

**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

---

**DECLARATION OF CREED JONES, PH.D.**  
**UNDER 37 C.F.R. § 1.68 IN SUPPORT OF PETITION**  
**FOR INTER PARTES REVIEW**

## TABLE OF CONTENTS

|      |                                                                                                                                 |    |
|------|---------------------------------------------------------------------------------------------------------------------------------|----|
| I.   | INTRODUCTION .....                                                                                                              | 1  |
| II.  | QUALIFICATIONS .....                                                                                                            | 6  |
| III. | LEVEL OF ORDINARY SKILL IN THE ART .....                                                                                        | 9  |
| IV.  | RELEVANT LEGAL STANDARDS .....                                                                                                  | 11 |
|      | A. Anticipation .....                                                                                                           | 11 |
|      | B. Obviousness .....                                                                                                            | 12 |
| V.   | THE '886 PATENT .....                                                                                                           | 13 |
|      | A. Summary of the '886 patent .....                                                                                             | 13 |
|      | B. Prosecution History .....                                                                                                    | 15 |
| VI.  | CLAIM CONSTRUCTION .....                                                                                                        | 16 |
| VII. | FOUNDATIONS .....                                                                                                               | 16 |
|      | A. Overview of Prior Art .....                                                                                                  | 16 |
|      | 1. Stone .....                                                                                                                  | 16 |
|      | 2. Hoyos .....                                                                                                                  | 18 |
|      | 3. Varghese .....                                                                                                               | 21 |
|      | 4. FFIEC Guidance .....                                                                                                         | 23 |
|      | 5. Campbell .....                                                                                                               | 26 |
|      | 6. Analogous Art .....                                                                                                          | 28 |
|      | B. Ground 1: Claims 1-12, 14-18, and 20-23 are Rendered Obvious<br>under §103(a) over Stone in view of Hoyos and Varghese. .... | 29 |
|      | 1. Combination of Embodiments of Stone .....                                                                                    | 29 |
|      | 2. Combination of Stone and Hoyos .....                                                                                         | 32 |
|      | 3. Combination of Stone, Hoyos, and Varghese .....                                                                              | 40 |
|      | 4. Claim 1 .....                                                                                                                | 47 |
|      | 5. Claim 2 .....                                                                                                                | 84 |
|      | 6. Claim 3 .....                                                                                                                | 85 |
|      | 7. Claim 4 .....                                                                                                                | 88 |

|     |                                                                                                         |     |
|-----|---------------------------------------------------------------------------------------------------------|-----|
| 8.  | Claim 5.....                                                                                            | 89  |
| 9.  | Claim 6.....                                                                                            | 90  |
| 10. | Claim 7.....                                                                                            | 93  |
| 11. | Claim 8.....                                                                                            | 93  |
| 12. | Claim 9.....                                                                                            | 93  |
| 13. | Claim 10.....                                                                                           | 93  |
| 14. | Claim 11.....                                                                                           | 94  |
| 15. | Claims 12 and 18.....                                                                                   | 96  |
| 16. | Claims 14 and 20.....                                                                                   | 97  |
| 17. | Claims 15 and 21.....                                                                                   | 98  |
| 18. | Claims 16 and 22.....                                                                                   | 100 |
| 19. | Claims 17 and 23.....                                                                                   | 101 |
| C.  | Ground 2: Claims 1-12, 14-18, and 20-23 are Rendered Obvious<br>under §103(a) over Stone-Guidance. .... | 102 |
| 1.  | Combination of Stone and Guidance (“Stone- Guidance”)....                                               | 102 |
| 2.  | Claim 1 .....                                                                                           | 105 |
| 3.  | Claim 2.....                                                                                            | 117 |
| 4.  | Claim 3.....                                                                                            | 117 |
| 5.  | Claim 4.....                                                                                            | 117 |
| 6.  | Claim 5.....                                                                                            | 119 |
| 7.  | Claim 6.....                                                                                            | 119 |
| 8.  | Claim 7.....                                                                                            | 121 |
| 9.  | Claim 8.....                                                                                            | 121 |
| 10. | Claim 9.....                                                                                            | 121 |
| 11. | Claim 10.....                                                                                           | 122 |
| 12. | Claim 11.....                                                                                           | 122 |
| 13. | Claims 12 and 18.....                                                                                   | 123 |
| 14. | Claims 14 and 20.....                                                                                   | 124 |

|       |                                                                                                                                                                                                                                                    |     |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 15.   | Claims 15 and 21.....                                                                                                                                                                                                                              | 125 |
| 16.   | Claims 16 and 22.....                                                                                                                                                                                                                              | 126 |
| 17.   | Claims 17 and 23.....                                                                                                                                                                                                                              | 127 |
| D.    | Grounds 3 and 4: Combination of Stone, Hoyos, Varghese, and Campbell (Ground 3, “Stone-Hoyos-Varghese-Campbell”) and Combination of Stone, Guidance, and Campbell (Ground 4, “Stone-Guidance-Campbell”) render obvious Claims 15-17 and 21-23..... | 127 |
| 1.    | Combination of Campbell with Combinations 1 and 2 .....                                                                                                                                                                                            | 128 |
| 2.    | Claims 15 and 21.....                                                                                                                                                                                                                              | 129 |
| 3.    | Claims 16 and 22.....                                                                                                                                                                                                                              | 131 |
| 4.    | Claims 17 and 23.....                                                                                                                                                                                                                              | 132 |
| VIII. | DECLARATION.....                                                                                                                                                                                                                                   | 135 |

| 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:<br><br>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:...]<br><br>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:<br><br>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:...]<br><br>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:]<br><br>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:<br><br>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:]<br><br>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:<br><br>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:...]<br><br>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] | <p>[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:]</p> <p>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.</p> |
| 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**

1. I, Dr. Creed Jones, have been retained by counsel for Apple Inc., (“Apple” or “Petitioner”) as a technical expert in connection with the proceeding identified above. I submit this declaration in support of Apple’s Petition for *Inter Partes* Review of U.S. Patent No. 11,526,886 (“the ’886 patent”).

2. Compensation for my work in this matter is based on an hourly rate. In addition, reasonable and customary expenses associated with my work and testimony in this matter are reimbursed. This compensation is not contingent on the outcome of this matter, nor is it contingent on the specifics of my testimony. I have no personal or financial stake, nor any interest in the outcome of the present proceeding.

3. In the preparation of this declaration, I have studied:

(1) APPL-1001, U.S. Patent No. 11,526,886 to Jakobsson (“’886 patent”);

(2) APPL-1002, Prosecution File History of U.S. App. No. 16/893,237 (issued as ’886 patent) (“’237 App”);

(3) APPL-1005, Prosecution File History of U.S. Prov. App. 61/332,140 (“’140 App”)

(4) APPL-1006, Prosecution File History of U.S. App. No. 13/099,981 (issued as U.S. Patent No. 8,458, 041) (“’981 App”)

- (5) APPL-1007, Prosecution File History of U.S. App. No.  
13/875,245 (issued as U.S. Patent No. 9,972,010) (“245 App”)
- (6) APPL-1008, U.S. Pub. No. 2010/0042535 to Stone (“Stone”)
- (7) APPL-1009, U.S. Patent No. 8,386,620 to Chatterjee  
 (“Chatterjee”)
- (8) APPL-1010, U.S. Pub. No. 2006/0282660 to Varghese et al.  
 (“Varghese”)
- (9) APPL-1011, U.S. Pub. No. 2009/0135188 to Ding et al.  
 (“Ding”)
- (10) APPL-1012 U.S. Patent No. 8,355,530 to Park et al.  
 (“Park”)
- (11) APPL-1013, U.S. Pub. No. 2010/0014720 to Hoyos et  
 al. (“Hoyos”)
- (12) APPL-1014, U.S. Pub. No. 2006/0158307 to Lee et al.  
 (“Lee”)
- (13) APPL-1015, U.S. Patent No. 8,150,772 to Mardikar et  
 al. (“Mardikar”)
- (14) APPL-1016, U.S. Pub. No. 2009/0157560 to Carter et al.  
 (“Carter”)
- (15) APPL-1017, U.S. Patent No. 5,164,992 to Turk et al.

(“Turk”)

(16) APPL-1018, U.S. Patent No. 7,814,332 to Beenau et al.

(“Beenau”)

(17) APPL-1019, U.S. Patent No. 10,373,173 to Winner et al.

(“Winner”)

(18) APPL-1020, U.S. Patent No. 7,856,472 to Arav

(“Arav”);

(19) APPL-1021, Heusch, et al., “Local Binary Patterns as an Image Preprocessing for Face Authentication,” IDIAP Research Institute Report, November 2005;

(20) APPL-1022, Oracle-Bharosa Acquisition Announcement, 2007, available at

<https://www.oracle.com/us/corporate/acquisitions/bharosa/oracle-bharosa-faq-072369.pdf> (“Oracle-Bharosa Acquisition Announcement”);

(21) APPL-1023, U.S. Patent No. 7,779,268 to Draper et al.

(“Draper”);

(22) APPL-1024, U.S. Patent No. 5,930,804 to Yu et al.

(“Yu”);

(23) APPL-1031, U.S. Patent No. 8,160,877 to Nucci et al.

(“Nucci”);

(24) APPL-1032, U.S. Patent No. 7,516,074 to Bilobrov

(“Bilobrov”);

(25) APPL-1033, J. P. Campbell, “Speaker recognition: a tutorial,” in Proceedings of the IEEE, vol. 85, no. 9, pp. 1437-1462, Sept. 1997 (“Campbell”)

(26) APPL-1034, U.S. App. Pub. No. 2009/0288012A1 to Hertel et al. (“Hertel”)

(27) APPL-1035, U.S. Patent No. 8,533,485 to Bansal et al. (“Bansal”)

(28) APPL-1036, U.S. App. Pub. No. 2006/0271460A1 to Hanif (“Hanif”)

(29) APPL-1037, Federal Financial Institutions Examination Council, FFIEC Press Release and FFIEC Guidance - Authentication in an Internet Banking Environment, Oct 12, 2005 (“Guidance”)

(30) APPL-1038, Bhargav-Spantzel et al., “Privacy Preserving Multifactor Authentication with Biometrics,” DIM’06, November 3, 2006 (“Bhargav-Spantzel”);

(31) APPL-1039, FDIC Financial Institution Letter, FFIEC

Guidance Authentication in an Internet Banking Environment,  
FIL-103-2005, October 12, 2005 (“FIL-103-2005” or “FDIC  
financial institution letter”)

(32) APPL-1040, Federal Financial Institutions Examination  
Council, FFIEC Guidance Press Release, Oct 12, 2005 (“FFIEC  
Guidance Press Release”)

(33) 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”)

(34) 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”).

4. In forming the opinions expressed below, I have considered:

- (1) The documents listed above;
- (2) Any additional documents discussed below; and
- (3) My own knowledge and experience based upon my work in the  
fields of security solutions, including biometric authentication

technologies as described below.

## II. QUALIFICATIONS

5. My qualifications for forming the opinions set forth in this Declaration are summarized here and explained in more detail in my *curriculum vitae*, which is attached as APPL-1004.

6. I have a Ph.D. degree in Computer Engineering from Virginia Polytechnic Institute and State University (“Virginia Tech”). I also have a M.S. degree in Electrical and Computer Engineering and a B.S. degree in Electrical Engineering from Oakland University.

7. I am currently a Collegiate Professor in the Electrical and Computer Engineering department of the College of Engineering at Virginia Tech. Previously, I was a Professor of Computer Science at California Baptist University, and at Seattle Pacific University.

8. For more than 25 years, I have studied, designed, and worked in the field of image processing, biometric identification, computer science, and software development. My experience includes numerous years of teaching and research, with research interests including image processing, computer vision and machine learning.

9. I have been active in the field of image processing since 1983, and I have extensive experience in the development of image processing algorithms and

software. I hold seven US patents in image processing systems and methods. My areas of expertise have included multi-spectral and hyperspectral imagery, automated inspection, optical character recognition, image formation and capture, and biometric feature extraction and matching.

**10.** I have been a developer of image processing software for over 30 years. I have implemented image processing solutions in C, C++, Java, Python, MATLAB and assembly programming languages, using a large number of platforms and environments including OpenCV, ImageJ, CImg, NIH Image and several proprietary packages. I have also managed groups of image processing software developers in several organizations.

**11.** I am a co-founder and the Chief Technology Officer of Globe Biomedical, a medical device start-up company located in Riverside, CA. Globe was founded to commercialize patented technology that uses imaging to monitor the progress of eye diseases, including glaucoma. This technology was invented by me and a colleague at California Baptist University.

**12.** I received my Bachelor of Science degree in Electrical Engineering from Oakland University in 1980, my Master of Science degree in Computer and Electrical Engineering from Oakland University in 1982, and my Doctor of Philosophy degree in Computer Engineering from the Virginia Polytechnic Institute and State University in 2005. My doctoral research and dissertation were

in the area of biometric identification. Specifically, my dissertation is titled “Color Face Recognition using Quaternionic Gabor Wavelets”, and comprises the development of one of the first full-color face recognition algorithms and methods.

**13.** In biometrics, I have served as an algorithm developer, systems engineer, standards developer and independent consultant. While on the staff of Sagem Morpho, I had responsibility for research and strategy in the areas of fingerprint capture systems and methods. SMI AFIS I have experience in several image-based biometric modalities: fingerprint, face, iris, vein pattern and hand geometry. My doctoral dissertation, Color Face Recognition using Quaternionic Gabor Filters, was the first description of a full-color face recognition algorithm using robust modern concepts and included both theoretical groundwork and a complete implementation in C++.

**14.** The ANSI-accredited body for the development of US National standards in Information Technology is INCITS, the International Committee for Information Technology Standards. From 2001 to 2006 I was the chair of the INCITS M1.3 subcommittee on standardization of biometric data interchange formats, as well as a key participant in its parent body, INCITS M1. During this time, I was also the technical editor of INCITS 378, Finger Minutia Format for Data Interchange, the most widely adopted standard for exchange of biometric feature data. I was also a key contributor to INCITS 381 - Fingerprint Image Data

Format, INCITS 385 – Face Recognition Data Format, INCITS, and the BioAPI standard.

**15.** In the international arena, biometrics standards are developed under ISO/IEC Joint Technical Committee 1, Subcommittee 37. I was a frequent member of the US delegation to JTC1 SC37, and to its Working Group 3 on biometric data standards. I was the chief technical editor of ISO/IEC 19794, fingerprint minutiae data format, and contributed to many other international standards such as ISO/IEC 29794 – biometric sample quality.

**16.** I have been and am currently a member of several professional organizations and committees. I am a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), a member of the ANSI/INCITS M1 Committee for biometrics standards, chair of ANSI/INCITS M1.3 Task Group on Biometric Data Interchange Formats - chair (2001 – 2006), chair of ANSI/INCITS B10.9 Task Group on biometrics (2001), technical editor of ANSI/INCITS B10.8 biometric task force (1999 - 2001), and a member of the BioAPI Industry Consortium (1999 – 2001).

### **III. LEVEL OF ORDINARY SKILL IN THE ART**

**17.** I understand that the level of ordinary skill may be reflected by the prior art of record, and that a Person of Ordinary Skill in The Art (“POSITA”) to which the claimed subject matter pertains would have the capability of

understanding the scientific and engineering principles applicable to the pertinent art. I understand that a POSITA has ordinary creativity, and is not an automaton.

**18.** I understand that there are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including (1) the levels of education and experience of persons working in the field at the time of the invention; (2) the sophistication of the technology; (3) the types of problems encountered in the field; and (4) the prior art solutions to those problems.

**19.** I have been informed by counsel that the earliest claimed priority date for the '886 patent is May 6, 2010, although any given claim of the '886 patent may or may not be entitled to the earliest claimed priority date. I am familiar with the biometric authentication technology pertinent to the '886 patent. I am also aware of the state of the art at the time of the earliest claimed priority date.

**20.** Based on the technologies disclosed in the '886 patent, I believe that a POSITA would include someone who had, as of the claimed priority date of the '886 patent, 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. In addition, I recognize that someone with less formal education but more experience, or more formal

education but less experience could have also met the relevant standard for a POSITA. I believe that I am at least a POSITA and, furthermore, I have supervised students and engineers who were also POSITAs. Accordingly, I believe that I am qualified to opine from the perspective of a POSITA regarding the '886 patent.

21. For purposes of this Declaration, unless otherwise noted, my opinions and statements, such as those regarding the understanding of a POSITA (and specifically related to the references I consulted herein), reflect the knowledge that existed in the art before the earliest claimed priority date of the '886 patent.

#### **IV. RELEVANT LEGAL STANDARDS**

22. I have been asked to provide my opinions regarding whether claims 1-12 (the "Challenged Claims") of the '886 patent would have been obvious to a POSITA at the time of the alleged invention in light of the prior art.

23. I am not an attorney. In preparing and expressing my opinions and considering the subject matter of the '886 patent, I am relying on certain legal principles explained to me by counsel.

24. I understand that a claim is unpatentable if it is anticipated under 35 U.S.C. § 102 or obvious under 35 U.S.C. § 103.

##### **A. Anticipation**

25. I have been informed by counsel that a patent claim is unpatentable as anticipated if each element of that claim is present either explicitly or inherently in

a single prior art reference. I have also been informed that, to be an inherent disclosure, the prior art reference must necessarily disclose the limitation, and the fact that the reference might possibly practice or contain a claimed limitation is insufficient to establish that the reference inherently teaches the limitation.

**B. Obviousness**

26. I have been informed and I understand that a claimed invention is unpatentable under 35 U.S.C. § 103(a) if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a POSITA at the time the invention was made. I understand that the appropriate analysis for determining obviousness of a claimed invention takes into account factual inquiries, including the level of ordinary skill in the art, the scope and content of the prior art, and the differences between the prior art and the claimed subject matter as a whole.

27. I have been informed and I understand that the United States Supreme Court has recognized several rationales for combining references or modifying a reference to show obviousness of claimed subject matter. Some of these rationales include the following: (a) combining prior art elements according to known methods to yield predictable results; (b) simple substitution of one known element for another to obtain predictable results; (c) use of a known technique to improve a similar device (method, or product) in the same way; (d) applying a known

technique to a known device (method, or product) ready for improvement to yield predictable results; (e) choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; and (f) some teaching, suggestion, or motivation in the prior art that would have led a POSITA to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention. I have also been informed and I understand that a demonstration of obviousness does not require a physical combination or bodily incorporation, but rather may be found based on consideration of what the combined teachings would have suggested to a POSITA at the time of the alleged invention.

## **V. THE '886 PATENT**

### **A. Summary of the '886 patent**

**28.** The '886 patent is directed at electronic transactions, and specifically financial transaction applications. APPL-1001, '886 patent, Abstract. Specifically, the '886 patent describes techniques for reducing fraud for financial transaction applications, including displaying a source icon that includes a graphical representation of an owner of the account, and “at least one of a photograph, a voice print, and location data will be taken prior to executing the transaction request” for fraud detection. APPL-1001, Abstract.

**29.** 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.

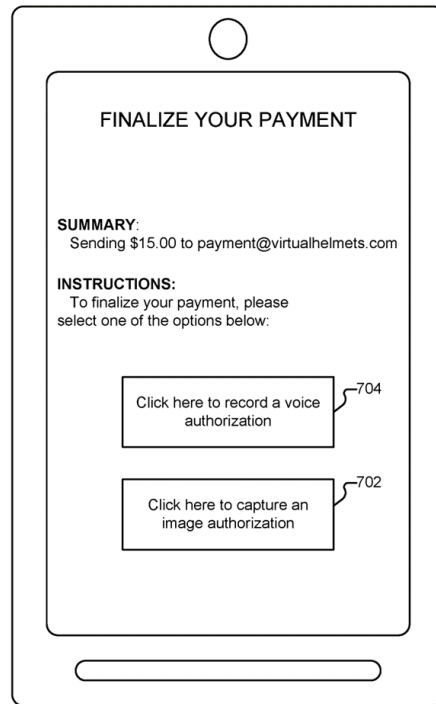


FIG. 7

**APPL-1001, FIG. 7**

**30.** Specifically, '886 patent describes that when box 702 is selected, “an analysis of the photograph is performed as part of the transaction,” and techniques “for confirming that the object being photographed is alive (e.g., by taking multiple photographs in rapid succession) can be employed to help make sure that the fraudster isn’t using camera 112 to photograph a printed picture of the legitimate user.” APPL-1001, 8:65-9:4.

**31.** However, as discussed below, these supposedly improved techniques for fraud detection in electronic transactions using biometric authentication (e.g., based on liveness analysis of successively taken photographs) and location were

well-known at the time of the claimed invention.

**B. Prosecution History**

**32.** On September 2, 2021, Examiner issued an Office Action including double patenting rejection over U.S. Patent Nos. 9,972,010 and 10,713,656, in addition to rejections under §§101, 112. APPL-1002, 85-96.

**33.** In response, Applicant amended claims address the rejections. APPL-1002, 117-125. Further, Applicant filed a terminal disclaimer to overcome the double patenting rejection. APPL-1002, 126-127.

**34.** On January 21, 2022, Examiner issued a final Office Action maintaining the §101 rejection. APPL-1002, 138-146. Applicant filed an RCE and amended the claims to recite “a physical location,” “capturing, using a camera, a set of images,” and “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.” APPL-1002, 171-182.

**35.** On August 22, 2022, a Notice of Allowance issued, with an Examiner amendment, apparently negotiated by the Applicant during an interview. APPL-1002, 184-198.

**36.** As I discuss below in more detail, the system presented in the ’886 patent was well known to persons of ordinary skill in the art before the earliest claimed priority date of the ’886 patent.

## **VI. CLAIM CONSTRUCTION**

**37.** It is my understanding that in order to properly evaluate the '886 patent, the terms of the claims must first be interpreted. It is my understanding that for the purposes of this *inter partes* review, the claims are to be construed under the so-called Phillips standard, under which claim terms are given their ordinary and customary meaning as would have been understood by one of ordinary skill in the art in light of the specification and prosecution history, unless the inventor has set forth a special meaning for a term. I have also been informed that claim terms only need to be construed to the extent necessary to resolve the obviousness inquiry.

**38.** I have reviewed the entirety of the '886 patent, as well as its prosecution history. It is my opinion that for purposes of applying the prior art presented herein to evaluate the patentability of the claims no term requires express construction. Accordingly, I have analyzed the claims consistent with their ordinary and customary meaning as would have been understood by a POSITA.

## **VII. GROUNDS**

### **A. Overview of Prior Art**

#### **1. Stone**

**39.** Stone is titled "Currency Display," and assigned to eBay on its face. Stone is analogous art to the '886 patent, because like the '886 patent, Stone is

directed to electronic transactions, and specifically, financial transaction applications. (Stone) APPL-1008, [0001]-[0005].

**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,” ((Stone) APPL-1008, [0016]), e.g., by providing visual representations of financial instruments and the amount, which reinforces the value of the amount to the user visually, and a visual representation when the monetary amount is transferred. *See also* (Stone) APPL-1008, FIGS. 1 and 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].

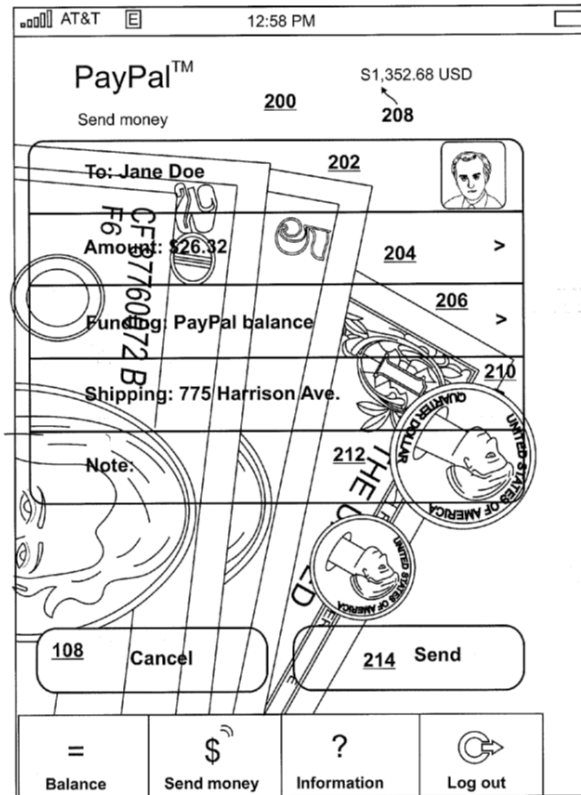


FIG. 2

(Stone) APPL-1008, FIG. 2

## 2. Hoyos

41. Hoyos is titled “Fraud Resistant Biometric Financial Transaction System and Method.” Hoyos is analogous art to the ’886 patent, because like the ’886 patent, it is directed at electronic transactions, and specifically, fraud detection for financial transaction systems. (Hoyos) APPL-1013, Abstract, [0002] (“This invention relates to biometric identification and authentication systems and methods, more particularly to authentication for financial transactions using biometrics.”).

42. Hoyos identifies that “in the field of authentication of financial transactions, high levels of accuracy and speed are critical.” (Hoyos) APPL-1013, [0009]. Furthermore, Hoyos identifies that one problem faced by biometric recognition systems is “the possibility of spoofing,” e.g., “a life-sized, high-resolution photograph of a person may be presented to an iris recognition system.” (Hoyos) APPL-1013, [0011]. To address these issues, as illustrated in FIG. 1 of Hoyos below, Hoyos describes an authentication method that has high levels of accuracy and speed with protection against spoofing.

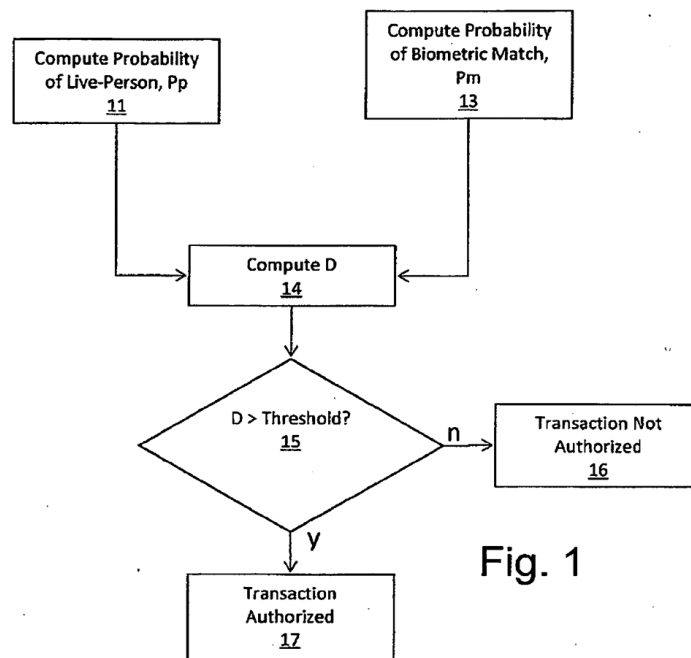


Fig. 1

(Hoyos) APPL-1013, FIG. 1

43. As shown in FIG. 1 of Hoyos above, Hoyos describes a method of authenticating financial transactions with fraud detection, which includes “acquiring biometric data from a person, calculating probability of liveness, Pp. of

the person and probability of a match,  $P_m$ . between the person and known biometric information, and providing an authenticating decision,  $D$ ., based on a combination of  $P_p$  and  $P_m$ .” (Hoyos) APPL-1013, [0017]. A financial transaction is authorized if the authentication decision  $D$  exceeds a preset threshold. (Hoyos) APPL-1013, [0033].

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

45. Hoyos provides that by authorizing transactions “by combining in one algorithm the live-person result with the match result,” various advantages are achieved, including addressing spoofing; “making it much more difficult for an

attempted fraudster to refine fraudulent methods” by eliminating clear feedback; greatly reducing “the reject rate of true authentications” by using the liveness probability that is less sensitive to conditions like illumination changes; providing “an enormous deterrent to criminals since the system is acquiring biometric data that they have no idea can or cannot be used successfully as evidence against them;” and by ensuring that some live-person data is captured, providing “a means to perform customer redress.” (Hoyos) APPL-1013, [0024], [0026], [0027], [0029].

### **3. Varghese**

**46.** 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, Oracle-Bharosa Acquisition Announcement, 1; (Varghese) APPL-1010, FIG. 14 (describing a configuration including “Bharosa Authenticator”).

**47.** Varghese is analogous art to the ’886 patent, because like the ’886 patent, it is directed at fraud detection for electronic transactions including financial transaction systems. APPL-1010, [0145] (describing additional authentication where the “service provider is a bank or other financial institution which seeks a higher security authentication interface for certain transactions.”), FIG. 14.

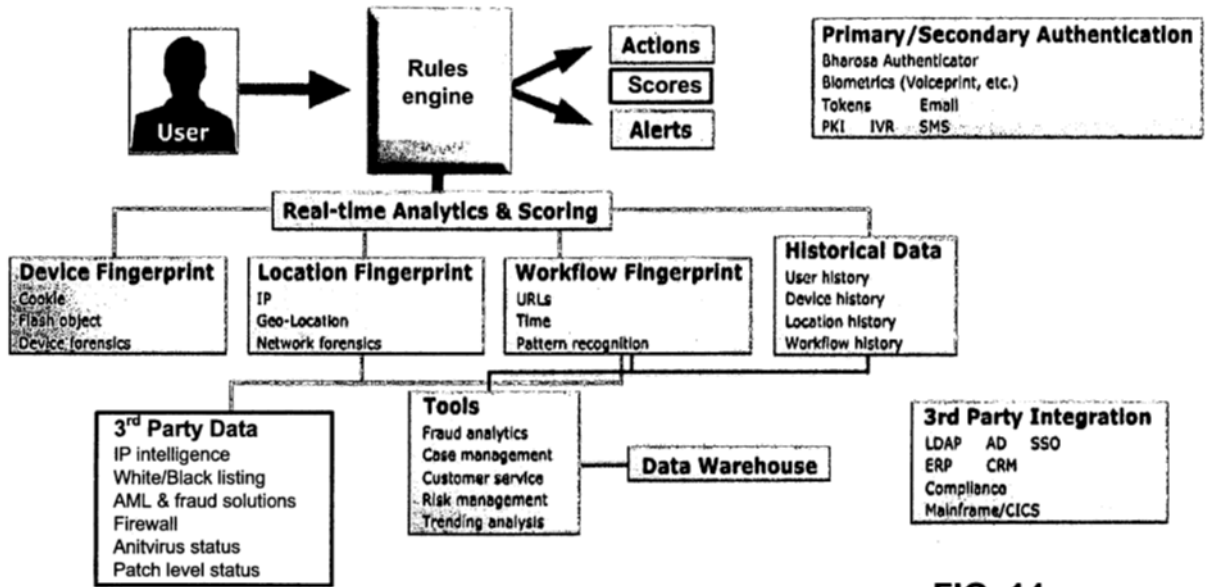


FIG. 14

(Varghese) APPL-1010, FIG. 14

48. As shown in FIG. 14 of Varghese above, Varghese describes performing real-time multi-factor authentication (e.g., location authentication using “Geo-Location” by user device IP address and voice authentication (e.g., using “Biometrics (Voiceprint, etc.)”) for improved fraud analysis. (Varghese) APPL-1010, FIG. 14. Varghese describes fraud analytics implementing various policies, which “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.” (Varghese) APPL-1010, [0097]-[0099]; *see also* (Varghese) APPL-1010, [0081], [0084], [0088], [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”), [0142], claim 31.

#### **4. FFIEC Guidance**

**49.** 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 for the federal examination of financial institutions.”<sup>1</sup> On Oct. 12, 2005, FFIEC issued its guidance titled “Authentication in an Internet Banking Environment.” (Guidance), APPL-1037<sup>2</sup>. The Guidance “describes enhanced authentication methods that regulators expect banks to use when authenticating the identity of customers using the on-line products and services,” and financial institutions are “expected to achieve compliance with the guidance no later than year-end 2006.” (FDIC financial institution letter) APPL-1039, 1.

**50.** The Guidance was publicly accessible to a POSITA at least as of October 2005—well before the earliest priority date. For example, it was available at each of official government websites for FFIEC and FDIC. (FFIEC press release), APPL-1038<sup>3</sup> (FFIEC press release of Oct. 12, 2005 with hyperlink to FFIEC guidance). For further example, FDIC sent both electronic and paper copies

---

<sup>1</sup> <https://web.archive.org/web/20051013063034/https://www.ffiec.gov/about.htm>.

<sup>2</sup> [https://web.archive.org/web/20051103035858/http://www.ffiec.gov/pdf/authentication\\_guidance.pdf](https://web.archive.org/web/20051103035858/http://www.ffiec.gov/pdf/authentication_guidance.pdf).

<sup>3</sup> <https://web.archive.org/web/20051026014312/https://www.ffiec.gov/press/pr101205.htm>.

of financial institution letter including the Guidance as the attachment. (FDIC financial institution letter), APPL-1039<sup>4</sup> (FDIC financial institution letter of Oct. 12, 2005 with FFIEC guidance attachment distributed to FDIC-Supervised Banks, paper copies available through FDIC's Public Information Center). A POSITA interested in the security for electronic transactions, exercising reasonable diligence, can locate the Guidance, because the POSITA would have looked to FFIEC and its five banking regulators (online, at physical offices, electronic letters, etc.) for requirements and guidance on designing secure electronic transaction systems and locate the Guidance.

51. Indeed, the Guidance was widely cited in numerous articles and patents. As shown below, Google Scholar<sup>5</sup> provides that Guidance was available in 45 online versions and was cited by 158 articles.

**[PDF] Authentication in an internet banking environment**

**[PDF] financialbrowser...**

FFIE Council - Retrieved June, 2005 - [financialbrowsers.com](http://financialbrowsers.com)

... of **Internet banking** should have effective and reliable methods to **authenticate** customers. ... s overall strategy for **Internet banking** and electronic commerce customer services. The level of ...

☆ Save  Cite Cited by 158 Related articles All 45 versions 

52. The FFIEC 2005 Guidance was referenced in numerous patent

---

<sup>4</sup><https://web.archive.org/web/20051019101009/http://www.fdic.gov/news/news/financial/2005/fil10305.html>

<sup>5</sup>[https://scholar.google.com/scholar?hl=en&as\\_sdt=0%2C44&q=Authentication+in+an+Internet+Banking+Environment](https://scholar.google.com/scholar?hl=en&as_sdt=0%2C44&q=Authentication+in+an+Internet+Banking+Environment)

disclosures filed before the earliest priority date as a driver for implementing multi-factor authentication. *See, e.g.*, US 8,776,176 by Oracle, 17:61-67 (“The multi-factor password-authenticated key exchange protocols would allow financial institutions and others to meet the most stringent two-factor recommendations set by the FFIEC mandate of OCC 2005-35 (Office of the Comptroller of the Currency (OCC) bulletin 2005-35 can be accessed on the Internet at the Federal Financial Institutions Examinations Council (FFIEC) website)” (filed as U.S. Patent Application 12/143,964, June 23, 2008); US 8,239,677 by Equifax, 1:62-66 (“Another driver of verification is the recently mandated Federal Financial Institutions Examination Council (FFIEC) guidelines for financial institutions. While they are not regulations, the FFIEC expects all FSPs to comply with the guidance by the end of 2006.”) (filed as U.S. Patent Application 11/545,247, October 10, 2006); US 8,032,932 by Citibank, 1:6-9 (“The Federal Financial Institutions Examination Council (FFIEC) required all financial institutions to support multi factor authentication (MFA) for accessing Internet-facing applications that hold personal data by Dec. 31, 2006.”)(filed as U.S. Patent Application 12/196,526, August 22, 2008).

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

authentication, layered security, or other controls reasonably calculated to mitigate those risks.” (Guidance) APPL-1037, 1-2. Where risk assessments indicate that the use of provides that there are “a variety of technologies and methodologies financial institutions can use to authenticate customers,” and “[t]level of risk protection afforded by each of these techniques varies.” (Guidance) APPL-1037, 2.

**54.** The Appendix of the Guidance discusses various authentication techniques that financial institutions can use to authenticate customers, including “Biometrics” including “face recognition” and “fingerprint recognition,” and “Internet Protocol Address (IPA) Location and Geo-Location.” (Guidance) APPL-1037, 2, 9-12. Biometrics techniques include face recognition systems that use facial images from “video cameras” and “include tests for liveness, such as blinking eyes,” and fingerprint recognition systems using fingerprints captured by fingerprint scanners. (Guidance) APPL-1037, 9-11. IPA location and geo-location technologies include techniques “to limit Internet users by determining where they are or, conversely, where they are not.” (Guidance) APPL-1037, 12.

## **5. Campbell**

**55.** Campbell is titled “Speaker Recognition: A Tutorial.” Campbell is analogous art to the ’886 patent, because like the ’886 patent, it is directed at technologies for reducing fraud transactions, specifically, speaker recognition techniques that “could substantially reduce this [high-tech computer thieves] crime

by reducing these fraudulent transactions.” (Campbell) APPL-1033, 1439.

56. 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.” (Campbell) APPL-1033, 1438.

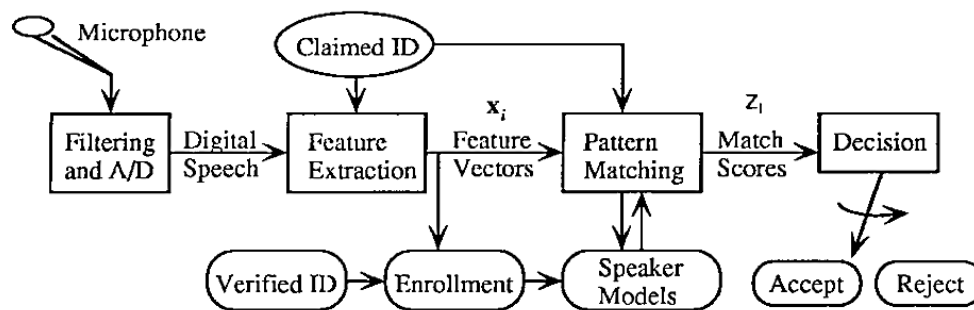


**Fig. 3.** Generic speaker-verification system.

**(Campbell) APPL-1033, FIG. 3**

57. Campbell describes a well-known speech processing technique for speaker verification using fast Fourier transform (FFT) for extracting frequency features of sounds. (Campbell) APPL-1033, 1445. Campbell explains that the mel-warped cepstrum technique using the FFT (where the features are based on the nonlinear human perception of the frequency of sounds and the cepstrum “can be considered as the spectrum of the log spectrum) “is very popular” and “has been demonstrated to work well in speaker-recognition systems.” (Campbell) APPL-

1033, 1445.

## 6. Analogous Art

58. 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). *See, e.g.*, ('886 Patent) APPL-1001, Title ("Method, Medium, and System for Reducing Fraud"), Background of the Invention ("Fraud can also be perpetrated in the context of electronic transactions. Electronic fraud can be particularly devastating because the perpetrator does not need physical access to a victim's credit card (or other resource) to perform the fraud."); APPL-1008, Title ("Currency Display"), [0001]-[0004] (describing electronic financial transactions), [0045] (considering "**biometric id**" and "security"); APPL-1013, Title ("Fraud Resistant Biometric Financial Transaction System and Method"), Abstract, [0002]; APPL-1010, Title ("System and Method for Fraud Monitoring, Detection, and Tiered User Authentication"), [0145] (describing additional authentication where the "service provider is a bank or other financial institution which seeks a higher security authentication interface for certain transactions."); (Campbell) APPL-1033, 1437 ("The literature abounds with different terms for speaker verification, including voice verification, speaker

authentication, voice authentication, talker authentication, and talker verification”), 1438 (speaker recognition methods “are probably the most natural and economical methods for solving the problems of unauthorized use of computer and communications systems and multilevel access control”), 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.**

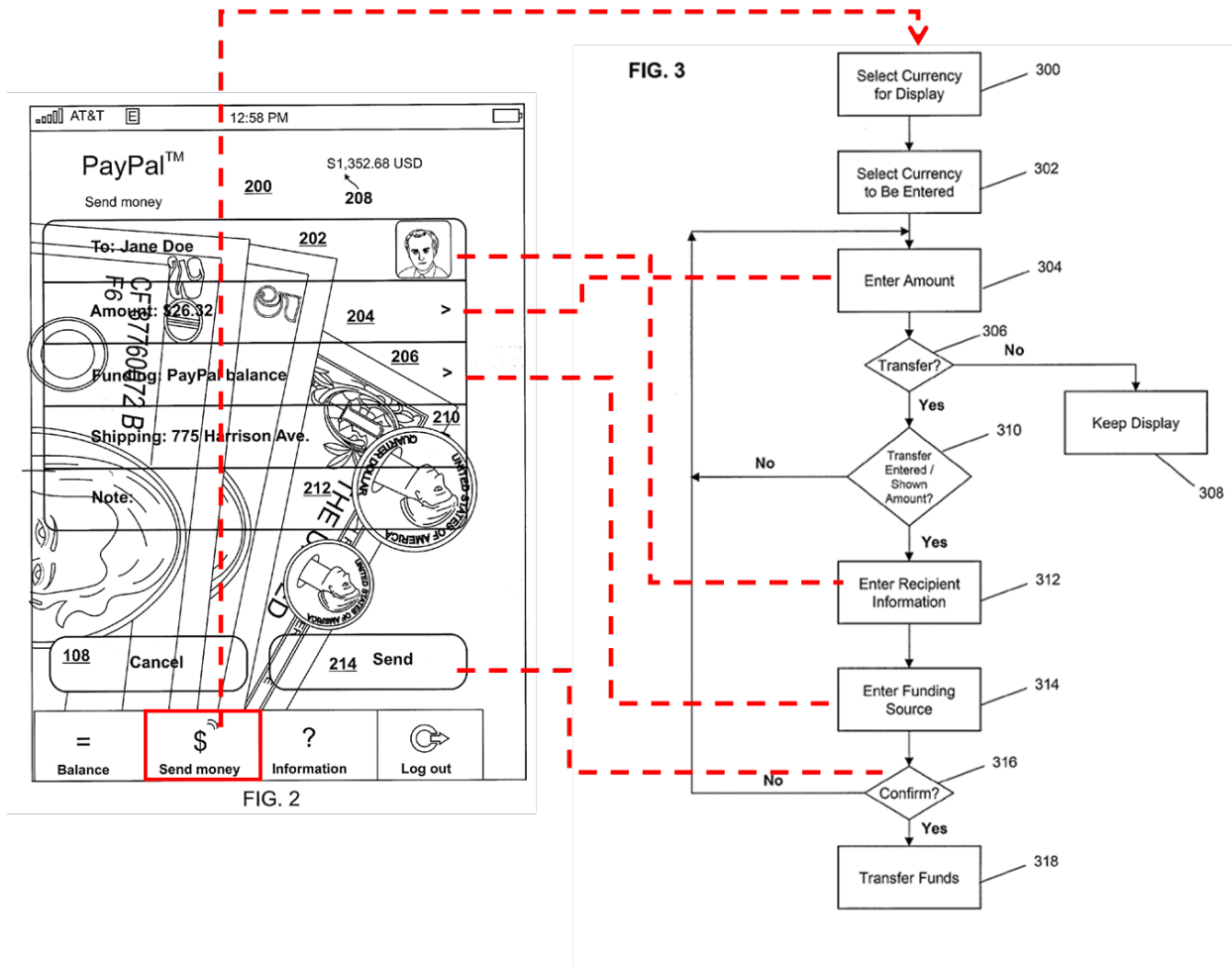
**1. Combination of Embodiments of Stone**

**59.** A POSITA would have been motivated to combine 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.”).

**60.** While FIG. 3 of Stone is a flowchart showing a method for performing an electronic transaction, and FIG. 2 shows a display on a user device, a POSITA would have understood that the display of FIG. 2 and modification thereof could be used to implement the embodiment of FIG. 3, e.g., by adding,

removing, modifying components, or by using alternative design choices of buttons and icons. APPL-1008, [0055]-[0056] (“It is contemplated that various alternate embodiments and/or modifications to the present invention, whether explicitly described or implied herein, are possible in light of the disclosure. For example, steps shown in FIG. 3 or described in connection with FIG. 3 may be omitted, performed in different order, modified, or added, while still achieving advantages of the present disclosure. Furthermore, the visual representation of the personalized currency may be static or dynamic, i.e., the visual can be an animation or a storyboard of an animation showing coins rolling or any other movement.”).

**61.** An example implementation relationship with FIGS. 2 and 3 of Stone is provided below.



**APPL-1008, FIGS. 2 and 3, annotated**

62. As shown in the example implementation of Stone above, various user actions in FIG. 2 correspond to the steps of FIG. 3, e.g., element 202 corresponds to block 312, element 204 corresponds to block 304, element 206 corresponds to block 314, and element 214 corresponds to block 316. After the user clicks the “\$Send money” icon of FIG. 2, the user interface for a financial transaction is displayed in the portion above the bottom task bar of FIG. 2, and the method of FIG. 3 or an obvious variation thereof begins to perform.

**63.** Any modification needed for combining the embodiments of FIGS. 2 and 3 based on design needs would have been within the skills of a POSITA. For example, while FIG. 2 does not explicitly include a user interface item corresponding to blocks 300, 302, and 306 of FIG. 3, techniques for implementing user interface items (e.g., icon or button) for these blocks were well-known. As shown in the annotated figures in the example implementation, after a user clicks the “\$Send money” icon in the bottom task bar of FIG. 2, a user transaction request (e.g., sending money to another user) is initiated.

## **2. Combination of Stone and Hoyos**

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

**65.** As discussed at VII.A.5, Stone and Hoyos each are analogous art to the ’886 patent. Stone describes a financial transaction system considering “security” and “biometric id,” which was well-known to be used for authentication and fraud detection. APPL-1008, [0045] (“User identifier 418 may include attributes related to the user, such as personal information (e.g., a user name,

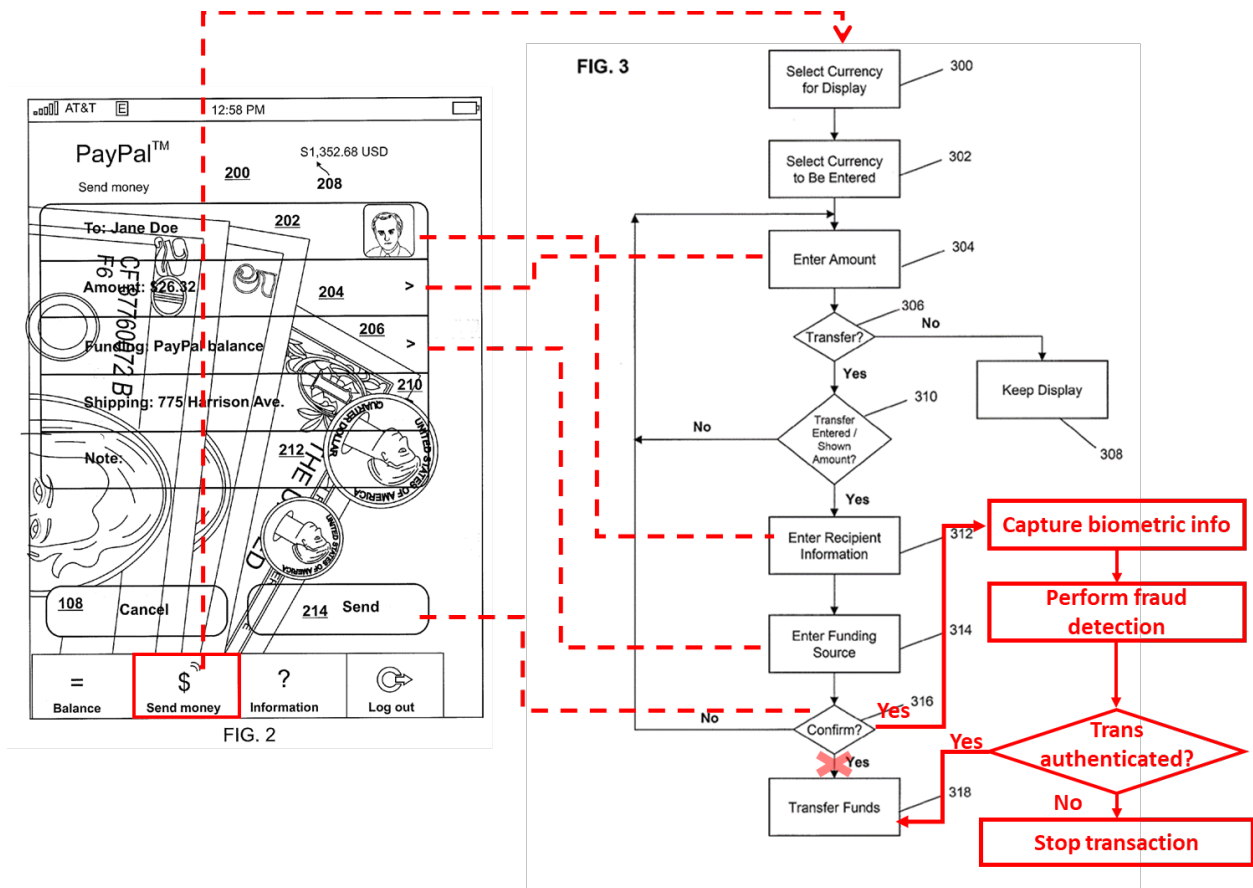
password, photograph image, biometric id, address, phone number, etc.) and banking information (e.g., banking institution, credit card issuer, user account numbers, security information, etc.); APPL-1010, [0079]; APPL-1013, Title (“Fraud Resistant Biometric Financial Transaction System and Method”), Abstract, [0002].

**66.** Further, it was well-known that such financial transactions of Stone had a need for authentication for fraud detection (e.g., with higher levels of security for some transactions). APPL-1013, [0009], [0011]; APPL-1010, [0148] (“For example, a bank or other financial institution may wish to invoke a higher security authentication interface during a session before transactions over a certain amount are sent to the server.”); APPL-1016, FIG. 3, [0073] (describing that for completing a financial transaction, “the transaction must then be authenticated before proceeding,” and “the necessary authentication level is determined based on the transaction criteria... based on factors such as value and type of transaction, as well as other factors.”).

**67.** In view of Stone’s need to implement authentication with fraud detection, a POSITA would have implemented biometric authentication and fraud detection as taught by Hoyos in the system of Stone. By applying Hoyos’ biometric authentication method “combining in one algorithm the live-person result with the match result,” various advantages are achieved in the combination,

including addressing spoofing; “making it much more difficult for an attempted fraudster to refine fraudulent methods” and thereby reducing iterative attacks by eliminating clear feedback; greatly reducing “the reject rate of true authentications” by using the liveness probability that is less sensitive to conditions like illumination changes; providing “an enormous deterrent to criminals since the system is acquiring biometric data that they have no idea can or cannot be used successfully as evidence against them;” and by ensuring that some live-person data is captured, providing “a means to perform customer redress.” APPL-1013, [0024], [0026], [0027], [0029].

**68.** Based on the combined functionality of the improved financial transaction system with biometric authentication, a POSITA would have been motivated to implement the following example Stone-Hoyos, annotated based on FIGS. 2 and 3 of Stone describing systems and methods for performing a financial transaction (e.g., fund transfer), incorporating Hoyos’ biometric authentication teachings. APPL-1008, FIGS. 2 and 3, APPL-1013, FIG. 1, [0017].



### Example of Stone-Hoyos

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

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

confirm (e.g., block 316) the transaction request.

**70.** A POSITA would have understood that performing authentication including capturing authentication data (e.g., biometric information) after and in response to user transaction request confirmation had various benefits over the alternative design choice of using only previously captured authentication information before user transaction request confirmation. One example advantage is that it enables performing 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, where Hoyos already describes contextual authentication by setting a higher decision threshold for a transaction with a higher amount/security type. (Hoyos) APPL-1012, [0028] (“A higher transaction may be authorized if the value of [decision probability] D is higher”). Another example advantage is that it captures real-time, more accurate data, which leads to more accurate and improved fraud detection and security (e.g., avoiding imposters from communicating based on stolen biometric data, reducing spoofing, etc.). (Varghese) APPL-1010, FIG. 14, [0097]-[0099] (real-time fraud analysis enforced “during post-authentication, for example when a user is making transaction requests”), TABLE 10 (describing real-time fraud analysis based on transaction parameters (e.g., type, amount) of user confirmed transaction requests); APPL-1015, FIG. 4 (reproduced below, illustrating capturing biometric

information and performing authentication after selecting desired transaction button); (Bansal) APPL-1035, 4:60-62 (describing real-time authentication data capture (e.g., real-time voice print authentication) has the benefit to “avoid imposters from communicating based on stolen biometric data”), 4:66-67 (describing using various “real-time biometric data such as voice prints, retina scans for fingerprint recordings”).

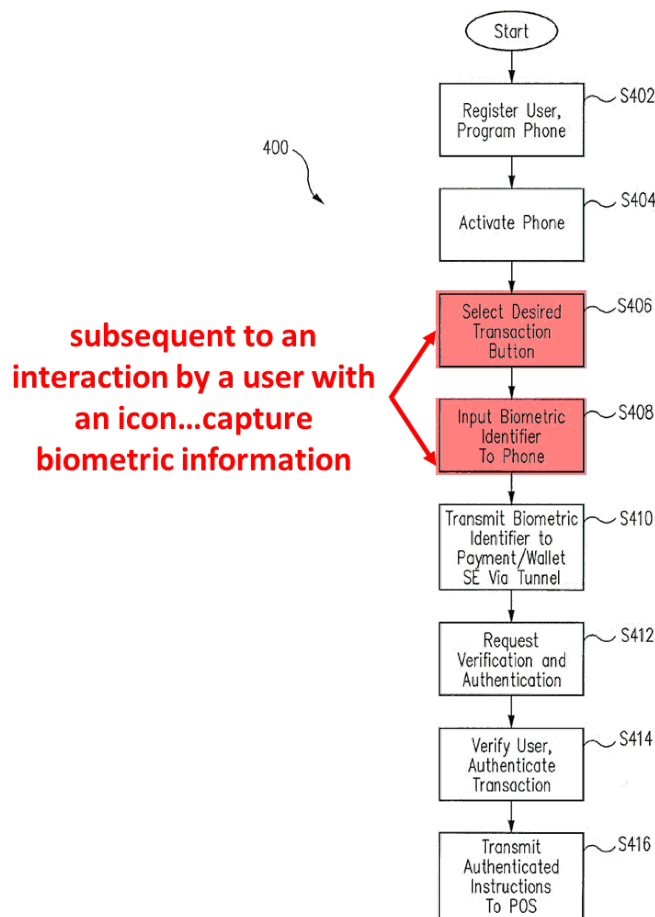


FIG. 4

**APPL-1015, FIG. 4, annotated**

71. A POSITA would have reasonably expected to succeed in configuring

Stone-Hoyos to leverage Hoyos' biometric authentication functionality since its implementation would have required only routine knowledge well within the skill of a POSITA prior to the earliest effective filing date. Stone and Hoyos each reference the financial transaction system performed using user devices with a camera for obtaining photographs for face biometric. APPL-1008, [0004] (describing user devices like "laptop, PDA, mobile phone, or other suitable device," which were well-known to easily connect to/include a camera); APPL-1013, Title, claims 13 and 14 (describing obtaining biometric data "from a web camera connected to computer" or "from a cellphone camera"), [0007] ("the face biometric is easy to acquire (a web camera for example)"); (Chatterjee) APPL-1009, 15:22-23 (it was well-known that mobile devices have digital camera functions, where "[user profile] pictures can be created using a digital camera function of mobile device"). Furthermore, Hoyos states that its invention "is capable of considerable modification, alteration and equivalents in form and function, as will occur to those ordinarily skilled in the pertinent arts." APPL-1013, [0040]. Accordingly, a POSITA would have therefore understood and found obvious to implement, in Stone's financial transaction system, biometric authentication including fraud detection as taught by Hoyos.

**72.** It would have been within the skills of a POSITA to implement the teachings of Hoyos in the system of Stone, e.g., implementing biometric

information capturing in the user device, and implementing fraud detection analysis locally using the user device, or remotely (e.g., by sending the biometric information to a payment provider device, or another remote device). APPL-1016, [0040], [0042] (describing that fraud detection can “be performed locally or by transmission of []data to a remote source”); [0076] (“The device 101 may perform some or all of the steps of the method 200 [including authentication and completion of transaction] in one embodiment, however in another embodiment, at least some steps may be performed at another device”).

**73.** For example, a POSITA would have been motivated to implement the fraud detection analysis based on the biometric information locally on the user device of Stone for the benefits including reduced latency (e.g., by minimizing communication delays between the user device and network server), offline analysis capabilities (allowing for analysis even when the user device is offline or has limited connectivity), enhanced privacy (by reducing the amount of data that needs to be transmitted to the server and minimizing potential privacy concerns), efficient resource utilization (helping distributing the processing load to the user device), customization for device characteristics (enhancing fraud detection by considering user device specific characteristics and capabilities), improved security (where a malicious actor needs to compromise the user device system), and reduced server load for cost savings and improved scalability (especially where the

system has a large user base). APPL-1015, FIG. 3, 4:4-10; APPL-1016, [0040], [0042]; (Bhargav-Spantzel) APPL-1038, 64 (“Biometric authentication can be implemented through systems performing the matching either on the server or on the client side,” where describing “security and privacy problems” and CPU-intensiveness of server side implementation, and “relatively simple and cheap” with security and privacy benefits of client side implementation).

### **3. Combination of Stone, Hoyos, and Varghese**

**74.** A POSITA would have been motivated to apply Varghese’s teaching of real-time multi-factor authentication for user transaction requests, including authentication based on physical location associated with the user and voice authentication, in Stone-Hoyos for improved security for financial transactions.

**75.** As discussed at VII.A.5, Varghese is analogous art to the ’886 patent. Varghese describes providing additional forms of authentication as needed, e.g., where the service provider is a bank or other financial institution which seeks a higher security authentication. APPL-1010, [0145] (“The rules engine then evaluates the returned user authentication information to further determine 512 whether or not other forms of authentication or verification are needed. Additional authentication, if needed, is performed 514 in accordance with the rules specified by the service provider. For example, optional step 514 can be where the service provider is a bank or other financial institution which seeks a higher security

authentication interface for certain transactions.”).

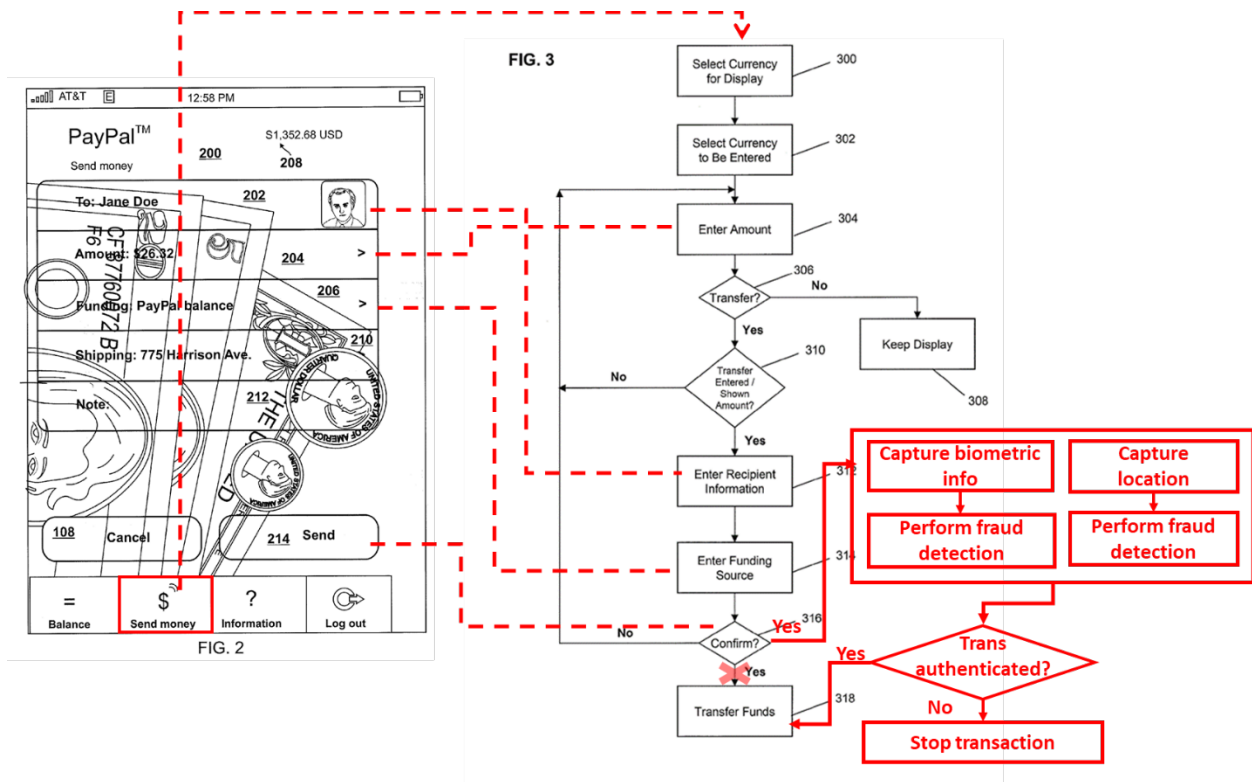
76. In view of Stone’s need to implement fraud detection with high levels of accuracy and the regulatory drive for using multifactor authentication for financial transactions, a POSITA would have implemented Varghese’s real-time multi-factor authentication for user transaction requests for improved security. It was well-known that multi-factor authentications “allows for increased authentication requirements” for increased security requirements, for example, “as the value of the transaction increases.” APPL-1016, [0036], APPL-1022, 1); APPL-1016 [0036] (describing multi-factor authentications including biometric validation including voice biometric validation and GPS location validation). It was well-known that “the number, type, and gradation (if any) of authentication can be varied as desired, based on the context of the transaction.” *Id.*; APPL-1022, 1 (“Driven by specific regulatory mandates such as FFIEC, PCI, and HIPAA, organizations are under pressure to proactively detect and prevent fraud and provide more granular reporting of their progress toward protecting the privacy of consumers. Bharosa provides key capabilities spanning strong authentication, mutual authentication, contextual authorization, proactive real-time risk monitoring and fraud detection, and real-time reporting and analysis.”).

77. Techniques using multi-factor authentication (including e.g., location authentication, voice authentication) to provide additional security for financial

transactions, as taught in Varghese, were well-known. APPL-1016, [0043]);

APPL-1016 [0043] (describing “GPS location authentication,” e.g., “reserved for significant transactions having high value, such as mortgages” where a mortgage may be prevented from closing if the person is not in a bank, “checking the GPS location for accuracy” where authentication may fail if the transaction is taking place at a retail store but the GPS indicates rapid movement, or if a detected temperature at the transaction location is sufficiently different from an expected transaction at the particular GPS location”).

**78.** Based on the combined functionality of the improved financial transaction system with fraud detection based on location, a POSITA would have been motivated to implement the following example Stone-Hoyos-Varghese for performing a financial transaction (e.g., fund transfer).



### Example of Stone-Hoyos-Varghese

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

79. Similar to the reasons discussed above at VII.B.2, as shown in the example of Stone-Hoyos-Varghese above, a POSITA would have been motivated to implement Varghese's real-time multi-factor authentication (including capturing authentication data and performing fraud detection thereupon) for user transaction request (also referred to as "post-authentication") after a user confirms a user transaction request, which is at least after the user interaction with the icon (e.g., user clicking the "\$Send money" icon of FIG. 2) to initiate the transaction request, and after user interactions with icons to continue (e.g., blocks 300-314) and confirm (e.g., block 316) the transaction request.

**80.** A POSITA would have understood that performing real-time multi-factor authentication including capturing authentication data (e.g., location, voice) after user transaction request confirmation has various benefits over the alternative design choice of using previously captured and stored authentication data. One example advantage is that it enables performing contextual authentication (e.g., determining security level and corresponding authentication factors and capturing specific type(s) of biometric/contextual data for authentication) for the specific transaction based on transaction information (e.g., type, amount) for improved fraud detection. (Varghese) APPL-1010, FIG. 14, [0091] (describing primary/secondary authentications including location authentication and voiceprint authentication), TABLE 10 (describing real-time fraud analysis based on transaction parameters (e.g., type, amount) of confirmed transaction requests); (Carter) APPL-1016, [0043] (describing GPS location authentication in multi-factor authentication can be “reserved for significant transactions having high value”). Another example advantage is that it provides more accurate and updated real-time information compared to using previously captured/stored authentication data, thereby providing improved fraud detection and security (e.g., real-time location data in particular in view of the location changes of mobile user devices); APPL-1010, [0148]; APPL-1015, FIG. 4.

**81.** Moreover, capturing the location data after user transaction

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

**82.** A POSITA would have reasonably expected to succeed in configuring Stone-Hoyos-Varghese to leverage Varghese's real-time multi-factor authentication functionality since its implementation would have required only routine knowledge well within the skill of a POSITA prior to the earliest effective filing date. Stone and Varghese each reference the financial transaction system performed using user devices that provide location data. APPL-1008, [0026] (describing that "user device may detect the location of the user and use the currency of that country. This detection may be determined through GPS or any other location-determining method"); APPL-1010, [0093] ("Location information characterizes the location of the device from which a request originates. Location can most easily be estimated from the device's IP address and the hierarchy of networks linking the device to the Internet."). A POSITA would have therefore understood and found obvious to implement, in Stone's financial transaction system, real-time multi-factor authentication/fraud detection (including location authentication using GPS, IP address, or any other location-determining method)

as taught by Varghese.

**83.** Similar to the reasons discussed above at VII.B.2, it would have been within the skills of a POSITA to implement the teachings of Varghese, locally or remotely, in the system of Stone. For example, a POSITA would have implemented the location capturing taught by Varghese in the user device of Stone (e.g., using IP address, GPS, or other suitable location capturing methods). For further example, a POSITA would have understood that the fraud detection analysis based on location data could be implemented with the alternative design choices of implementing the fraud detection locally using the user device, or remotely (e.g., by sending the location data to a payment provider device, or another remote device) in the system of Stone. APPL-1016, [0040], [0042] (describing that fraud detection can “be performed locally or by transmission of []data to a remote source”), [0076] (“The device 101 may perform some or all of the steps of the method 200 [including authentication and completion of transaction] in one embodiment, however in another embodiment, at least some steps may be performed at another device connected to the device 101, such as the central computer 162 of FIG. 2.”)

**84.** In particular, a POSITA would have been motivated to implement the fraud detection analysis based on location locally on the user device of Stone for the benefits including reduced latency (e.g., by minimizing communication delays

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

#### **4. Claim 1**

**[1.0] A system, comprising:**

**85.** Stone discloses or at least renders obvious the preamble to the extent that it is limiting.

**86.** Specifically, as shown in FIG. 4 of Stone below, Stone describes “a

system 400 configured to utilize the currency display over a network 402.” APPL-1008, [0040]. “System 400 includes at least a user device 404, one or more recipient 406 devices, and at least one payment provider server 408 in communication over the network 402.” APPL-1008, [0040].

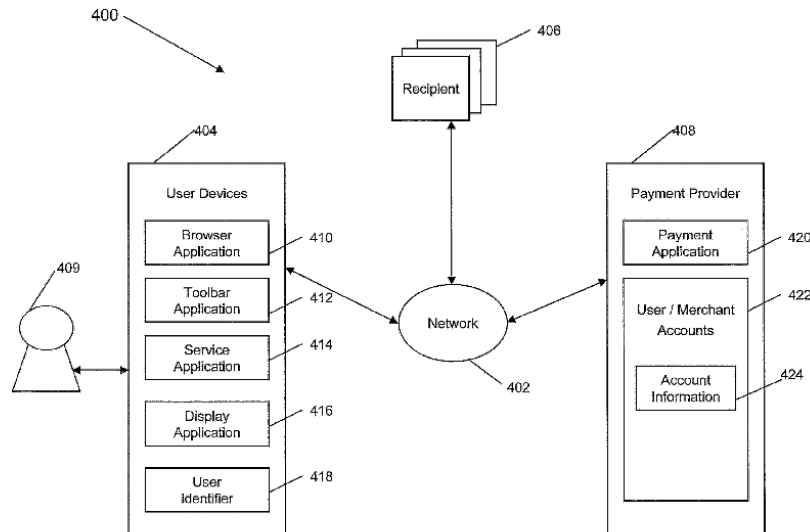


FIG. 4

#### APPL-1008, FIG. 4

87. 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.” (Stone) 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.” (Stone) APPL-1008, [0041]. Stone further describes that its system includes software “such as program code and/or data...stored on one or more computer readable mediums.” (Stone) APPL-1008, [0054].

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

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

**89.** Stone alone or Stone-Hoyos-Varghese renders obvious this element.

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

**91.** Specifically, as shown in FIG. 5 of Stone below, Stone describes “system 500 suitable for implementing embodiments of the invention, including user device 404, one or more recipient devices 406, and payment processing device 408,” where system 500 includes a processor (processing component 504). APPL-1008, [0049] (“System 500, such as part of a cell phone, personal computer and/or a network server, includes a bus 502 or other communication mechanism for communicating information, which interconnects subsystems and components, such as a processing component 504 (e.g., processor, micro-controller, digital

signal processor (DSP), etc.); APPL-1008, claim 1 (“1. A device comprising:...a processor configured to convert the money amount into a visual representation of a specific type of currency”).

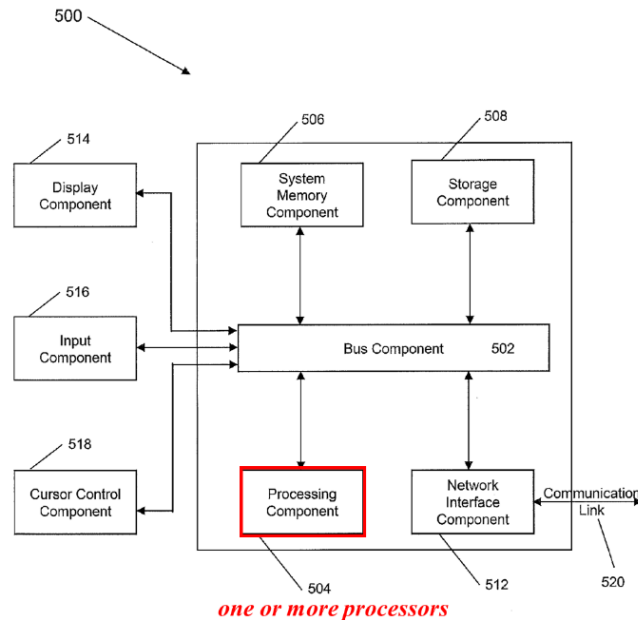


FIG. 5

### APPL-1008, FIG. 5, annotated

92. As shown in FIG. 4 of Stone below, the system 400 includes one or more processors (e.g., processor 504 in user device 404 alone, or in combination with other processors including the processor 504 of payment provider device 408) configured to process data, such as computer program instructions, for perform processes for a transaction. See also APPL-1001, 2:21-23 (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.”).

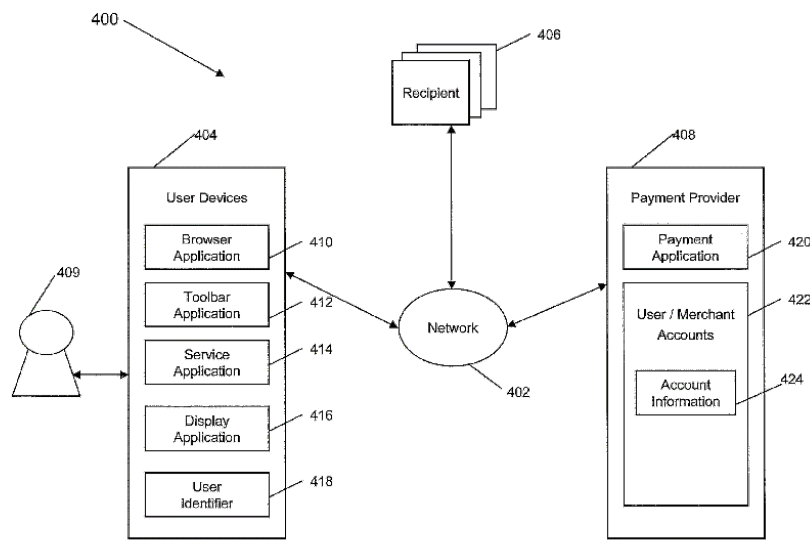


FIG. 4

**APPL-1008, FIG. 4**

**93. 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 initiating, authenticating, and completing the electronic transaction.

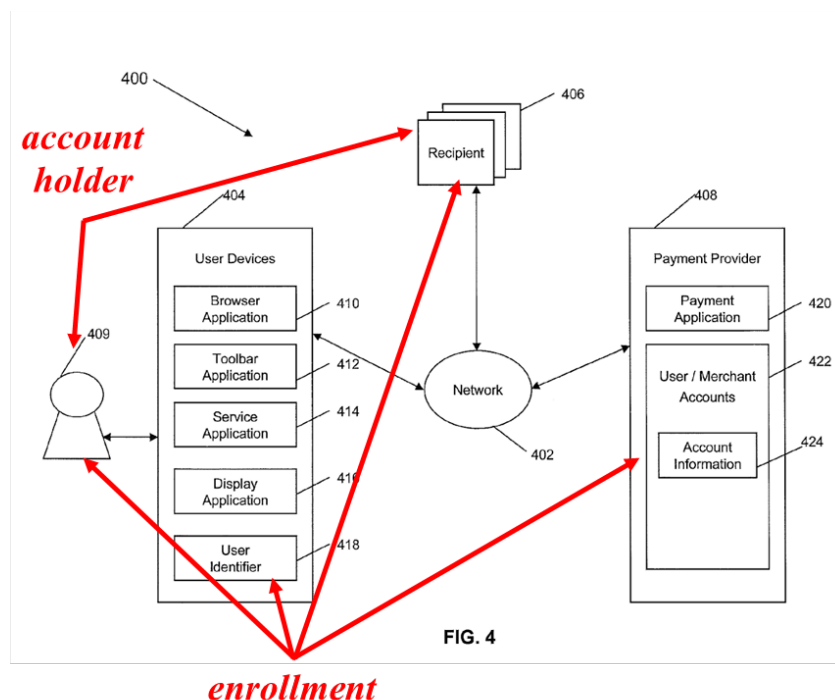
**94.** Therefore, Stone alone or Stone-Hoyos-Varghese renders obvious “one or more processors” as claimed.

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

**95.** Stone discloses or at least renders obvious this element.

**96.** Specifically, Stone discloses one or more processors (e.g., one or

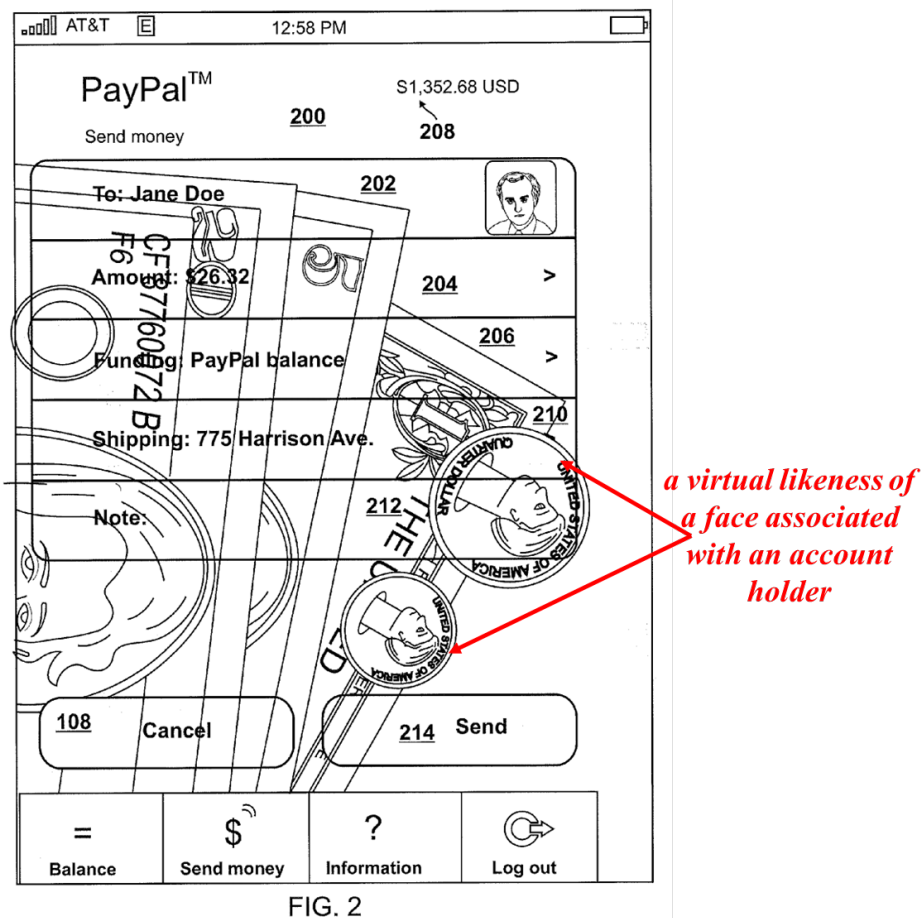
more processors of devices of system 400) configured to render, in one or more interfaces (e.g., interface 100 of FIG. 1, interface 200 of FIG. 2), a virtual likeness of a face (e.g., either a photo of the user on the personalized currency, or a photo of recipient of the electronic transaction, each disclosed by Stone) associated with an account holder (user 409 or recipient each having a user account 422). APPL-1008, [0048] (“a plurality of user and recipient accounts 422, each of which may include account information 424 associated with individual users, including user 409, and the one or more recipient device 406.”).



**APPL-1008, FIG. 4, annotated**

97. First, as shown in annotated FIG. 2 below, Stone discloses one or more processors configured to *render, in one or more interfaces* (a display e.g.,

display 200 showing the visual representation of the personalized currency), a *virtual likeness of a face associated with an account holder* (a photograph of a user's face on the personalized currency). 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”).



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

98. 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 name box 202 indicating the recipient of funds as well as 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**”).

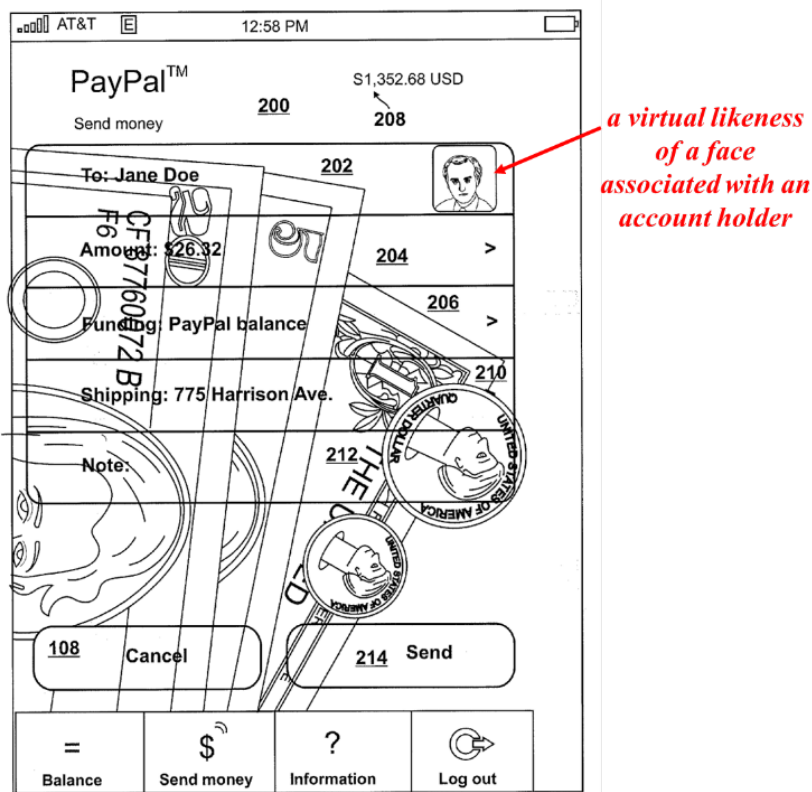


FIG. 2

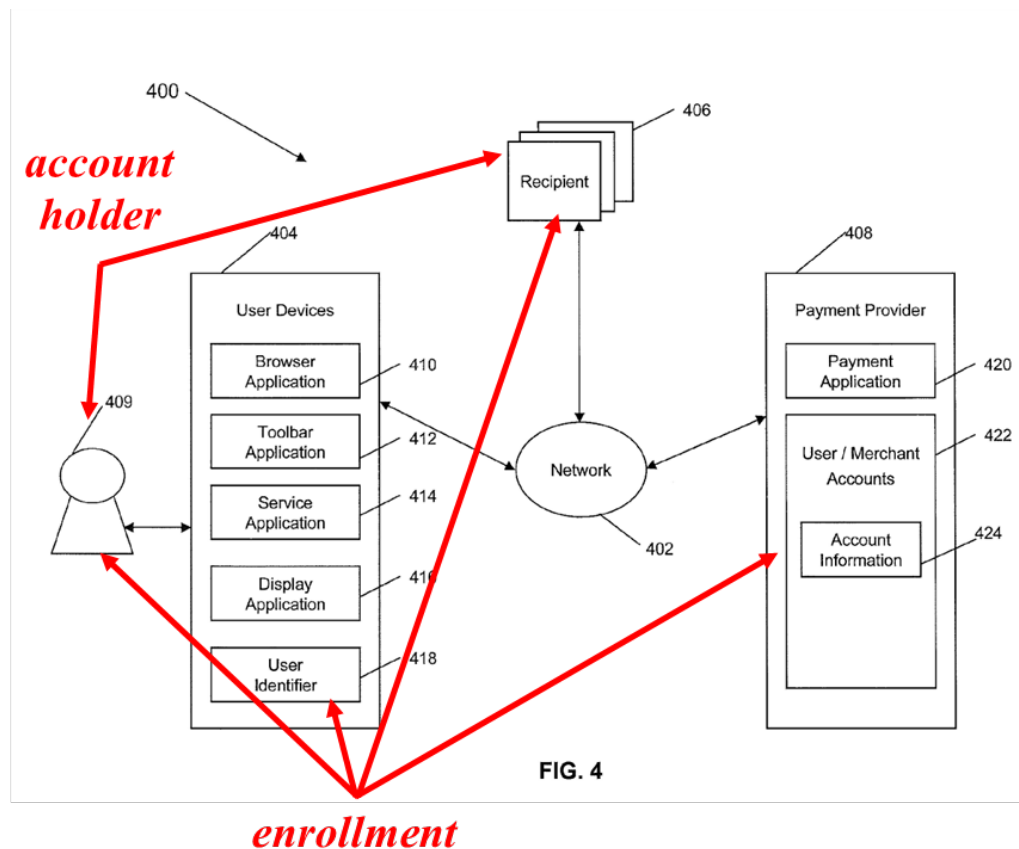
### APPL-1008, FIG. 2, annotated

99. Therefore, Stone discloses or at least 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;*

**100.** Stone discloses or at least renders obvious this element.

**101.** Stone discloses that the virtual likeness of the face (displayed photograph of the account holder of either sender or recipient) was selected by the account holder as part of an enrollment/registration, during which the account holder (user 409) registers, using user device 404 and user identifier 418, with the payment provider 408 and generates a user account 422 including account information 424, where the user identifier 418 includes photograph selected by the user (e.g., used for display on virtual currency, profile icon, etc.). Similar features apply to recipient account holder.



APPL-1008, FIG. 4, annotated

102. Specifically, Stone describes that user identifier 418 of user device 408 “may include attributes related to the user, such as personal information (e.g., a user name, password, photograph image, biometric id, address, phone number, etc.) and banking information).” APPL-1008, [0045].

103. The photograph image of user identifier 418 teaches the virtual likeness of the face as recited in [1.2.1], because Stone teaches that “user identifier 418 may be passed with a user money transfer request to payment provider server 408, and user identifier 418 may be used by payment provider server 408 to

associate user 409 with a particular user account maintained by payment provider server 408.” APPL-1008, [0045], [0048] (“In one embodiment, payment provider server 408 may be configured to maintain a plurality of user and recipient accounts 422, **each of which may include account information 424 associated with individual users**, including user 409, and the one or more recipient device 406.”) Similarly, for a recipient as the account holder, the virtual likeness of the face was selected by the recipient as part of an enrollment. APPL-1008, [0046] (“recipient devices 406 may be the same or have the same basic features as user device 404,” and “recipient devices 406 may include attributes related to the recipient, such as personal and banking information, as well as icon information.”).

**104.** A POSITA would have understood that Stone’s user account registration process teaches the enrollment process as claimed, where the user selects its photograph as its user profile icon during the enrollment/registration process (e.g., including biometric enrollment of user registration/enrollment). Furthermore, Stone teaches an enrollment process, because it was well-known that “biometric id” of its user identifier 418 was captured during an enrollment process, where the stored biometric id (often referred to as “enrollment” biometric data) is used as “enrollment data” for comparison with the later captured data for authentication. A POSITA would have understood that “biometric id” means “biometric identification information.” APPL-1013, [0079] (“obtaining biometric

identification information (e.g., fingerprints, retinal scans, or the like),” APPL-1014, [0009]; (Heusch) APPL-1021, Abstract; (Draper) APPL-1023, 8:3-9:39; (Hoyos) APPL-1013, [0003]; (Yu) APPL-1024, 3:6-11.

**105.** 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 an enrollment with a service provider, and the selected user image is then used for display, e.g. for profile image display or for using the image displayed on the currency as discussed above regarding FIG. 2 of Stone. 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] (describing another example for transferring fund by sliding the visual currency to a recipient icon on the display, such as a picture of the recipient); (Hanif), APPL-1036, [0002] (application from Stone’s common-assignee 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 such that the user could determine which image to use as

the profile image for display both on its own display and on other users' display, for benefits including for example, "increase[ing] a level of trust between [buyers and sellers to] increase online sales and corresponding profits"). (Hanif), APPL-1036, [0006]; 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 to other like-minded people in the ad hoc networking process. In some implementations, the user can select profile image 504 from pictures stored on mobile device 500."**)

106. Furthermore, Stone's disclosure of enrollment/registration is consistent with the description of the '886 patent. Specifically, the '886 patent uses "enrollment" and "registration" interchangeably, and describes an enrollment/registration process with an online retailer. APPL-1001, 5:39-41, 7:64-8:1 ("as part of an enrollment process, Alice was asked to photograph herself...As part of the checkout process, Alice is shown the image she provided at registration (502)").

107. Therefore, Stone discloses or renders obvious this element.

*[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*

108. Stone in view of Hoyos and Varghese renders this element obvious.

109. First, as shown in annotated FIGS. 2 and 3 of Stone below, each of the

annotated control elements/blocks (e.g., “\$Send money,” 202, 206, 214, personalized currency, blocks 300, 302, 306, 312, 314, and 316) and other control elements (e.g., (“Send,” “Confirm,” or “Proceed”)) 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 annotated control elements/blocks is implemented 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.



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-1008, [0024] (“a send button 214 to transfer the funds in noted in box 204.”); APPL-1008, [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].

**112.** 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] (describing using icons for improved visual presentation, stating “the display may show the specific card, such as a PayPal card, Visa, MC, AMEX, etc., as contrasted to a generic representation of a card or no visual at all.”), [0035]; see also e.g., APPL-1008, [0024] (“In this example, display 200 has a name box 202

indicating the recipient of funds as well as a picture of the recipient, ... and a send button 214 to transfer the funds in noted in box 204.”), [0025] (describing “[s]ending can be the user tapping on an appropriate button on the display, such as ‘Send,’ ‘Confirm,’ or ‘Proceed’, where a POSITA would have understood to implement “Confirm?” (block 316) of FIG. 3); APPL-1008, [0020], [0036] (describing “drag[ging] the currency to the other user’s icon to transfer the funds to the other user,” or sliding the currency to the recipient’s icon). It was well-known that clicking/tapping on/sliding/dragging (including from/to) an icon by a user discloses an “an interaction by a user with an icon” as claimed. APPL-1020, 27, 34-36; APPL-1019, 6:24-26.

**113.** 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.” (Varghese) 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. (Varghese) 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”).

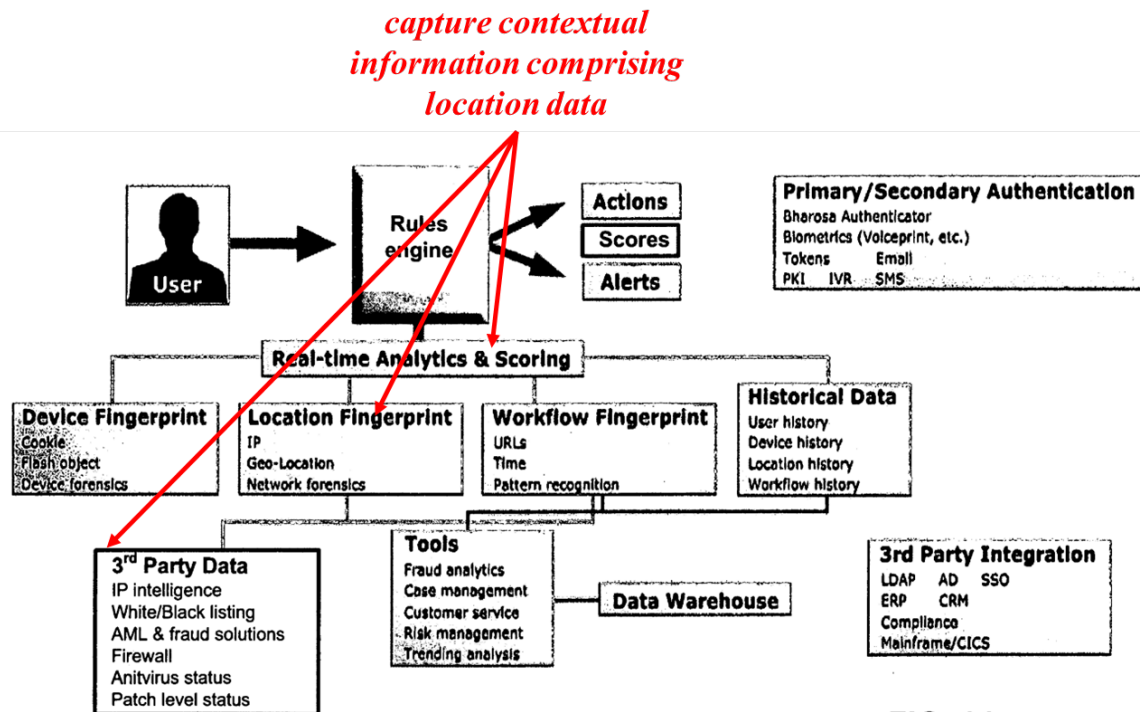


FIG. 14

(Varghese) APPL-1010, FIG. 14, annotated

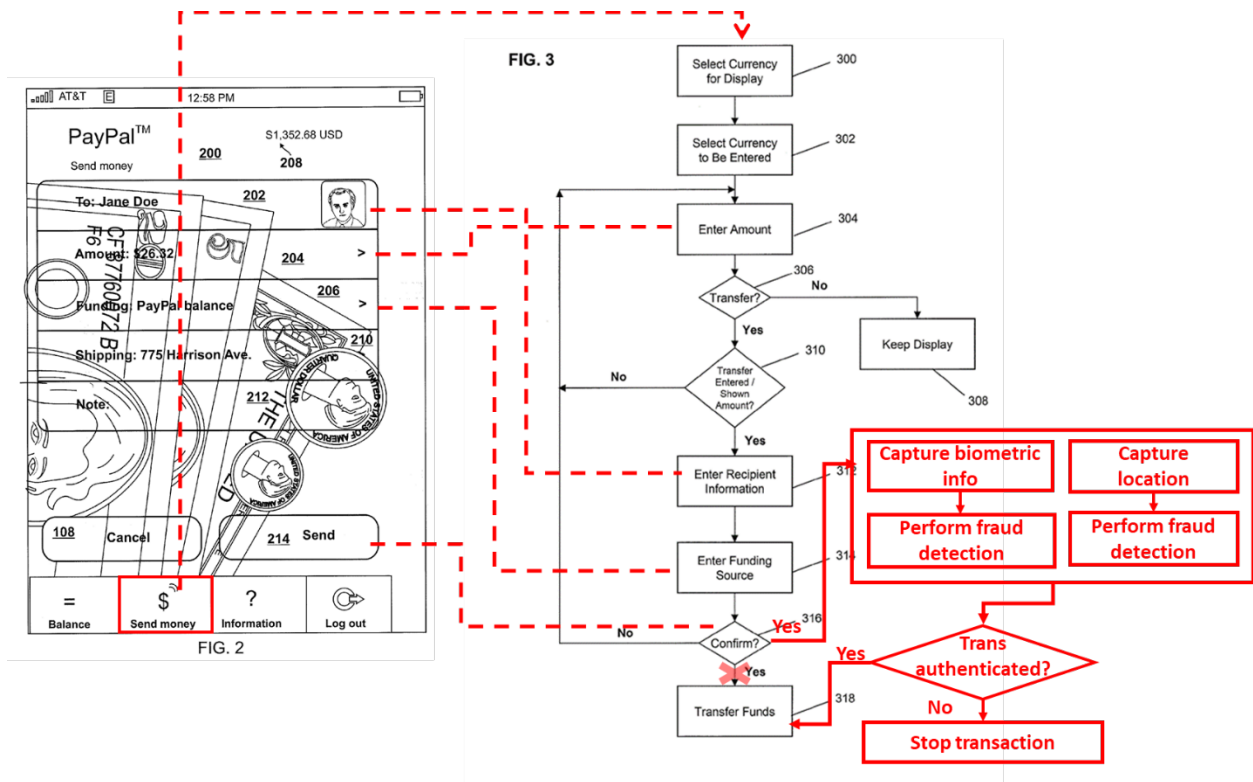
**114.** A POSITA would have understood “real-time” authentication as described in Varghese includes both real-time capture and real-time analysis of authentication data, which provides more accurate fraud analysis by using more accurate, real-time data. (Carter) APPL-1016, [0043] (describing real-time GPS capture for GPS location authentication, where “[a high value] transaction will be prevented unless the person is identified to be a specific location. For example, a mortgage may be prevented from closing if the person is not in a bank” as verified by GPS location); [0044] (describing obtaining “the location of the transaction” to determine “the level of authentication”); (Bansal) APPL-1035, 4:60-62 (describing real-time authentication data capture (e.g., real-time voice print authentication) has the benefit to “avoid imposters from communicating based on stolen biometric data”), 4:66-67 (describing using various “**real-time biometric data** such as voice prints, retina scans for fingerprint recordings”).

**115.** Varghese’s location data captured for “post-authentication” is contextual information of the transaction, e.g., a user location from which the transaction request originates. APPL-1010, [0081] (“Rule Conditions Useful in Device and **Location Fingerprinting**”), [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.

**116. Third**, as discussed at VII.B.3, a POSITA would have been motivated to apply Varghese’s teaching of real-time multi-factor authentication including location authentication (capturing location data and performing fraud analysis based thereupon) after user transaction request confirmation in the electronic financial transaction system of Stone, which is performed **subsequent to** user transaction confirmation (e.g., after user interaction with any of the icons for initiating, continuing, and confirming the transaction request) for improved security.

**117.** Based on the combined functionality of the improved financial transaction system with real-time multi-factor authentication including location authentication, a POSITA would have been motivated to implement the following example Stone-Hoyos-Varghese for performing a financial transaction:



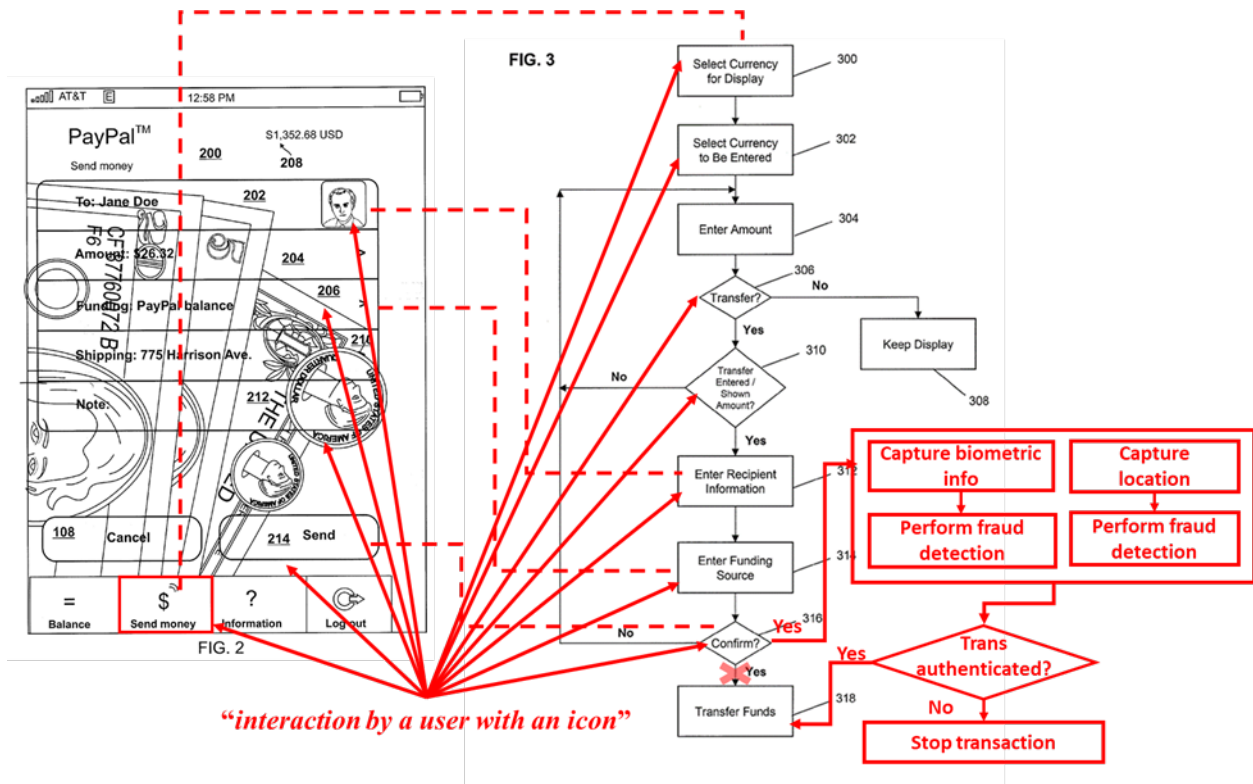
### Example of Stone-Hoyos-Varghese

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

118. As shown in the example of Stone-Hoyos-Varghese above, a POSITA would have been motivated to implement Varghese's teaching for real-time multi-factor authentication (including capturing 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., block 316) the transaction request. This has various benefits over the alternative design choice of using a previously captured and stored authentication 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 block 316) for improved security.

**119.** 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 multi-factor 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)

120. 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), 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

121. Stone in view of Hoyos and Varghese renders this element obvious.

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

**123. 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-1013, [0017] (“a method of authenticating financial transactions comprising **acquiring biometric data from a person**, calculating probability of liveness,  $P_p$ , of the person and probability of a match,  $P_m$ , between the person and known biometric information...”).

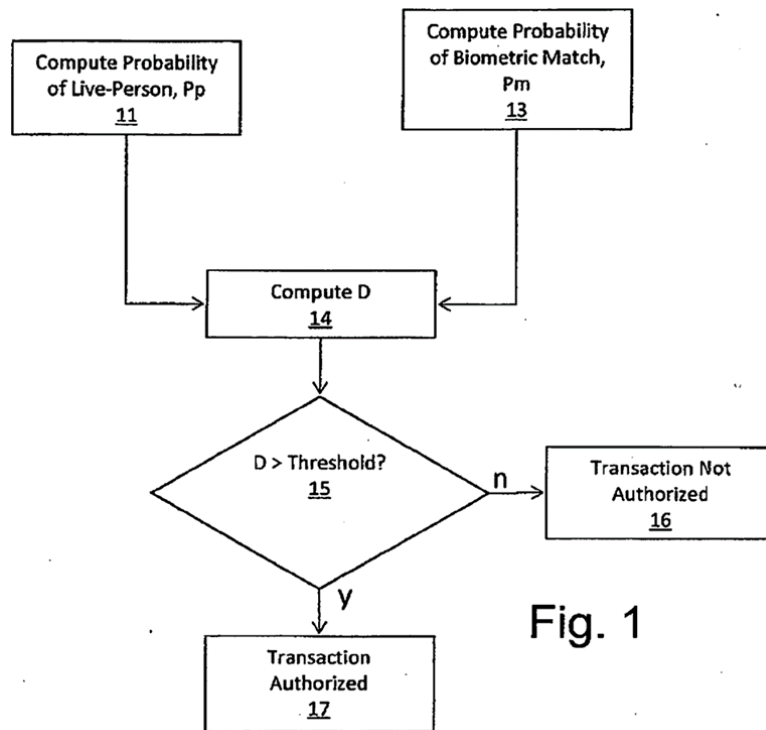


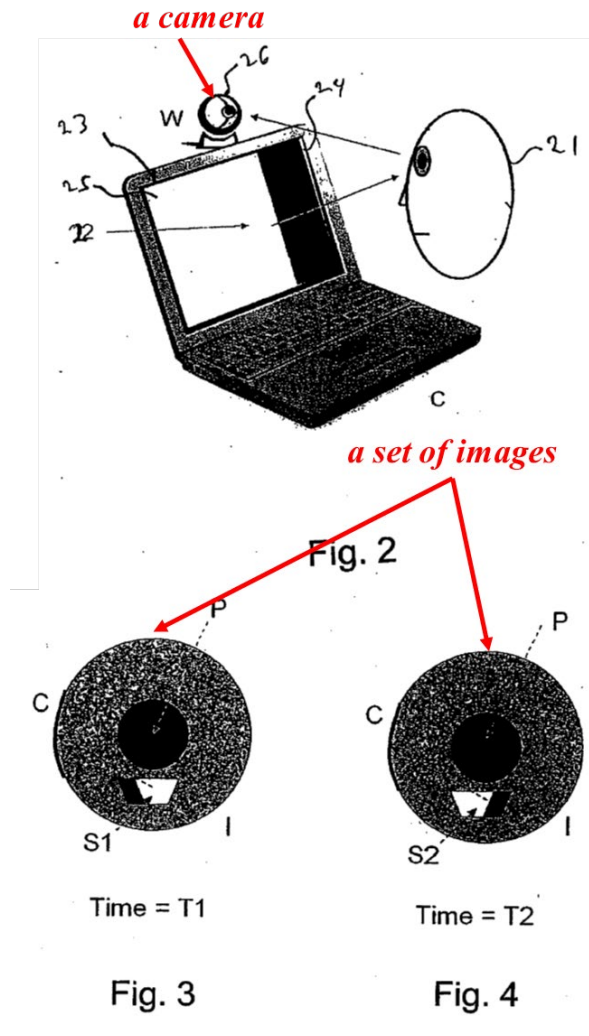
Fig. 1

APPL-1013, FIG. 1

**124.** 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), in addition to “finger or palm temperature,” images for “facial features” comparison, “iris recognition, fingerprint image recognition, finger vein image recognition, or palm vein image recognition,” “other imagery,” and/or other authentication information “as will occur to those ordinarily skilled in the pertinent arts.” APPL-1013, [0003], [0012], [0018]-[0022], [0040]. 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.

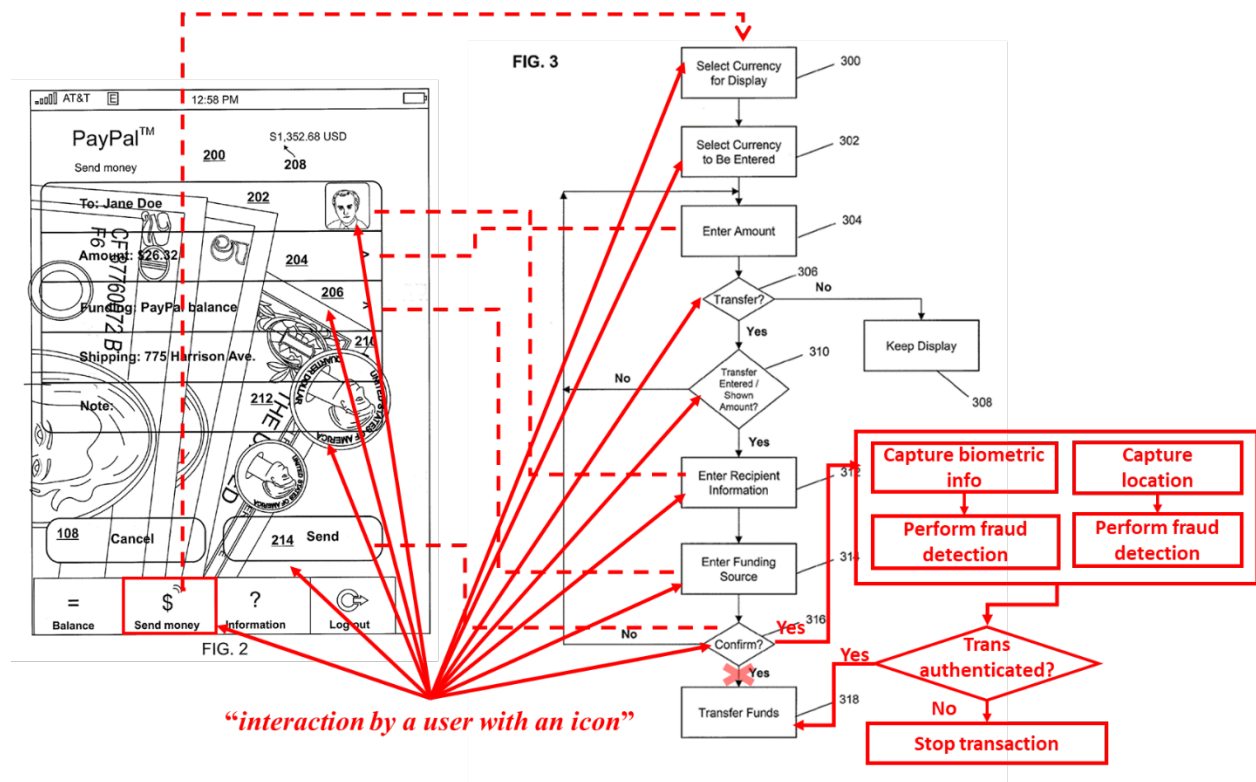
**125.** As an example, and shown in annotated FIGS. 2, 3, and 4 of Hoyos below, Hoyos describes capturing the set of biometric information comprises capturing, using a camera (web-camera 26), a set of images (“obtaining first image of a user positioned in front of a computer screen from a first perspective; 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-1013, [0018]-[0020], claim 7.



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

**126. 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. APPL-1013, [0015]; APPL-1008, [0004] (Stone describing user devices well-known to be easily connected to/include a camera for obtain photographs); (Chatterjee) APPL-1009, 15:22-23 (“The [user profile] pictures can be created using a digital camera function of mobile device 500”).



### Example of Stone-Hoyos-Varghese

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

127. In Stone-Hoyos-Varghese, by authorizing transactions “by combining in one algorithm the live-person result with the match result” as taught by Hoyos, various advantages are achieved, including addressing spoofing; “making it much more difficult for an attempted fraudster to refine fraudulent methods” by

eliminating clear feedback; greatly reducing “the reject rate of true authentications” by using the liveness probability that is less sensitive to conditions like illumination changes; providing “an enormous deterrent to criminals since the system is acquiring biometric data that they have no idea can or cannot be used successfully as evidence against them;” and by ensuring that some live-person data is captured, providing “a means to perform customer redress.” APPL-1013, [0024], [0026], [0027], [0029].

**128.** Implementations of biometric authentication systems as taught by Hoyos in financial transaction systems, and the benefits of liveness detection in fraud detection for anti-spoofing were well-known in the art. APPL-1013, Title, claim 1; APPL-1010, [0079]; APPL-1013, [0011]; *see also* VII.B.2: Combination of Stone and Hoyos.

**129.** For the reasons discussed at VII.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 images for liveness analysis and as an input image for biometric information 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.

**130.** 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 ((Hoyos) APPL-1012, [0028]), capturing real-time, more accurate data that leads to more accurate and improved fraud detection and security ((Varghese) APPL-1010, FIG. 14, [0097]-[0099], TABLE 10), APPL-1015, FIG. 4).

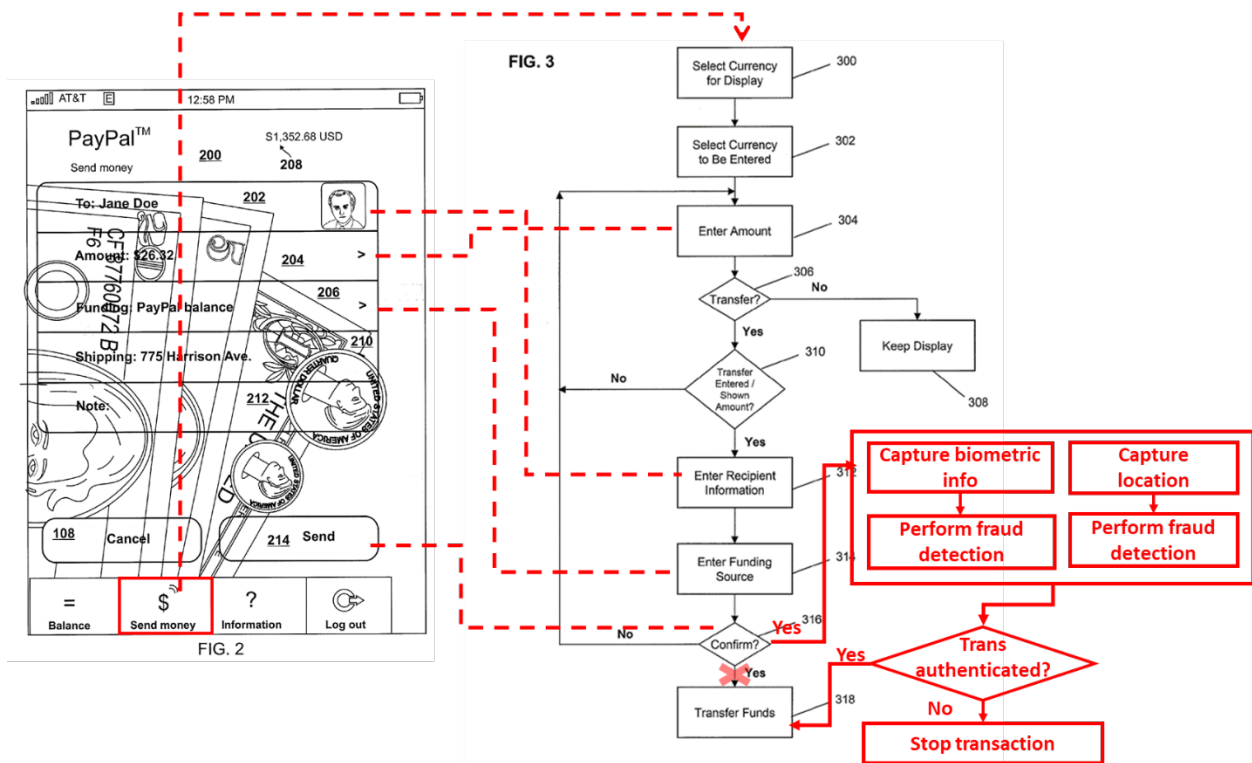
**131.** Therefore, Stone-Hoyos-Varghese renders obvious this element.

**[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*

**132.** Stone in view of Hoyos and Varghese renders this element obvious.

**133. First,** continuing with Stone-Hoyos-Varghese discussed at [1.3.1]-[1.3.2], 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-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)

134. **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.”).

*facilitate a fraud detection  
analysis...based at least in part on:  
the physical location*

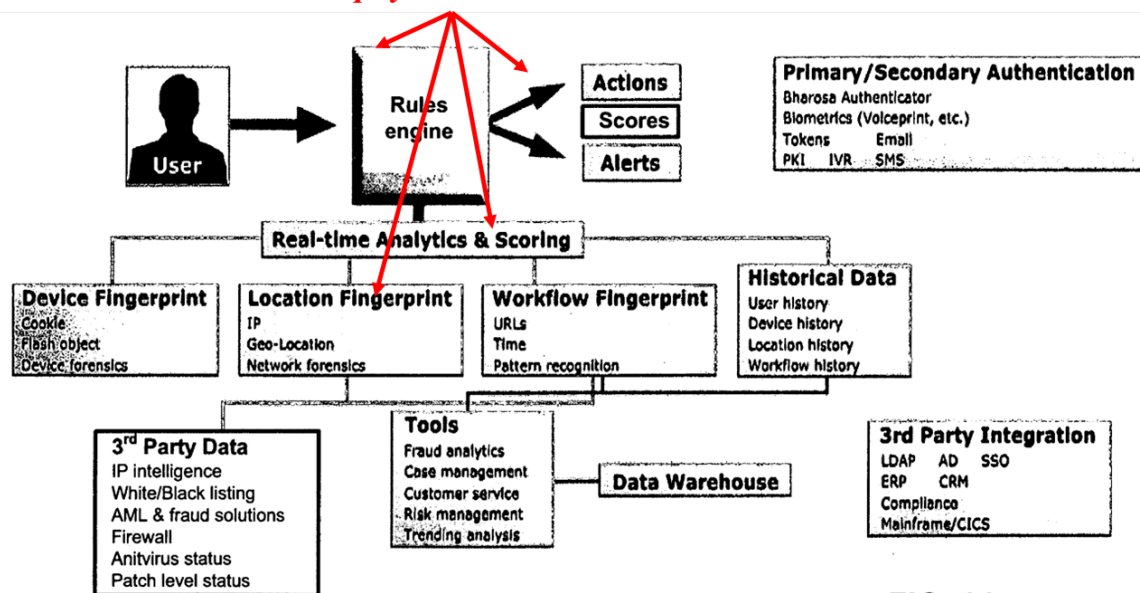


FIG. 14

APPL-1010, FIG. 14, annotated

135. As discussed at [1.3.1], in Stone-Hoyos-Varghese, a POSITA would

have been motivated to apply Varghese's teachings of real-time multi-factor 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-1016, [0036], [0043] (describing the well-known knowledge to implement multi-factor 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); VII.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*

**136.** Stone in view of Hoyos and Varghese renders this element obvious.

**137. 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.

**138. 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-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.

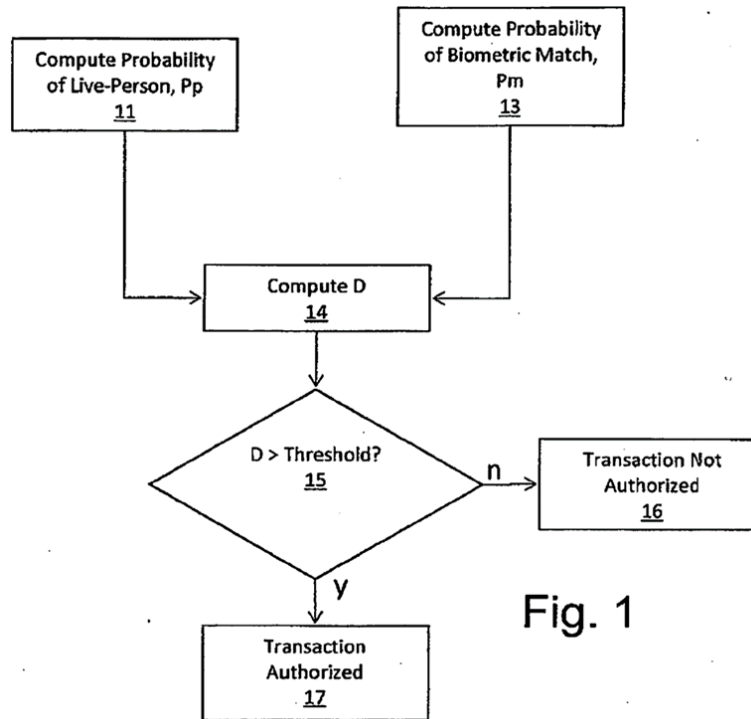


Fig. 1

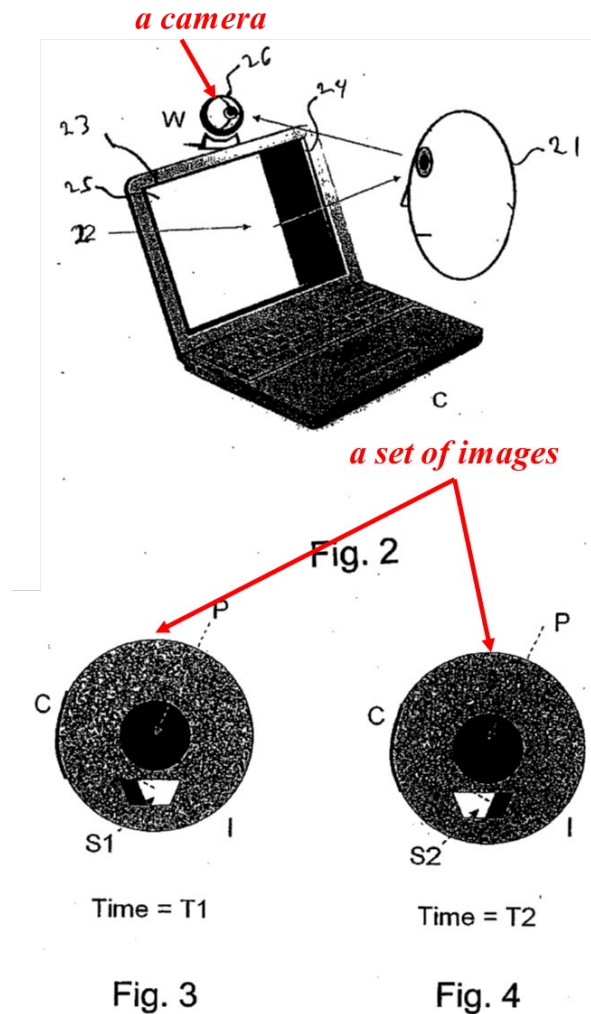
APPL-1013, FIG. 1

**139. 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-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]. It was well-known to capture a sequence of images (e.g., video) and use adjacent (successively captured) images/frames of a human face for liveness analysis. APPL-1011, Abstract; APPL-1012, Abstract.

**140.** 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-1013, [0035] (“The difference between the two images is recorded and the difference at each pixel is squared. The images are then blurred by convolving with a low-pass filter and then threshold the image. Areas above threshold are areas of change between the two images. The system expects to see a change primarily on the cornea, where a sharp image of the screen is reflected.”); [0036] (“Referring to FIGS. 3 and 4 which represent cornea C with pupil P and section S1 at time T1 and S2 at time T2, with I representing an iris, given the curved geometry of the cornea, for a live curved and reflective cornea, the black and white area should have a particular curved shape—specifically a curved black bar and a curved white area (much like a fish-eye lens view). A template of the expected view is correlated with the first image obtained on the web-camera only in the region of the eye as detected by the prior step), and the peak value of the correlation is detected. The process is then repeated with the template expected from the second image.”); [0037] (“The minimum of the two

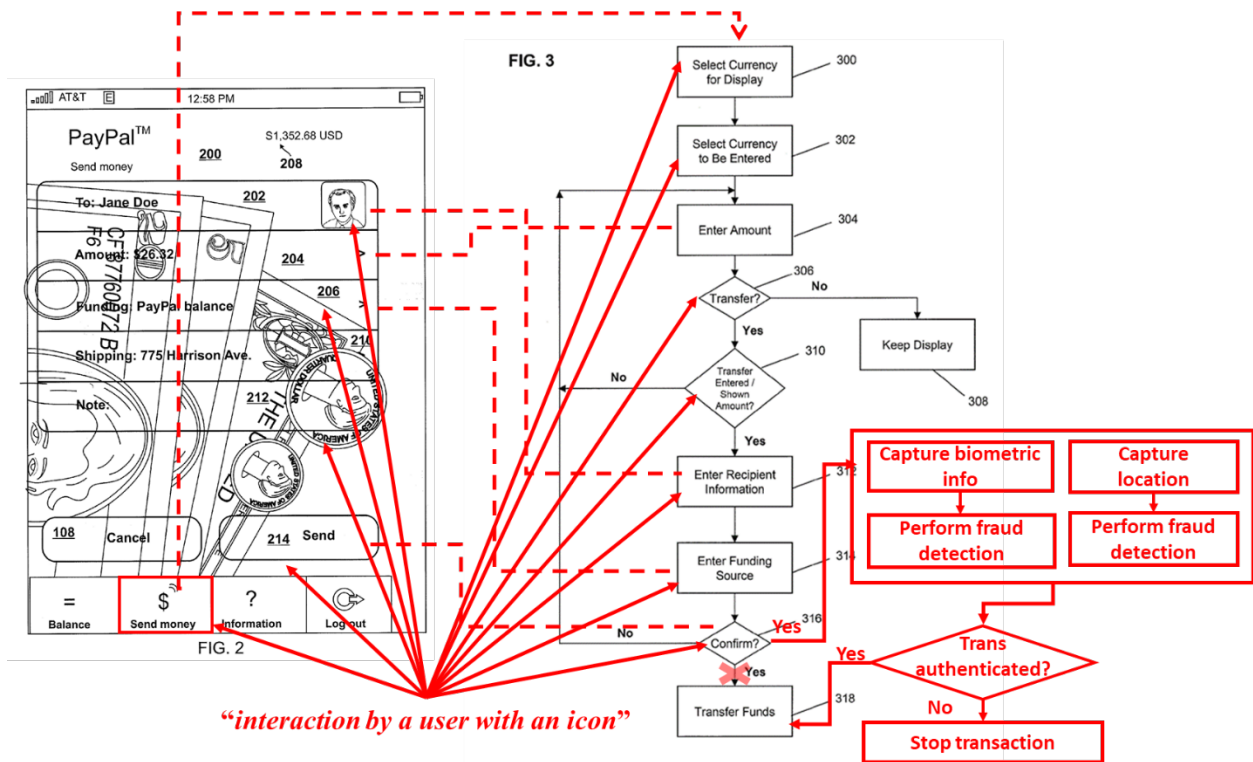
correlation scores (which will lie between -1 to 1) is correlated and normalized it to be between 0 and 1 by adding 1 and dividing by 2. This is the probability of measure of liveness= $P(p)$ .”).



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

**141.** Continuing with the combination as discussed at [1.3.1], [1.3.2], and [1.4.1], 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 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. APPL-1013, [0015]; *see also* VII.B.2, APPL-1008, [0045]; APPL-1010, [0079].



### Example of Stone-Hoyos-Varghese

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

142. 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.***

**143.** Stone discloses or at least renders obvious this element.

**144.** 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.

**145.** 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].

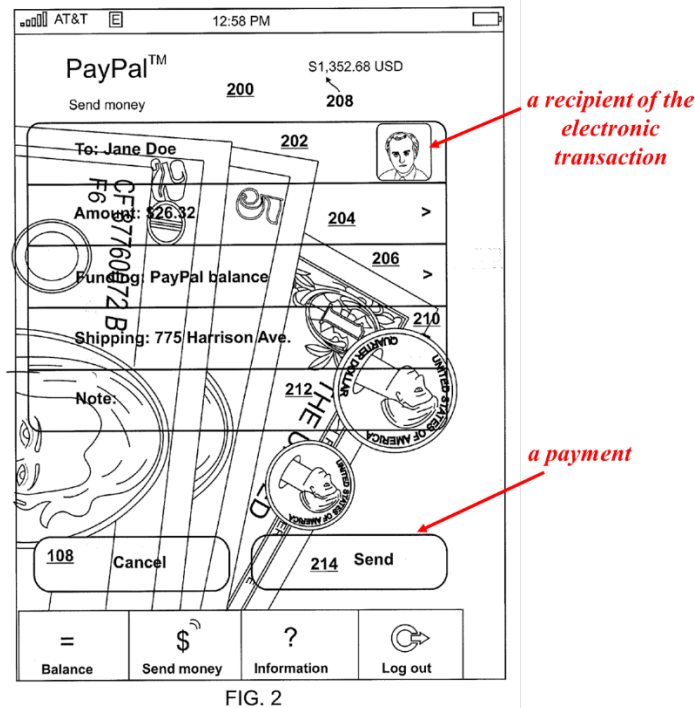
**146.** Therefore, Stone discloses or at least renders obvious this limitation, and Stone-Hoyos-Varghese renders obvious claim 1 in its entirety.

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.*

147. Stone discloses or renders obvious this element.

148. 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”).



APPL-1008, FIG. 2, annotated

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

### 6. Claim 3

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

150. Stone discloses or renders obvious this element.

151. **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].



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.”

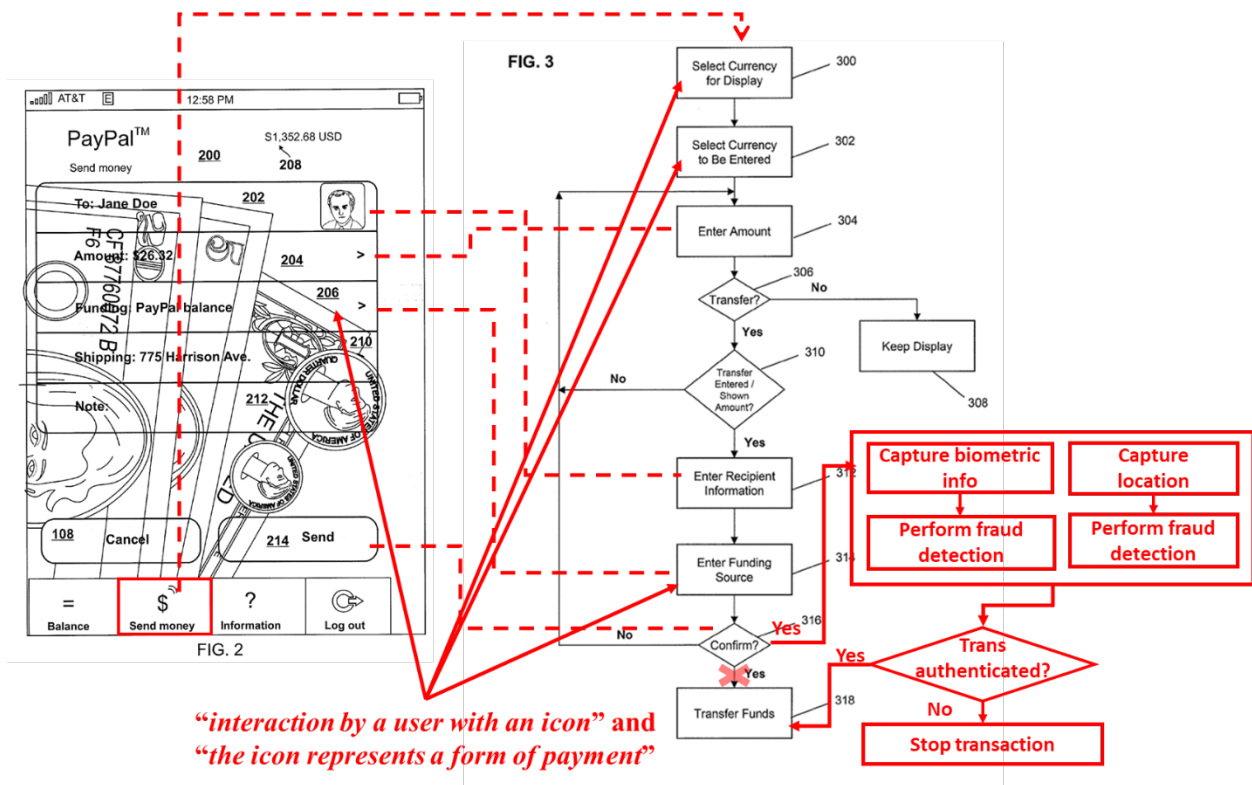
APPL-1008, [0035]. Further, Stone itself describes using a visual image to present the selected funding source in the display. APPL-1008, [0038] (“the display may

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).



**Example of Stone-Hoyos-Varghese**

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

**153. 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.

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

**7. Claim 4**

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

**155.** Stone-Hoyos-Varghese renders obvious this element.

**156.** 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.

**157. 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”).

**158. 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].

**159.** 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-1009, 9:30-35.

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

## **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.***

**161.** Stone discloses or renders obvious this element.

**162.** Specifically, Stone describes user device 404 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,” which displays one or more interfaces (e.g., FIG. 2) as discussed above. (Stone) APPL-1008, [0006] (“The user’s device, such as a mobile phone, displays the actual currency representing the entered amount on background of the display or screen.”), [0022], [0024], [0041], [0044], [0046]. A POSITA would have understood that the system of Stone includes user devices of different types and Internet connections (e.g., Wi-

Fi, landline, mobile network, etc.) to cater to a broader customer base by accommodating diverse user preferences and user devices, where the user devices include at least one of a phone, a tablet device, or a laptop.

**163.** Accordingly, Stone discloses or renders obvious this element.

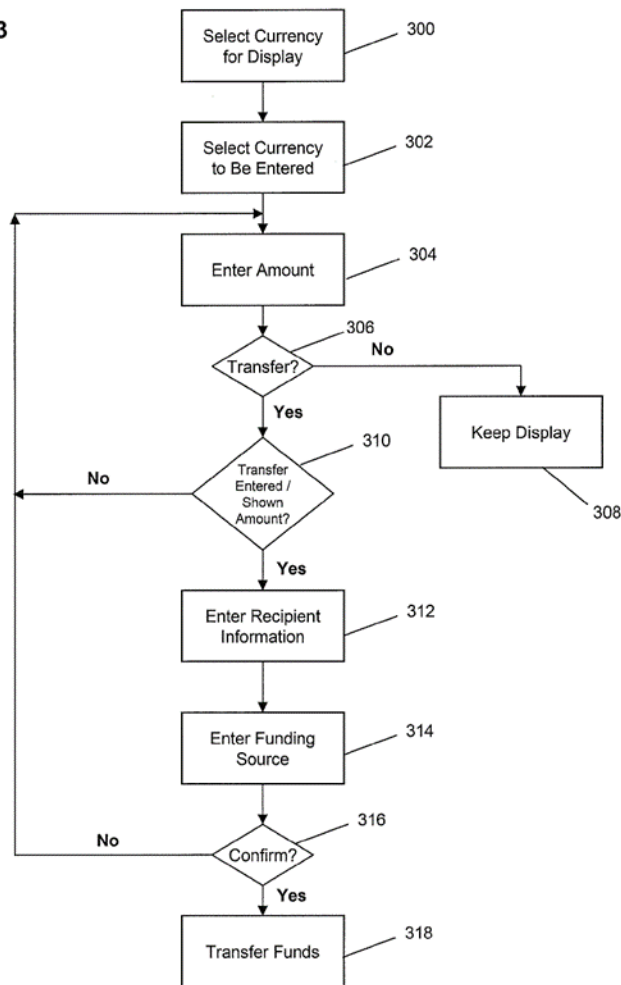
## **9. Claim 6**

**[6.0] *A method, comprising:***

**164.** Stone discloses or at least renders obvious the preamble to the extent that it is limiting.

**165.** 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

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

*[6.1.1] rendering, in one or more interfaces, a virtual likeness of a face associated with an account holder,*

167. Stone discloses or at least renders obvious this element for reasons discussed at [1.2.1].

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

**168.** Stone discloses or at least renders obvious this element for reasons discussed at [1.2.2].

***[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***

**169.** Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [1.3.1].

***[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***

**170.** Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [1.3.2].

***[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***

**171.** Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [1.4.1].

***[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.***

**172.** Stone-Hoyos-Varghese renders obvious this element for reasons

discussed at [1.4.2].

**10. 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.***

**173.** Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [2.0].

**11. Claim 8**

***[8.0] The method of claim 6, wherein the icon represents a form of payment.***

**174.** Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [3.0].

**12. Claim 9**

***[9.0] The method of claim 6, wherein the image comprises at least one of a photograph or an avatar.***

**175.** Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [4.0].

**13. 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.***

**176.** Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [5.0].

**14. Claim 11**

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

**177.** Stone discloses or at least renders obvious the preamble to the extent that it is limiting.

**178.** 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”).

**179.** Therefore, Stone discloses or at least renders obvious this element.

***[11.1.1] rendering, in one or more interfaces, a virtual likeness of a face associated with an account holder, wherein the virtual likeness of the face was selected by the account holder as part of an enrollment;***

**180.** Stone discloses or at least renders obvious this element for reasons discussed at [1.2.1].

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

**181.** S Stone discloses or at least renders obvious this element for reasons discussed at [1.2.2].

***[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***

**182.** Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [1.3.1].

***[11.2.2] [subsequent to an interaction by a user...] capturing a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images; and***

**183.** Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [1.3.2].

***[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***

**184.** Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [1.4.1].

***[11.3.2] [facilitating 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.***

**185.** Stone-Hoyos-Varghese renders obvious this element for reasons discussed at [1.4.2].

**15. Claims 12 and 18**

***[12.0/18.0] The system recited in claim 1/ 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.***

**186.** Stone-Hoyos-Varghese renders obvious this element.

**187.** First, Hoyos discloses that 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.

**188.** Specifically, Hoyos describes that in its fraud detection method using a combination of a probability of a live person  $P_p$  and a probability of a match  $P_m$ , “[t]he probability of a match,  $P_m$ , can be calculated in any way which is desired, for example by iris recognition...”). APPL-1013, [0022]. Hoyos further describes that “[u]sing the method described in Turk, et al., U.S. Pat. No. 5,164,992, **a face recognition match score,  $P_m$** , is calculated and then normalized to be between 0 and 1.” APPL-1013, [0038]; *see also* APPL-1017 (describing the details of a face recognition system); APPL-1013, claim 7. Therefore, a POSITA would have understood that Hoyos’ computing of the face recognition match score  $P_m$  teaches determining whether a face is detected as claimed, because it provides an indication of the probability of whether the stored high-confidence face is detected in the captured images.

**189.** To the extent that Patent Owner argues that Hoyos does not explicitly

teach determining whether a face is detected as claimed, it was well-known to implement POSITA's basic authentication knowledge facial recognition to determine whether a face (e.g., a stored high-confidence user face) is detected as an additional form of authentication, in the financial transaction system of Stone-Hoyos-Varghese for improved security, where "the face biometric is easy to acquire (a web camera for example)." APPL-1013, [0007]; [0003]; APPL-1010, [0145]; APPL-1016, FIG. 4, [0042]. Hoyos, citing Turk, describes face detection as a part of a "system for identifying members of an audience, the system including an imaging system which generates an image of the audience; a selector module for selecting a portion of the generated image; a detection means which analyzes the selected image portion to determine whether an image of a person is present; and a recognition module responsive to the detection means for determining whether a detected image of a person identified by the detection means resembles one of a reference set of images of individuals." APPL-1013, [0004].

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

**16. Claims 14 and 20**

***[14.0/20.0] The system recited in claim 1, wherein the set of images comprises a plurality of images successively captured using the camera.***

**191.** Stone-Hoyos-Varghese renders obvious this element.

**192.** Continuing with Stone-Hoyos-Varghese as discussed at [1.3.2], as

shown in FIGS. 3 and 4 of Hoyos below, in Hoyos, 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]. It was well-known to capture a sequence of images (e.g., video) and use adjacent (successively captured) images/frames of a human face for liveness analysis. APPL-1011, Abstract; APPL-1012, Abstract.

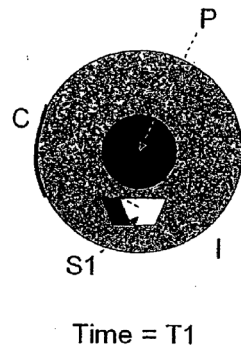


Fig. 3

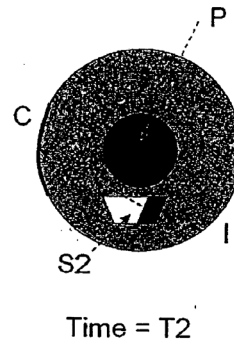


Fig. 4

**APPL-1013, FIGS. 3 and 4**

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

**17. Claims 15 and 21**

***[15.0/21.0] The system recited in claim 1/method of claim 6, wherein the set of captured biometric information further comprises an audio sample.***

194. Stone-Hoyos-Varghese renders obvious this element.

**195.** First, as shown in annotated FIG. 14 of Varghese below, Varghese describes real-time multi-factor authentication including voice authentication, which includes capturing biometric information including an audio sample. APPL-1010, FIG. 14, [0078] (describing a higher level of security implemented to include “call to provide voice **recognition**”), [0079], [0084] (“a voiceprint which can require a user to verbally []response to a challenge”). A POSITA would have understood that Varghese’s obtaining biometric data with “call to provide voice recognition,” “requiring a user’s verbal response” teaches capturing an audio sample for voice recognition. (Campbell) APPL-1033, FIG. 3 (illustrating that a generic speaker-verification system includes capturing an audio sample (speech captured by Microphone)).

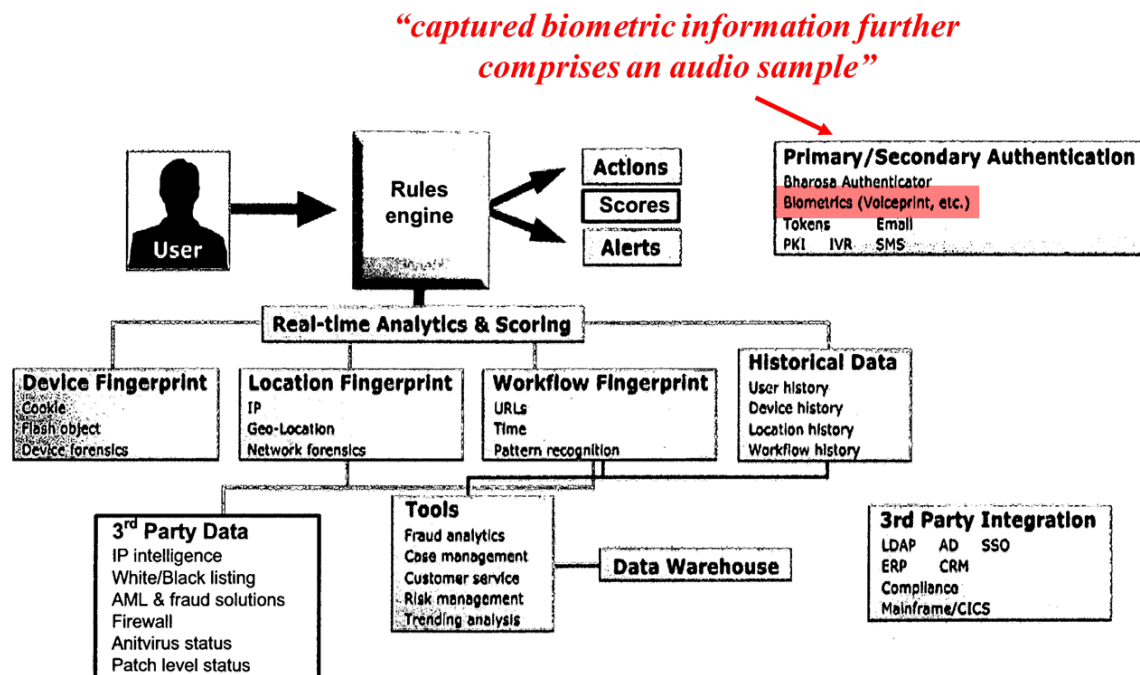


**FIG. 14**

**APPL-1010, FIG. 14, annotated**

196. **Second**, continuing with Stone-Hoyos-Varghese of claim 1, a POSITA would have been motivated to implement the multi-factor authentications including voice authentication as taught by Varghese for improved security. APPL-1010, [0145]; APPL-1018, 51:12-15, 52:20-24; APPL-1016, FIG. 4, [0036], [0040]-[0041] (describing multi-factor authentications including voice biometric validation); (Campbell) APPL-1033, 1438 (speaker recognition methods “are probably **the most natural and economical methods** for solving the problems of unauthorized use of computer and communications systems and multilevel access control”); VII.B.3.

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

**18. Claims 16 and 22**

*[16.0/22.0] The system recited in claim 15/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.*

198. Stone-Hoyos-Varghese renders obvious this element.

199. Continuing with Stone-Hoyos-Varghese of claims 15/21, 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). APPL-1016, [0036], [0040]-[0041]; APPL-1018, 51:12-15; (Campbell) APPL-1033, FIG. 3 (illustrating that a generic speaker-verification system includes making an accept/reject decision based on a determination of whether the audio sample (speech captured by Microphone) matches a previously recorded voice sample (“Verified ID”)).

**200.** Accordingly, in view of POSITA’s fundamental and basic knowledge of biometric authentication, Stone-Hoyos-Varghese performs biometric authentication decision (accept/reject) based on the captured audio sample for improved security, based on a determination of whether the audio sample matches a previously recorded voice sample. APPL-1010, [0145].

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

## **19. Claims 17 and 23**

***[17.0/23.0] The system recited in claim 16/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.***

**202.** Stone-Hoyos-Varghese renders obvious this element.

**203.** 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 a Fast Fourier Transform (FFT), because the 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. (Campbell) APPL-1033, 1445 (describing using the FFT for frequency feature extraction for speaker recognition); (Nucci) APPL-1031, 12:15-19 (describing using the FFT for feature extraction for speaker recognition); (Bilobrov) APPL-1032, FIG. 2 (illustrating using the FFT for voice fingerprint).

**204.** Accordingly, continuing with Stone-Hoyos-Varghese of claims 16/22, in view of POSITA's fundamental and basic knowledge of using the FFT for speaker recognition, Stone-Hoyos-Varghese performs determination of whether the audio samples match based on performing an FFT, which renders obvious this element. APPL-1010, [0145].

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

**205.** 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.

**1. Combination of Stone and Guidance ("Stone-Guidance")**

**206.** 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.

**207. First**, as discussed at VII.A.5, Guidance is analogous art to the '886 patent.

**208. Second**, Guidance “addresses why financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services.” APPL-1037, 1. A POSITA would have understood that the multifactor real-time risk-based authentication taught by Guidance provides “improved authentication technologies” for reducing fraud and identity theft and improving customer protection, even for service providers of financial transactions not regulated by FFIEC. APPL-1022, 1. As such, a POSITA would have been motivated to apply the multifactor real-time risk-based authentication taught by Guidance in Stone, because Stone had a need for authentication for fraud detection (e.g., with higher levels of security for higher-risk financial transactions), and because the Guidance was a recognized driver for implementing multi-factor 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]); above at ¶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).

**209. 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-1039, 1; APPL-1008, [0041]-[0042] (Stone describing user devices implemented with various appropriate computing devices (e.g., personal computer, wireless telephone, etc.) with wired and/or wireless communication over network). 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. (Guidance) APPL-1037, 8 ("selection and use of any technique should be based upon the assessed risk associated with a particular electronic banking product or service"); (Carter) APPL-1016, [0036] ("The multi-factor authentication allows for increased authentication requirements as the value of the transaction increases," where "higher authentication levels may require different types of authentication.")). 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).

## 2. Claim 1

***[1.0] A system, comprising:***

**210.** Stone discloses or renders obvious the preamble to the extent that it is limiting for the reasons discussed at Ground 1:[1.0].

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

**211.** Stone alone or Stone-Guidance renders obvious this element.

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

**213. 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.

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

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

**215.** Stone discloses or at least renders obvious this element for the reasons discussed at Ground 1:[1.2.1].

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

**216.** Stone discloses or at least renders obvious this element for the reasons discussed at Ground 1:[1.2.2].

**[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*

**217.** Stone-Guidance renders this element obvious.

**218. 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.



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. (Guidance) APPL-1037, 3, 11-12; (Varghese), APPL-1010, [0035].

**221.** 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. (Varghese), APPL-1010, [0012], [0035]; (Carter) 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. (Hoyos) APPL-1013, [0007]; (Guidance) APPL-1037, 11.

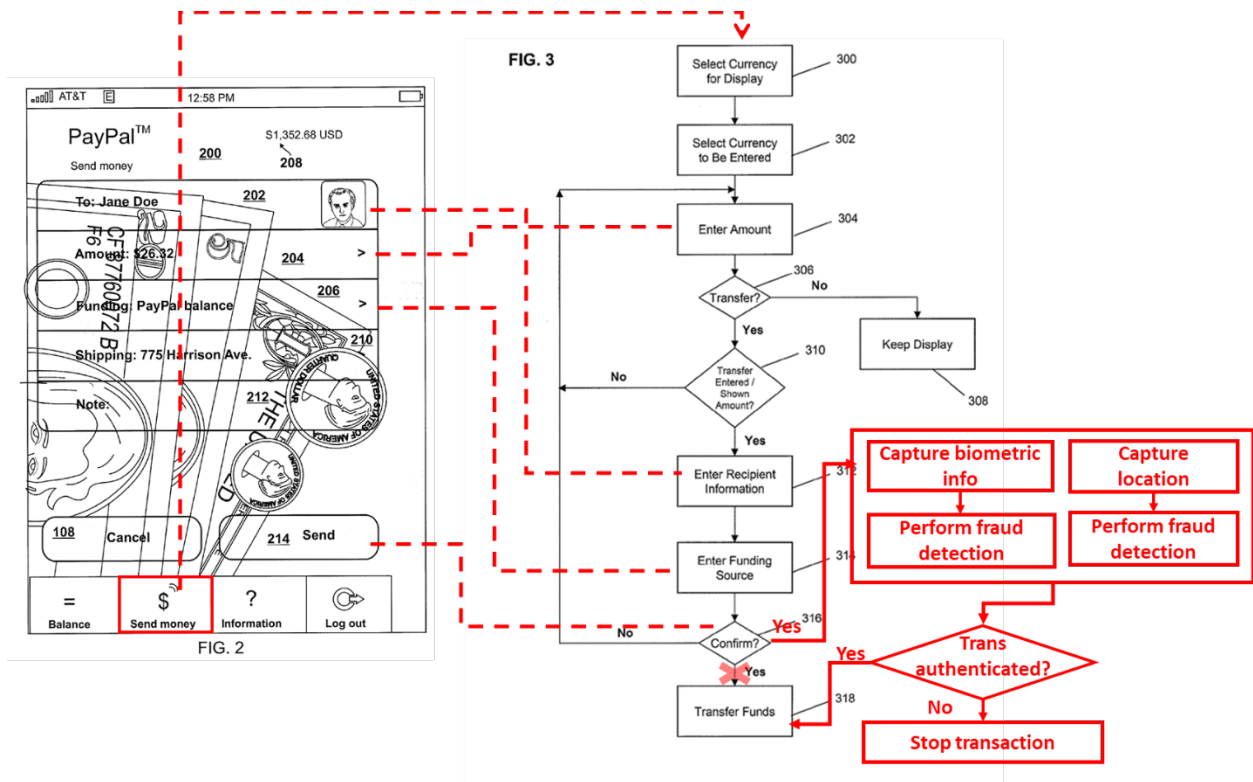
**222.** Guidance’s physical location authentication teaches capturing real-

time location data usable to determine a physical location associated with the user.

(Guidance) APPL-1037, 12. For example, Guidance describes “geo-location technology” to “limit Internet users by determining where they are.” (Guidance) APPL-1037, 12. While Guidance describes an example geo-location technique based on electronic travel times over Internet “may not be suitable for some wireless networks that can also be access the Internet such as cellular/digital telephones,” Stone describes that its system implementing user devices of different types (“mobile phone, laptop computer, PDA, or personal computer,” or “other suitable device”) and various communication connections (“the Internet and/or one or more intranets, landline networks, wireless networks, and/or other appropriate types of communication networks”). APPL-1008, [0022], [0024], [0041], [0044], [0046]. In Stone-Guidance, a POSITA would have been motivated to apply suitable well-known techniques (e.g., Geolocation by IP address as described in Varghese, GPS as described in Stone for location detection, etc.) for capturing location data of different types of user devices (e.g., personal computer, a mobile phone, etc.). (Guidance) APPL-1037, 12-13; (Varghese) 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.”); (Carter) APPL-1016, [0036] (using GPS for capturing mobile device location data); (Stone) 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).

**223. 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. (Guidance) 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)

224. 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).

**225.** 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.

**226.** 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*

**227.** Stone-Guidance renders this element obvious.

**228. 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.

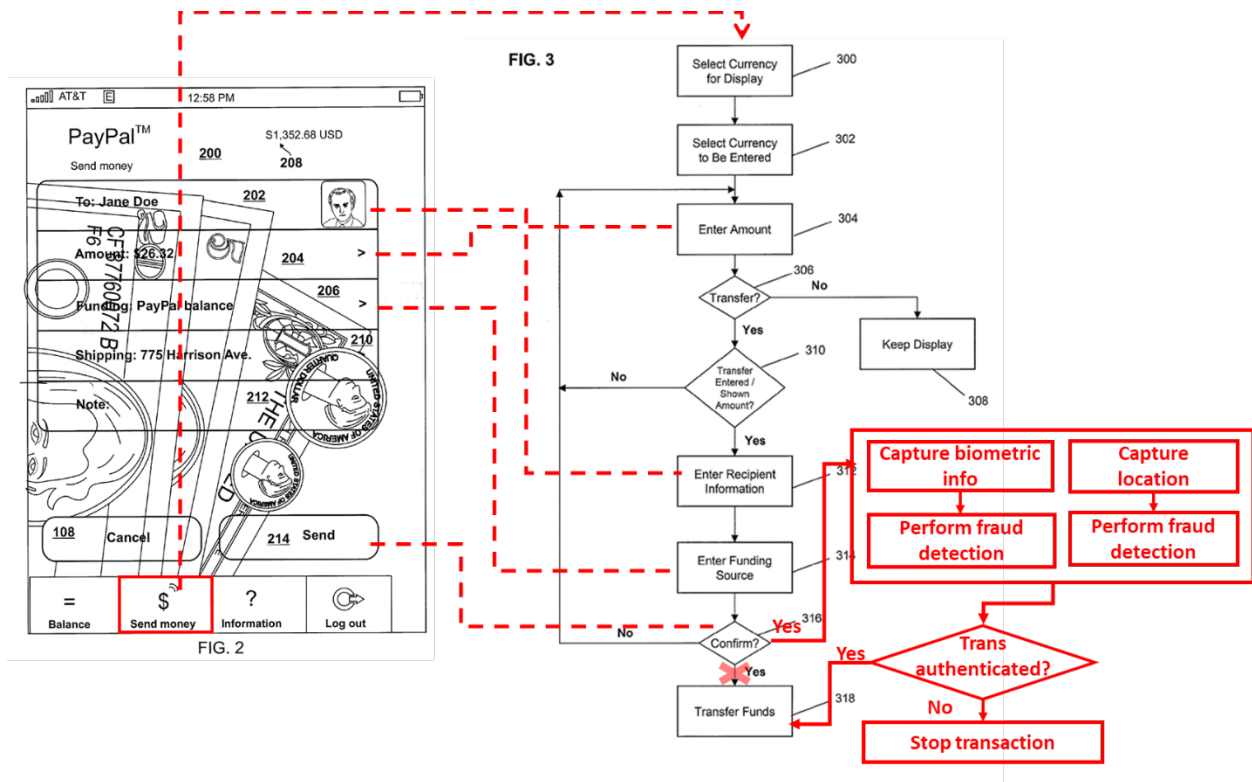
**229. Second**, Guidance's face recognition with liveness tests teaches capturing the set of biometric information comprises capturing, using a camera, a set of images. Specifically, Guidance describes that biometric authentication using face recognition with liveness tests using facial scans captured 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." (Guidance) 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). *See, e.g.*, (Kollreider) APPL-1044, 2; (Hoyos) APPL-1013, FIGs. 2-4, claims 5-6; APPL-1011, Abstract; APPL-1012, Abstract.

**230.** 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*

**231.** Stone-Guidance renders this element obvious.

**232. 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. (Guidance) 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-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)

**233. 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).

**234.** For location authentication, Guidance describes authentication based on “geo-location technology” to “limit Internet users by determining where they are.” (Guidance) 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.,* (Varghese) 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. See, e.g., (Carter) APPL-1016, [0036]; *see also* (Stone), 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).

235. Therefore, Stone-Guidance 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**

236. Stone-Guidance renders this element obvious.

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

238. A POSITA would have been motivated to apply the 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.” (Guidance) APPL-1037, 11.

239. 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.***

240. Stone discloses or at least renders obvious this element for reasons discussed at Ground 1:[1.5].

### 3. 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.***

241. Stone discloses or renders obvious this element for the reasons discussed at Ground 1:[2.0].

### 4. Claim 3

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

242. Stone discloses or renders obvious this element for the reasons discussed at Ground 1:[3.0].

### 5. Claim 4

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

243. Stone-Guidance renders obvious this element.

**244.** 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.

**245. 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. (Guidance) APPL-1037, 11 (“Most face recognition systems focus on **specific features on the face** and make a two-dimensional map of the face. Newer systems make three-dimensional maps. The systems capture facial images from video cameras and generate templates that are stored and used for comparisons.”).

**246. 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-1008, [0007], [0024], [0020], [0036].

**247.** 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-1009, 9:30-35.

**248.** Therefore, Stone-Guidance renders obvious this element.

**6. 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.*

**249.** Stone-Guidance renders obvious this element.

**250. First,** Stone discloses or at least renders obvious this element for reasons discussed Ground 1:[5.0]. APPL-1008, [0004], [0006], [0022], [0024].

**251. Second,** 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. While Guidance describes an example geo-location technique that based on electronic travel times over Internet “may not be suitable for some wireless networks that can also be access the Internet such as cellular/digital telephones,” a POSITA would have applied suitable well-known techniques (e.g., GPS as described in Stone for location detection) for capturing location data of a mobile phone. (Guidance) APPL-1037, 12-13; (Stone) APPL-1008, [0026]; (Carter) APPL-1016, [0036].

**252.** Therefore, Stone-Guidance renders obvious this element.

**7. Claim 6**

**[6.0]** *A method, comprising:*

**253.** Stone discloses or at least renders obvious the preamble to the extent that it is limiting for reasons discussed at Ground 1:[6.0].

***[6.1.1] rendering, in one or more interfaces, a virtual likeness of a face associated with an account holder,***

**254.** Stone discloses or at least renders obvious this element for reasons discussed at Ground 1:[1.2.1].

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

**255.** Stone discloses or at least renders obvious this element for reasons discussed at Ground 1:[1.2.2].

***[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***

**256.** Stone-Guidance renders obvious this element for reasons discussed at Ground 2:[1.3.1].

***[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***

**257.** Stone-Guidance renders obvious this element for reasons discussed at Ground 2:[1.3.2].

***[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***

**258.** Stone-Guidance renders obvious this element for reasons discussed at Ground 2: [1.4.1].

***[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.***

**259.** Stone-Guidance renders obvious this element for reasons discussed at Ground 2: [1.4.2].

**8. 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.***

**260.** Stone discloses or at least renders obvious this element for reasons discussed at Ground 2: [2.0].

**9. Claim 8**

***[8.0] The method of claim 6, wherein the icon represents a form of payment.***

**261.** Stone discloses or at least renders obvious this element for reasons discussed at Ground 2:[3.0].

**10. Claim 9**

***[9.0] The method of claim 6, wherein the image comprises at least one of a photograph or an avatar.***

**262.** Stone discloses or at least renders obvious this element for reasons discussed at Ground 2:[4.0].

**11. 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.***

**263.** Stone-Guidance renders obvious this element for reasons discussed at Ground 2:[5.0].

**12. Claim 11**

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

**264.** Stone discloses or at least renders obvious the preamble to the extent that it is limiting for reasons discussed at Ground 1:[11.0].

***[11.1.1] rendering, in one or more interfaces, a virtual likeness of a face associated with an account holder, wherein the virtual likeness of the face was selected by the account holder as part of an enrollment;***

**265.** Stone discloses or at least renders obvious this element for reasons discussed at Ground 1: [1.2.1].

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

**266.** Stone discloses or at least renders obvious this element for reasons discussed at Ground 1: [1.2.2].

***[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***

**267.** Stone-Guidance renders obvious this element for reasons discussed at Ground 2:[1.3.1].

***[11.2.2] [subsequent to an interaction by a user...] capturing a set of biometric information, wherein capturing the set of biometric information comprises capturing, using a camera, a set of images; and***

**268.** Stone-Guidance renders obvious this element for reasons discussed at Ground 2: [1.3.2].

***[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***

**269.** Stone-Guidance renders obvious this element for reasons discussed at Ground 2: [1.4.1].

***[11.3.2] [facilitating 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.***

**270.** Stone-Guidance renders obvious this element for reasons discussed at Ground 2: [1.4.2].

### **13. Claims 12 and 18**

***[12.0/18.0] The system recited in claim 1/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.***

**271.** Stone-Guidance renders obvious this element.

**272.** As discussed at [1.3.1]-[1.4.2], Stone-Guidance implements multifactor real-time authentication including physical location authentication and biometric authentication including face recognition with liveness test. Guidance

describes that face recognition includes detecting a face in the captured set of images. (Guidance) APPL-1037, 10 (describing detecting a face by “focus[ing] on specific features on the face”); APPL-1017 (describing the details of a face recognition system).

273. Therefore, Stone-Guidance renders obvious this element.

#### 14. Claims 14 and 20

*[14.0/20.0] The system recited in claim 1, wherein the set of images comprises a plurality of images successively captured using the camera.*

274. Stone-Guidance renders obvious this element.

275. As discussed at Ground 2: [1.3.2], Guidance describes that the face recognition with liveness tests using facial scans captured by a camera that is “a video device,” such that the set of images include a plurality of images (frames of a video) successively captured using the video camera device. (Guidance) APPL-1037, 11 (“Most face recognition systems focus on **specific features on the face** and make a two-dimensional map of the face. Newer systems make three-dimensional maps. The systems capture facial images from video cameras and generate templates that are stored and used for comparisons.”). This is consistent with the well-known knowledge that a plurality of video frames (images) captured using a video camera are used to perform liveness test (e.g., based on blinking eyes or other liveness tests). *See, e.g.*, (Kollreider) APPL-1044, 2, APPL-1011,

Abstract; APPL-1012, Abstract.

276. Accordingly, Stone-Guidance renders obvious this element.

**15. Claims 15 and 21**

*[15.0/21.0] The system recited in claim 1/method of claim 6, wherein the set of captured biometric information further comprises an audio sample.*

277. Stone-Guidance renders obvious this element.

278. **First**, Guidance describes real-time multi-factor authentication including “voice authentication,” e.g., by authenticating based on “voice pattern.” (Guidance) APPL-1037, 7 and 10. Guidance also describes that biometric authentication including voice authentication includes capturing results with a “live-scan process” and comparing the results with the registered templates in the system (e.g., voice templates for voice authentication). (Guidance) APPL-1037, 10. (Campbell) APPL-1033, FIG. 3 (illustrating that a generic speaker-verification system includes capturing an audio sample (speech captured by Microphone).

279. 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-1010, [0145]; APPL-1018, 51:12-15, 52:20-24; APPL-1016, FIG. 4, [0036], [0040]-[0041] (describing multi-factor authentications including voice biometric validation); (Campbell) APPL-1033, 1438 (speaker recognition methods “are probably **the most natural and**

**economical methods** for solving the problems of unauthorized use of computer and communications systems and multilevel access control”); *see also* VII.D.1 below.

**280.** Accordingly, Stone-Guidance renders obvious this element.

## **16. Claims 16 and 22**

***[16.0/22.0] The system recited in claim 15/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.***

**281.** Stone-Guidance renders obvious this element.

**282.** Guidance describes that biometric authentication including voice authentication includes capturing results with a “live-scan process” and comparing the results with the registered templates in the system (e.g., voice templates for voice authentication). (Guidance) APPL-1037, 10. In fact, as discussed at Ground 1:[16.0/22.0], 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). APPL-1016, [0036], [0040]-[0041]; APPL-1018, 51:12-15; (Campbell) APPL-1033, FIG. 3.

**283.** Accordingly, Stone-Guidance renders obvious this element.

**17. Claims 17 and 23**

***[17.0/23.0] The system recited in claim 16/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.***

**284.** Stone-Guidance renders obvious this element.

**285.** As discussed at Ground 1:[17.0/23.0], 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 an FFT, because the 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. (Campbell) APPL-1033, 1445; (Nucci) APPL-1031, 12:15-19; (Bilobrov) APPL-1032, FIG. 2.

**286.** Accordingly, in Stone-Guidance implementing multifactor real-time authentication including voice authentication, determination of whether the audio samples match is based on performing an FFT, which renders obvious this element. APPL-1010, [0145].

**D. Grounds 3 and 4: Combination of Stone, Hoyos, Varghese, and Campbell (Ground 3, “Stone-Hoyos-Varghese-Campbell”) and Combination of Stone, Guidance, and Campbell (Ground 4, “Stone-Guidance-Campbell”) render obvious Claims 15-17 and 21-23.**

**287.** The claim analysis for Grounds 3 and 4 rely on the same analysis and evidence as provided for Ground 1 (Stone-Hoyos-Varghese) and Ground 2 (Stone-

Guidance), respectively, expect for where additional analysis is provided, as noted for respective limitations of the claims below. The additional analysis provided below applies for both Grounds 3 and 4.

### **1. Combination of Campbell with Combinations 1 and 2**

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

**289. First,** as discussed at VII.A.5, Campbell is analogous art to the ’886 patent, describing speaker recognition techniques including speaker verification/authentication techniques to reduce fraudulent transactions.

**290. Second,** as discussed at Grounds 1-2: Claims 15-17 and 20-23, in each of Grounds 1-2, a POSITA would have been motivated to implement multifactor authentications including voice authentication for improved security. APPL-1010, [0145]; APPL-1018, 51:12-15, 52:20-24; APPL-1016, FIG. 4, [0036], [0040]-[0041](describing multi-factor authentications including voice biometric validation); (Campbell) APPL-1033, 1438 (speaker recognition is “probably the most natural and economical methods for solving the problems of unauthorized use of computer and communications systems and multilevel access control” with low cost in light of “the ubiquitous telephone network and microphones bundled with

computers”).

**291.** In view of the combination’s need of voice authentication techniques, a POSITA would have been motivated to implement Campbell’s “very popular” speaker recognition techniques using the FFT-based feature extraction in each of Stone-Hoyos-Varghese and Stone-Guidance, because they had “been demonstrated to work well in speaker-recognition systems.” (Campbell) APPL-1033, 1445.

**292.** A POSITA would have reasonably expected to succeed in configuring each of Stone-Hoyos-Varghese and Stone-Guidance to use the well-known recognition techniques using the FFT-based feature extraction of Campbell, since its implementation would have required only routine knowledge well within the skill of a POSITA prior to the earliest effective filing date. For example, Campbell described the FFT-based feature extraction technology “has been demonstrated to work well in speaker-recognition system.” (Campbell) APPL-1033, 1438-1439, Table 2 (listing a sampling of the chronological advancement in the speaker verification technology starting from 1974).

## **2. Claims 15 and 21**

***[15.0/21.0] The system recited in claim 1/method of claim 6, wherein the set of captured biometric information further comprises an audio sample.***

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

**294. First**, as discussed at Grounds 1 and 2: Claims 15 and 21, each of Grounds 1-2 implements multi-factor authentication including voice authentication and renders obvious capturing an audio sample for biometric authentication.

**295. Second**, to the extent that it is argued that each of Grounds 1 and 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. (Campbell) APPL-1033, 1440 (explaining speech signal acquisition, where a microphone converts the acoustic wave into an analog signal, which is then sampled to form a digital signal).

**296.** Accordingly, to implement voice authentication in Grounds 1 and 2, a POSITA would have applied Campbell’s teaching of the fundamental knowledge of capturing the audio sample for voice authentication.

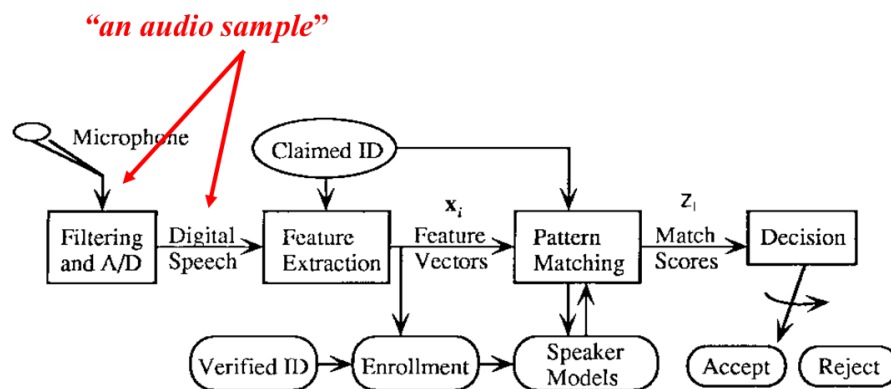


**Fig. 3.** Generic speaker-verification system.

**(Campbell) APPL-1033, FIG. 3, annotated**

**297.** Accordingly, Campbell as combined with Grounds 1 and 2 renders obvious this element.

**3. Claims 16 and 22**

***[16.0/22.0] The system recited in claim 15/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.***

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

**299. First,** Grounds 1 and 2 each implements real-time multi-factor authentication including voice authentication, and renders obvious matching the captured audio sample with a previously recorded voice sample.

**300. Second,** to the extent that it is argued that Ground 1 or 2 does not explicitly describe the matching, 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.

(Campbell) APPL-1033, 1438 (explaining that the general speaker verification model includes “enrollment to generate speaker reference models” and generating a match score for an accept/reject decision based on matching (including feature extraction and, pattern matching), making an accept/reject decision, and enrollment to generate speaker reference models”). Accordingly, to implement voice

authentication in Grounds 1 and 2, a POSITA would have applied Campbell's teaching of the fundamental knowledge of providing an accept/reject decision based on a matching result between the audio sample and a previously recorded voice sample.

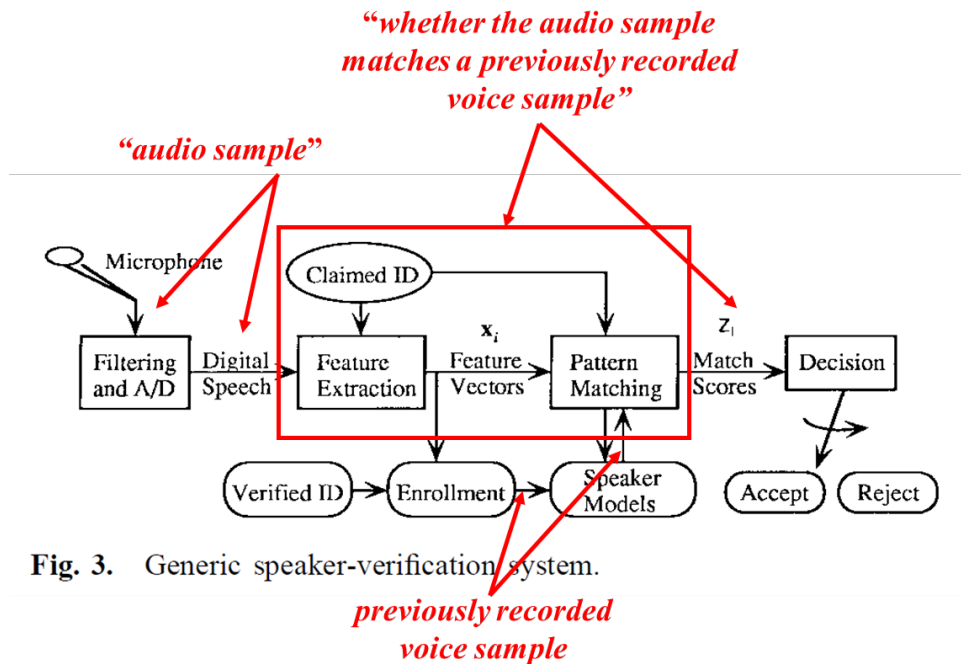


Fig. 3. Generic speaker-verification system.

**(Campbell) APPL-1033, FIG. 3, annotated**

**301.** Accordingly, Campbell as combined with Grounds 1 and 2 renders obvious this element.

**4. Claims 17 and 23**

**[17.0/23.0]** *The system recited in claim 16/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.*

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

element.

**303. First**, Grounds 1-2 each implement real-time multi-factor authentication including voice authentication, and renders obvious that the audio sample matching is based on FFT, the fundamental tool for converting the time-domain audio signal into the frequency domain for generating and comparing frequency domain features of the audio samples.

**304. Second**, to the extent that it is argued that Grounds 1-2 each does not explicitly describe using the FFT, in view of the combination's need of voice authentication techniques, a POSITA would have been motivated to implement Campbell's "very popular" speaker recognition techniques using the FFT-based feature extraction for matching in Grounds 1 and 2, because they had "been demonstrated to work well in speaker-recognition systems." (Campbell) APPL-1033, 1445 (using the FFT to extract features "based on the nonlinear human perception of the frequency of sound" to generate a match score between the captured sample and the previously recorded voice).

**305.** A POSITA would have reasonably expected to succeed in configuring Grounds 1-2 each to use the well-known recognition techniques using the FFT-based feature extraction and matching of Campbell, since its implementation would have required only routine knowledge well within the skill of a POSITA prior to the earliest effective filing date. (Nucci) APPL-1031, 12:15-19; (Bilobrov)

APPL-1032, FIG. 2; VII.C.1.

**306.** Accordingly, Campbell as combined with Grounds 1 and 2 each renders obvious this element.

**VIII. DECLARATION**

**307.** I declare that all statements made herein of my own knowledge are true, that all statements made on information and belief are believed to be true, and that these statements were made with knowledge that willful false statements so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code.

Dated: January 29, 2024



---

Dr. Creed Jones