...] an analysis of the set of captured biometric information comprising a determination of whether the user is alive based at least in part on an analysis of the set of images captured using the camera; and

Stone-Guidance renders this element obvious. APPL-1003, ¶¶236-239.

Specifically, Guidance describes that in biometric authentication, face recognition systems use facial images from a camera with “tests for **liveness**, such as blinking eyes.” APPL-1037, 11. Techniques for liveness tests based on a plurality of facial images from a camera (still or video camera) were wellknown. APPL-1003, ¶237 (citing APPL-1044, 2; APPL-1013, FIGs. 2-4, claims 5-6; APPL-1011, Abstract; APPL-1012, Abstract).

A POSITA would have been motivated to apply the face recognition with liveness test in the multifactor real-time authentication as applied in Stone-Guidance because “Testing for liveness reduces the chance that the person

requesting access is using a photograph of an authorized individual.” APPL-1037, 11. APPL-1003, ¶238.

Therefore, Stone-Guidance renders obvious this element.

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

Stone discloses or renders obvious this element for reasons discussed at Ground 1:[1.5]. APPL-1003, ¶239. Accordingly, Stone-Guidance renders obvious claim 1.

3. Claims 2-3

Stone discloses or renders obvious these claims for the reasons discussed at Ground 1:[2.0]-[3.0]. APPL-1003, ¶¶240-241.

4. Claim 4

[4.0] ...wherein the image comprises at least one of a photograph or an avatar.

Stone-Guidance renders obvious this element. APPL-1003, ¶¶243-248.

The term “*the image*” in claim 4 lacks antecedent basis. Regardless of the lack of antecedent basis, the claim is rendered obvious by Stone-Guidance.

First, to the extent that “*the image*” is of “a set of images” of [1.3.2], as discussed at [1.3.2], Guidance describes capturing a set of images using a camera (e.g., still or video camera) to capturing facial scans, which teaches that the set of captured images include a photograph of the user. APPL-1037, 11; APPL-1003, ¶245.

Second, to the extent that “*the image*” is “*a virtual likeness of a face*” of [1.2.1], Stone teaches that the image (e.g., shown on the currency or recipient icon) includes a photograph, as discussed in Ground 1: [1.2.1]. APPL-1003, ¶246 (citing APPL-1008, [0007], [0024], [0020], [0036]).

Additionally, a POSITA would have been motivated to implement the virtual likeness in Stone using an avatar, because an avatar and a photo were well-known alternative choices for the profile image. APPL-1003, ¶247; APPL-1009, 9:30-35.

Therefore, Stone-Guidance renders obvious this claim.

5. Claim 5

[5.0]...wherein the one or more interfaces are associated with at least one of a phone, a tablet device, or a laptop.

Stone renders obvious this element. APPL-1003, ¶¶249-252.

Stone teaches this element for reasons discussed Ground 1: [5.0]. APPL-1003, ¶250.

Further, in Stone-Guidance, a POSITA would have been motivated to use location authentication method suitable for the specific type of user device, e.g., GPS for capturing location for a user device implemented as a mobile phone. APPL-1003, ¶251 (citing APPL-1037, 12-13; APPL-1008, [0026]; APPL-1016, [0036]).

Therefore, Stone-Guidance renders obvious this claim.

6. Claim 6

[6.0]-[6.1.2]

Stone discloses or renders obvious [6.0]-[6.1.2] for reasons discussed at Ground 1:[6.0], [1.2.1]-[1.2.2]. APPL-1003, ¶¶252-254.

[6.2.1]-[6.3.2]

Further, Stone-Guidance renders obvious [6.2.1]-[6.3.2] for reasons discussed at Ground 2:[1.3.1]-[1.4.2]. APPL-1003, ¶¶255-258.

Therefore, Stone-Guidance renders obvious this claim.

7. Claims 7, 8, 9, 10

Stone discloses or renders obvious elements of these claims for reasons discussed at Ground 2:[2.0], [3.0], [4.0], [5.0]. APPL-1003, ¶¶259-262.

Therefore, Stone-Guidance renders obvious these claims.

8. Claim 11

[11.0]-[11.1.2]

Stone discloses or renders obvious these elements for reasons discussed at Ground 1:[11.0], [1.2.1], and [1.2.2]. APPL-1003, ¶¶263-265.

[11.2.1]-[11.3.2]

Stone-Guidance renders obvious these elements for reasons discussed at Ground 2:[1.3.1]-[1.4.2]. APPL-1003, ¶¶266-269.

Accordingly, Stone-Guidance renders obvious this claim.

9. Claims 12 and 18

[12.0/18.0]...wherein the analysis of the set of images captured using the camera further comprises determining whether a face is detected in the captured set of images.

Stone-Guidance renders obvious this element. APPL-1003, ¶¶271-273.

As discussed at Ground 2: [1.3.1]-[1.4.2], Stone-Guidance implements multifactor authentication including face recognition with liveness test, where face recognition teaches detecting a face in the captured set of images. APPL-1037, 10 (describing detecting a face by “focus[ing] on specific features on the face”); APPL-1017; APPL-1003, ¶272.

Therefore, Stone-Guidance renders obvious this claim.

10. Claims 14 and 20

[14.0/20.0]...wherein the set of images comprises a plurality of images successively captured using the camera.

Stone-Guidance renders obvious this element. APPL-1003, ¶¶274-276.

As discussed at Ground 2:[1.3.2], Guidance as applied in Stone-Guidance describes that the face recognition with liveness tests using facial scans (a set of images) captured by a camera that is “a video device.” Thus, Guidance teaches that the set of images for liveness test include a plurality of images (frames of a video) successively captured using the video camera device. APPL-1037, 11. This is consistent with the well-known knowledge that a plurality of successively captured images using a camera (still or video) are used to perform liveness test (e.g., based

on blinking eyes or other liveness tests). APPL-1003, ¶275 (citing APPL-1044, 2, APPL-1011, Abstract; APPL-1012, Abstract); APPL-1013, FIGS. 2-4 (*see* Ground 1: Claims 14-20).

Accordingly, Stone-Guidance renders obvious this claim.

11. Claims 15 and 21

[15.0/21.0]...wherein the set of captured biometric information further comprises an audio sample.

Stone-Guidance renders obvious this element. APPL-1003, ¶¶278-281.

Guidance describes multifactor authentication including “voice authentication,” which includes capturing results with a “live-scan process” and comparing the results (captured audio sample) with the registered templates in the system. APPL-1003, ¶¶279; APPL-1037, 7-10; APPL-1033, FIG. 3.

In Stone-Guidance, a POSITA would have been motivated to implement additional voice authentication for improved security in response to a transaction request with a higher risk. APPL-1003, ¶280; APPL-1010, [0145]; APPL-1018, 51:12-15, 52:20-24; APPL-1016, FIG. 4, [0036], [0040]-[0041]; APPL-1033, 1438; *see also* IX.D.1 below.

Accordingly, Stone-Guidance renders obvious this claim.

12. Claims 16 and 22

[16.0/22.0] ...wherein facilitating the fraud detection analysis...is further based at least in part on a determination of whether the audio sample matches a previously recorded voice sample.

Stone-Guidance renders obvious this element. APPL-1003, ¶¶282-284.

As discussed at Ground 2: [15.0/21.0], Stone-Guidance implements voice authentication that compares the captured audio sample with the registered templates in the system (previously recorded voice sample) and provides an authentication decision based on the comparison, and thus teaches this element. APPL-1037, 10; Ground 1: [16.0/22.0]; APPL-1003, ¶283; APPL-1016, [0036], [0040]-[0041]; APPL-1018, 51:12-15; APPL-1033, FIG. 3.

Accordingly, Stone-Guidance renders obvious this claim.

13. Claims 17 and 23

[17.0/23.0] ...wherein the determination of whether the audio sample matches the previously recorded voice sample is based at least in part on performing a Fast Fourier Transform.

Stone-Guidance renders obvious this element, because in Stone-Guidance, a POSITA would have been motivated to use FFT for determining whether the audio samples match, for the same reasons discussed at Ground 1: [17.0/23.0]. APPL-1003, ¶¶285-287; APPL-1033, 1445; APPL-1031, 12:15-19; APPL-1032, FIG. 2.

Accordingly, Stone-Guidance renders obvious this claim.

D. Grounds 3 and 4: Combination of Stone, Hoyos, Varghese, and Campbell (Ground 3) and Combination of Stone, Guidance, and Campbell (Ground 4) Render Obvious Claims 15-17 and 21-23.

The claim analysis for Ground 3 (Stone-Hoyos-Varghese-Campbell) and Ground 4 (Stone-Guidance-Campbell) rely on the same analysis and evidence as provided for Grounds 1 and 2 respectively, except for where additional analysis (applying to both Grounds 3 and 4) is provided below. APPL-1003, ¶¶287-305.

1. Combination of Campbell with each of Grounds 1 and 2

A POSITA would have been motivated to apply Campbell's teaching of speaker verification techniques including FFT-based feature extraction each of Stone-Hoyos-Varghese and Stone-Guidance to achieve better performance for reducing fraudulent transactions. APPL-1003, ¶¶288-292.

First, as discussed at IX.A.5, Campbell is analogous art to the '886 patent, describing speaker verification/authentication techniques to reduce fraudulent transactions. APPL-1003, ¶289.

Second, as discussed at Grounds 1-2: Claims 15-17 and 20-23, in Grounds 1-2 each, a POSITA would have been motivated to implement multifactor authentications including voice authentication for improved security. APPL-1003, ¶290; APPL-1010, [0145]; APPL-1018, 51:12-15, 52:20-24; APPL-1016, FIG. 4, [0036], [0040]-[0041]; APPL-1033, 1438.

A POSITA would have been motivated to apply Campbell's "very popular" speaker recognition techniques using the FFT-based feature extraction to implement voice authentication in each of Grounds 1-2, because they had "been demonstrated to work well in speaker-recognition systems." APPL-1033, 1445; APPL-1003, ¶¶291-292 (citing APPL-1033, 1438-1439, Table 2).

2. Claims 15 and 21

[15.0/21.0]...wherein the set of captured biometric information further comprises an audio sample.

Campbell as combined with Grounds 1 and 2 renders obvious this element. APPL-1003, ¶¶293-297.

To the extent that it's argued that each of Grounds 1-2 does not explicitly describe an audio sample, as shown in annotated FIG. 3 below, Campbell describes the well-known fundamental knowledge that captured biometric information for voice authentication includes an audio sample. APPL-1033, 1440. Thus, POSITA would have applied Campbell's teaching of capturing the audio sample to implement voice authentication of Grounds 1-2. APPL-1003, ¶¶294-296.

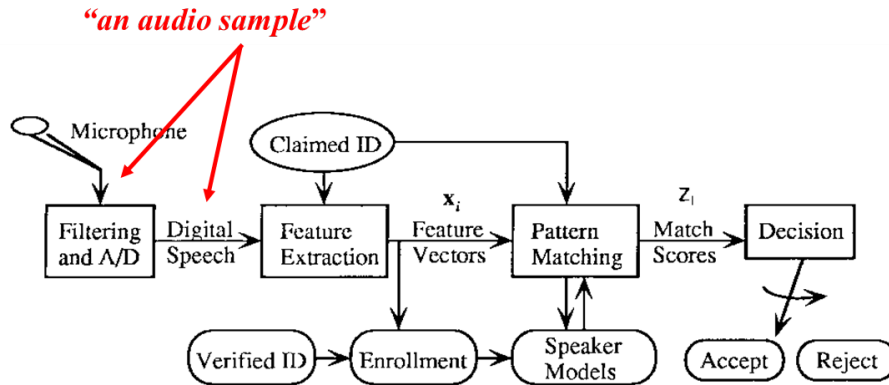


Fig. 3. Generic speaker-verification system.

APPL-1033, FIG. 3, annotated

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

3. Claims 16 and 22

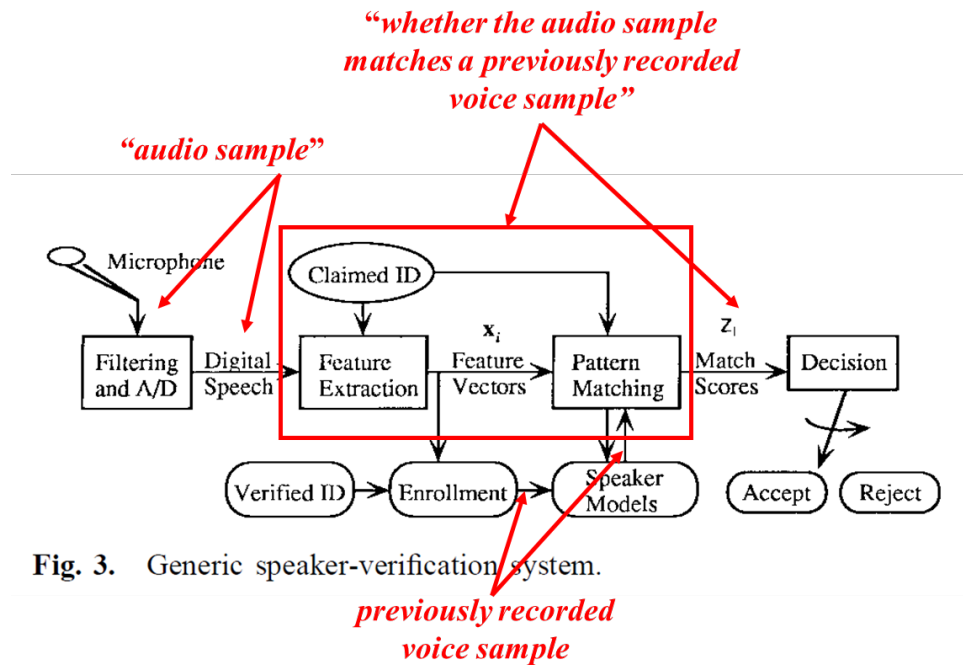
[16.0/22.0] ...wherein facilitating the fraud detection analysis...is further based at least in part on a determination of whether the audio sample matches a previously recorded voice sample.

Campbell as combined with Grounds 1 and 2 renders obvious this element.

APPL-1003, ¶¶298-301.

To the extent that it's argued that Grounds 1-2 each do not explicitly describe the matching as claimed, as shown in annotated FIG. 3 below, Campbell describes the well-known fundamental knowledge of matching the captured audio sample with a previously recorded voice sample for voice authentication in "enrollment." APPL-1033, 1438; APPL-1003, ¶¶299-300. Thus, a POSITA would have applied Campbell's teaching of providing an accept/reject decision based on a matching result to implement voice authentication of Grounds 1-2. APPL-1003,

¶¶299-300; Grounds 1-2: Claims 16 and 22.



APPL-1033, FIG. 3, annotated

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

4. Claims 17 and 23

[17.0/23.0] ...wherein the determination of whether the audio sample matches the previously recorded voice sample is based at least in part on performing a Fast Fourier Transform.

Campbell as combined with Grounds 1 and 2 each renders obvious this element. APPL-1003, ¶¶302-306.

To the extent that each of Grounds 1-2 does not explicitly describe using FFT, a POSITA would have been motivated to apply Campbell’s “very popular” method using FFT-based feature extraction for matching to implement voice

authentication of Grounds 1-2, because they had “been demonstrated to work well in speaker-recognition systems.” APPL-1033, 1445; APPL-1003, ¶¶303-305 (citing APPL-1031, 12:15-19; APPL-1032, FIG. 2); Grounds 1-2: Claims 17 and 23; IX.C.1.

Accordingly, Stone-Hoyos-Varghese-Campbell and Stone-Guidance-Campbell 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*⁴ factors favor institution.

Denial would be improper based on factors in *Apple v. Fintiv*, IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020) (precedential). Patent Owner asserted the ’886 patent against Apple in WDTX-1-23-cv-00324 (“the Parallel District Court Proceeding”). *See supra* Section II.B.

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

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 (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. *See eCardless Bancorp, Ltd. v. PayPal Holdings, Inc. et al.*, Dkt. 65 (Third Scheduling Order), Case No. 22:cv-00245 (W.D. Tex.); *ParkerVision, Inc. v. Realtek Semiconductor Corp.*, Dkt. 65 (Agreed Scheduling Order) Case No. 22-cv-01162 (W.D. Tex.). 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 and denied Apple's motion for transfer to NDCA, though no written order has issued. Preliminary constructions apply plain and ordinary meaning. APPL-1026, 1-2. This Petition is not duplicative because it challenges claims 3, 8, 15-17, and 21-23, which are not asserted in the Parallel District Court Proceeding. *See* APPL-1029, 2. Moreover, Apple stipulates that, if the Board institutes trial, it will not pursue the same grounds raised in this Petition in the Parallel District Court Litigation. *See Sand Revolution II, LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020). The stipulation reduces any overlap and mitigates concerns of duplicative efforts or potentially conflicting decisions.

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

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

B. *Advanced Bionics* Test Favors Institution.

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

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 Campbell during the prosecution. Moreover, they are non-cumulative, because they teach the amended features resulting in the notice of allowance. *See* APPL-1002, 171-198.

XI. CONCLUSION

Petitioner has established a reasonable likelihood that Challenged Claims of the '886 patent are unpatentable, and requests institution of *inter partes* review.

Dated: January 30, 2024

Respectfully submitted,
/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 13,504 (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-1040, APPL-1044, 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