

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner

Case: IPR2024-00330
U.S. Patent No. 10,713,656

**DECLARATION OF DR. MICHAEL T. GOODRICH IN SUPPORT OF
PATENT OWNER'S RESPONSE FOR U.S. PATENT NO. 10,713,656**

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Background and Qualifications	1
III.	Materials Reviewed	7
IV.	Legal Standards	10
V.	Person of Ordinary Skill in the Art.....	14
VI.	Claim Construction.....	15
VII.	Background.....	15
A.	The '656 Patent	15
B.	Petitioner's Asserted Prior Art	20
1.	Stone – U.S. Patent Pub. No. 2010/0042535 (Ex. 1008)	20
2.	Hoyos – US Patent Pub. No. 2010/0014720 (Ex. 1013)	22
3.	FFIEC Guidance (Ex. 1037)	23
4.	Varghese – U.S. Patent Pub. No. 2006/0282660 (Ex. 1010).....	25
5.	Borovsky – U.S. Patent Pub. US 2010/0317335 (Ex. 1041).....	27
VIII.	The '656 Patent Is Not Invalid Based On Petitioner's Asserted Prior Art.....	29
A.	Ground 1 Does Not Render the Challenged Claims Obvious.	29
1.	A POSITA would not have been motivated to combine Stone with Hoyos and Varghese and would not have had a reasonable expectation of success.....	29
2.	Stone-Hoyos-Varghese does not disclose or render obvious limitation [1.2].....	41
3.	Stone-Hoyos-Varghese does not disclose or render obvious limitation [1.9].....	47
4.	Stone-Hoyos-Varghese does not render the dependent challenged claims obvious.....	50

B.	Ground 2 Does Not Render the Challenged Claims Obvious	51
1.	Stone-FFIEC Guidance does not disclose or render obvious limitations [1.2] or [1.9]	52
2.	A POSITA would not have been motivated to combine Stone with the FFIEC Guidance	52
3.	Stone-FFIEC Guidance does not render the dependent claims obvious	55
C.	Grounds 3 and 4 Do Not Render the Challenged Claims Obvious	55
IX.	Conclusion	57

I, Michael T. Goodrich declare as follows:

I. Introduction

1. I have been retained by Patent Owner Carbyne Biometrics, LLC (“Patent Owner”) as an independent expert consultant in this proceeding before the United States Patent and Trademark Office (“PTO”) against Apple Inc. (“Petitioner”) regarding U.S. Patent No. 10,713,656 (“the ’656 Patent”). I have been asked to consider whether certain references disclose or suggest the features recited in claims 1-19 (“the Challenged Claims”) of the ’656 Patent. My opinions are set forth below.

2. I am being compensated at my customary rate of \$800 per hour for my work in this proceeding plus reimbursement of direct expenses. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other interest in this proceeding.

II. Background and Qualifications

3. My educational background, career history, publications, and other relevant qualifications provided here are only a summary.

4. Based on my education, research, and work experience, I am knowledgeable about the subject matter of the ’656 Patent and the related prior art.

5. I have over 35 years of experience in computer science, including the topics of databases (including searching and indexing). For instance, in my peer-reviewed paper, C-103, which, according to Google Scholar, has been cited over 100 times, my coauthors and I introduce novel techniques for organizing the indexing structures of how data is stored so that alterations from an original version can be detected, and the changed values specifically identified. Further, my patent, U.S. Patent No. 7,299,219, “High Refresh-Rate Retrieval of Freshly Published Content using Distributed Crawling,” which according to Google Scholar has been cited over 100 times, is directed at search engines, claiming a system for gathering fresh information added to a network such as the Internet and for processing the gathered fresh information (such as financial news), where a link server sends a batch of links to check to a crawler, which then executes its crawling assignment by filtering the encountered content and extracting only that which is new or changed. Also, my patent, U.S. Patent No. 9,152,716, is directed to an improved search engine technique that allows a user to ensure that an untrusted search engine provides complete and correct search results without requiring large proofs for large data collections, using techniques for a trusted crawler to index a distributed collection of documents and create an authenticated search structure that allows an untrusted search server to return reliably complete and correct search results. In my capacity

as a Distinguished Professor at University of California, Irvine, my responsibilities include teaching undergraduate and graduate students, performing research in computer science, mentoring PhD students and postdoctoral fellows, and serving on various university committees. I have held this distinguished position since July 2019 and I have been a professor at the University of California, Irvine since 2001. I have also served as an associate dean in the School of Information and Computer Sciences and as department chair for the Department of Computer Science.

6. Prior to my current position, I was a member of the faculty in the Department of Computer Science at Johns Hopkins University from 1987 to 2001, where my responsibilities included teaching, performing research in Computer Science, and serving on university committees.

7. I obtained a PhD in Computer Sciences from Purdue University in 1987. I also obtained a B.A. in Mathematics and Computer Science from Calvin College, which is now known as Calvin University, in 1983.

8. I have taught undergraduate and graduate courses concerning algorithms, data structures, software design, networking, and computer security beginning with my work as a graduate student at Purdue in 1983 and continuing as a professor at Johns Hopkins and University of California, Irvine. In addition, I have taught courses on algorithms and Internet technologies, including how web browsers

and search engines work, at Johns Hopkins, UC-Irvine, and during a sabbatical at Brown University. I supervise a research team that has, over the years, comprised over twenty PhD students and several postdoctoral fellows. My current focus of our research concerns networking, computer security, algorithm design, parallel and distributed computing, and data structures.

9. As shown in my CV, I have authored or coauthored over 350 peer-reviewed publications, and I have served as an editor and peer reviewer for scholarly publications and journals, including refereed conference proceedings on the topics of networking, computer security, parallel computing, databases, and algorithms. I have also published several books concerning algorithms, data structures, and computer security, including *Algorithm Design and Applications*, published by Wiley, and *Introduction to Computer Security*, published by Addison-Wesley. Further, I have published research papers on topics dealing specifically with financial data, financial documents, and financial transactions. For example, in my paper, C-101, which was published and presented at the International Conference on Financial Cryptography and Data Security, my coauthors and I presented computationally “lightweight” schemes for performing biometric authentication that carry out the comparison stage without revealing any information that can later be used to impersonate the user (or reveal personal biometric information). Unlike some

previous computationally expensive schemes, which make use of slower cryptographic primitives, this paper presents methods that are particularly suited to financial institutions that authenticate users with biometric smartcards, sensors, and other computationally limited devices. Also, in my papers, C-83, C-85, and C-87, my coauthors and I developed techniques to allow for untrusted content distributors, such as financial news and stock quote aggregators, to be able to publish financial data and documents so that users who query the information are presented with both the information and a cryptographic proof of its authenticity. In addition, in my papers, C-84 and C-151, my coauthors and I presented protocols for improving the security, privacy, and profitability of online auctions. Further, publications P-3, P-6, P-8, J-63, J-71, J-78, C-83, C-85, C-91, C-92, C-101, C-113, C-119, C-126, O-9, and O-13 specifically address authentication.

10. I am a Fellow of several industry and professional organizations, including Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), and American Association for the Advancement of Science (AAAS). I also regularly attend and present at computer science conferences concerning algorithms, networking, and computer security, including SIAM Symposium on Discrete Algorithms (SODA), ACM Symposium on Computer and Communications Security (CCS), and ACM Symposium on Parallelism in

Algorithms and Architectures (SPAA).

11. I have received several awards and recognitions for my work concerning algorithms and distributed computing, including the Dean's Award for Research in the School of Information and Computer Sciences at University of California, Irvine ("for contributions in the area of parallel and distributed algorithms"), the Robert B. Pond Sr. Award for Excellence in Undergraduate Teaching from Johns Hopkins University, the IEEE Computer Society Technical Achievement Award ("for outstanding contributions to the design of parallel and distributed algorithms for fundamental combinatorial and geometric problems"), and the Chancellor's Award for Excellence in Fostering Undergraduate Research from Univ. of California, Irvine. In addition, I have been elected as a foreign member of the Royal Danish Academy of Sciences and Letters.

12. I am an inventor on four U.S. patents, including US 7,257,711, "Efficient Authenticated Dictionaries with Skip Lists and Commutative Hashing," which discloses methods for authenticating information that is distributed from centralized servers through third-party information distributors, US 7,299,219, "High Refresh-Rate Retrieval of Freshly Published Content using Distributed Crawling," which, as I mentioned above, discloses a system for retrieving highly refreshed information quickly from Internet sources, US 8,681,145, "Attribute

Transfer Between Computer Models Including Identifying Isomorphic Regions in Polygonal Meshes,” which discloses technology for finding matchings between different geometric models, and US 9,152,716, “Techniques for Verifying Search Results Over a Distributed Collection,” which, as I mention above, discloses a technology for verifying information that is extracted by web crawling processes on the Internet.

13. A copy of my curriculum vitae listing my full employment history is included as Exhibit 2038.

III. Materials Reviewed

14. The opinions contained in this declaration are based on the documents I reviewed, my professional judgment, as well as my education, experience, and knowledge regarding security, device architecture, communications, and coding.

15. In forming my opinions expressed in this declaration, I reviewed the Apple’s Petition for *Inter Partes* Review, Carbyne LLC’s Patent Owner’s Preliminary Response, Apple’s reply in support of its IPR Petition and Carbyne’s surreply thereto. I have also reviewed the following materials and information:

Number	Title
1001	U.S. Patent No. 10,713,656 to Jakobsson et al. (“the ’656 Patent”)
1002	File History of U.S. Patent No. 10,713,656
1003	Declaration of Creed Jones, Ph.D. in Support of Petition for <i>Inter Partes</i> Review

Number	Title
1005	Prosecution File History of U.S. Prov. App. 61/332,140 (“140 App”)
1006	Prosecution File History of U.S. App. No. 13/099,981 (issued as U.S. Patent No. 8,458,041) (“981 App”)
1007	Prosecution File History of U.S. App. No. 13/875,245 (issued as U.S. Patent No. 9,972,010) (“245 App”)
1008	U.S. Pub. No. 2010/0042535 to Stone (“Stone”)
1009	U.S. Patent No. 8,386,620 to Chatterjee (“Chatterjee”)
1010	U.S. Pub. No. 2006/0282660 to Varghese et al. (“Varghese”)
1011	U.S. Pub. No. 2009/0135188 to Ding et al. (“Ding”)
1012	U.S. Patent No. 8,355,530 to Park et al. (“Park”)
1013	U.S. Pub. No. 2010/0014720 to Hoyos et al. (“Hoyos”)
1014	U.S. Pub. No. 2006/0158307 to Lee et al. (“Lee”)
1015	U.S. Patent No. 8,150,772 to Mardikar et al. (“Mardikar”)
1016	U.S. Pub. No. 2009/0157560 to Carter et al. (“Carter”)
1017	U.S. Patent No. 5,164,992 to Turk et al. (“Turk”)
1018	U.S. Patent No. 7,814,332 to Beenau et al. (“Beenau”)
1019	U.S. Patent No. 10,373,173 to Winner et al. (“Winner”)
1020	U.S. Patent No. 7,856,472 to Arav (“Arav”)
1023	U.S. Patent No. 7,779,268 to Draper et al. (“Draper”)
1024	U.S. Patent No. 5,930,804 to Yu et al. (“Yu”)
1033	J. P. Campbell, “Speaker Recognition: a Tutorial,” in Proceedings of the IEEE, vol. 85, no. 9, pp. 1437-1462, Sept. 1997 (“Campbell”)
1034	U.S. App. Pub. No. 2009/0288012A1 to Hertel et al. (“Hertel”)
1035	U.S. Patent No. 8,533,485 to Bansal et al. (“Bansal”)
1036	U.S. App. Pub. No. 2006/0271460A1 to Hanif (“Hanif”)
1037	Federal Financial Institutions Examination Council, FFIEC Press Release and FFIEC Guidance - Authentication in an Internet Banking Environment, Oct 12, 2005, https://www.ffiec.gov/pdf/authentication_guidance.pdf (retrieved January 17, 2024), accessible through hyperlinks in https://www.ffiec.gov/press/pr101205.htm (APPL-1040) and https://www.fdic.gov/news/inactive-financial-institution-letters/2005/fil10305.html (APPL-1039) (“Guidance”)

Number	Title
1038	Bhargav-Spantzel et al., “Privacy Preserving Multifactor Authentication with Biometrics,” DIM’06, November 3, 2006 (“Bhargav-Spantzel”)
1039	FDIC Financial Institution Letter, FFIEC Guidance Authentication in an Internet Banking Environment, FIL-103-2005, October 12, 2005, https://www.fdic.gov/news/inactive-financial-institution-letters/2005/fil10305.html (retrieved January 17, 2024), including hyperlink for APPL-1037 (“FIL-103-2005”)
1040	Federal Financial Institutions Examination Council, FFIEC Guidance Press Release, Oct 12, 2005, https://www.ffiec.gov/press/pr101205.htm (retrieved January 17, 2024), including hyperlink for APPL-1037 (“FFIEC Guidance Press Release”)
1041	U.S. App. Pub. No. 2010/0317335A1 to Borovsky (“Borovsky”)
1042	Ekler et al., “Similarity Management in Phonebook-Centric Social Networks,” 2009 Fourth International Conference on Internet and Web Applications and Services, Venice/Mestre, Italy, 2009, pp. 273-279, doi: 10.1109/ICIW.2009.46 (“Ekler”)
1043	U.S. Patent No. 8,954,500 to Marlow et al. (“Marlow”)
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”)
1045	Narayanan et al., “De-anonymizing Social Networks,” 2009 30th IEEE Symposium on Security and Privacy, 2009 (“Narayanan”)
1046	U.S. App. Pub. No. US2008/0270038A1 to Partovi et al. (“Partovi”)
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”)

Number	Title
2010	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 42 (Apple’s Opening Claim Construction Brief) (W.D. Tex. October 4, 2023)

Number	Title
2011	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 49 (Carbyne’s Response to Apple’s Proposed Claim Construction) (W.D. Tex. October 25, 2023)
2012	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 54 (Apple’s Reply Claim Construction Brief) (W.D. Tex. November 8, 2023)
2013	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 62 (Carbyne’s Sur-Reply to Apple’s Claim Construction Brief) (W.D. Tex. November 22, 2023)
2014	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 69 (Minute Entry re Markman Hearing and Motion to Transfer Venue) (W.D. Tex. December 12, 2023)
2025	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Apple’s Amended Preliminary Invalidity Contentions (W.D. Tex. October 6, 2023) (excerpts)
2031	CV of Dr. Michael Goodrich

16. I also reviewed any other materials I refer to in this declaration in support of my opinions.

17. My opinions contained in this declaration are based on the documents I reviewed and my knowledge and professional judgment. My opinions have also been guided by my understanding of how a person of ordinary skill in the art would have understood the state of the art, the prior art, and the claims and the specification of the ’656 Patent at the time of the alleged invention.

IV. Legal Standards

18. I am not an attorney. As a technical expert, I am not offering any legal opinions. Rather, I am offering technical assessments and opinions. In rendering my

analysis, I have been informed by counsel regarding various legal standards for determining patentability. I have applied those standards in forming my technical opinions expressed in this report.

19. The patent claims describe the invention made by the inventors and describe what the patent owner owns and what the owner may prevent others from using. I understand that an independent claim sets forth all the requirements that must be met to be covered by that claim. I further understand that a dependent claim does not itself recite all the requirements of the claim but refers to another claim and incorporates all of the requirements of the claim to which it refers.

20. It is my understanding that a claimed invention is unpatentable if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Obviousness, as I understand it, is based on the scope and content of the prior art, the differences between the prior art and the claim, and the level of ordinary skill in the art. I understand that a claim could have been obvious from a single prior art reference or from a combination of two or more prior art references.

21. I understand that when evaluating obviousness, one must not consider whether the claimed invention would have been obvious to a layman or to an expert;

not use hindsight when comparing the prior art to the claimed invention; not consider what was learned from the teachings of the patent. In particular, I understand that it is improper to use the patent claims as a road map for selecting and combining items of prior art. In other words, one should avoid using the challenged patent as a guide through the prior art references, combining the right references in the right way so as to achieve the result of the claims at issue. Instead, one must put oneself in the place of a person of ordinary skill at the time the invention was made and consider only what was known before the invention was made and not consider what was only known after the invention was made.

22. I understand that obviousness should be considered in light of the problems known to the person having ordinary skill in the art at the relevant time and the complexity of the alternatives for solving the problem. That individual elements of the claimed invention are disclosed in the prior art is not alone sufficient to reach a conclusion of obviousness.

23. I understand that certain factors (also called secondary considerations) may support or rebut the obviousness of a claim. I understand that such secondary considerations include, for instance, commercial success of the patented invention, skepticism of those having ordinary skill in the art at the time of invention, unexpected results of the invention, any long-felt but unsolved need in the art that

was satisfied by the alleged invention, the failure of others to make the alleged invention, praise of the alleged invention by those having ordinary skill in the art, and copying of the alleged invention by others in the field. I understand that there must be a nexus—a connection—between any such secondary considerations and the alleged invention. I also understand that contemporaneous and independent invention by others is a secondary consideration tending to show obviousness.

24. I also understand that while it may be helpful to identify a reason for a combination, common sense should guide the analysis and no rigid requirement of finding a teaching, suggestion, or motivation to combine is required. When a product is available, design incentives and other market forces can prompt variations of the product, either in the same field or different one. If a person of ordinary skill in the art can implement a predictable variation, obviousness likely bars its patentability. For the same reason, if a technique has been used to improve one device and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique would have been obvious. I understand that a claim would have been obvious if common sense directs one to combine multiple prior art references or add missing features to reproduce the alleged invention recited in the claims.

V. Person of Ordinary Skill in the Art

25. It is my understanding that Petitioner provides the following definition of a person of ordinary skill in the art (POSITA):

Here, a Person of Ordinary Skill in the Art (“POSITA”) at the time of the claimed invention would have had a bachelor’s degree in electrical engineering, computer engineering, computer science, or a related field, and at least two years of experience in the research, design, development, and/or testing of biometric authentication techniques, and related firmware and software, or the equivalent, with additional education substituting for experience and vice versa.

Petition at 4.

26. It is my understanding that the Board’s Institution Decision (Paper 10) adopted Petitioner’s description of a POSITA “except for the language ‘at least’ that qualifies the experience level and allows the experience level to encompass an expert’s level of skill.” Institution Decision (Paper 10) at 11-12.

27. For my opinions in this declaration, I apply the Petitioner’s POSITA definition with the Board’s clarifying instruction. Now and as of the priority date of the ’656 Patent, I meet the level of skill described above. Further, I have taught thousands of undergraduate and graduate computer science students since 1987, including on topics relevant to the research, design, development, and/or testing of biometric authentication techniques for hardware, software, and firmware solutions; hence, I have extensive experience with respect to the knowledge of a POSITA.

28. Based on my knowledge and experience, I understand what a person of ordinary skill in the art would have known at the times of the alleged invention. My opinions herein are, where appropriate, based on my understandings as to a person of ordinary skill in the art at those times.

VI. Claim Construction

29. It is my understanding that Petitioner does not assert that any claim terms of the '656 Patent require construction. *See* Pet. 5. In the absence of the need for an explicit construction, it is my understanding that claim terms are given their plain and ordinary meaning as understood by a POSITA when read in light of the patent's specification. For the purposes of this declaration and the opinions herein, I have given all claim terms of the Challenged Claims their plain and ordinary meaning.

VII. Background

A. The '656 Patent

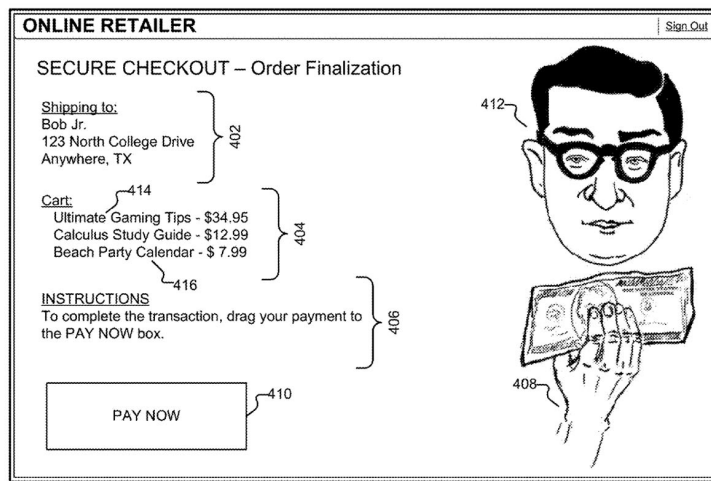
30. The '656 Patent is titled "Method, Medium, and System for Reducing Fraud." The application for the '656 Patent was filed on April 9, 2018, and claims priority through a sequence of continuations and applications going back to provisional application No. 61/332,140 filed on May 6, 2010. The '656 Patent provides systems and methods for preventing or reducing fraud in electronic

transactions. *See* Ex. 1001. As the '656 Patent states, there are two primary reasons why, even an otherwise honest person, would refrain from committing fraud: (1) associated feelings of guilt and (2) the risk of getting caught. *Id.* at 1:22-1:32, 4:24-4:26.

31. The '656 Patent explains that electronic payment fraud presents “an ongoing problem” that is “particularly devastating” because it can eliminate these two deterrents by removing the physical aspects of a transaction. *Id.* at 1:19, 1:24-1:27, 4:17-4:19. To this end, electronic payment transactions lower the risk that a fraudster will be caught, or at least the fraudster’s perception of this risk, by removing the physical barriers to the victim, the victim’s credit card, or the victim’s wallet. *See id.* 1:27-1:30. Removing the need for physical access to the victim also serves to eliminate the human element of a transaction and alleviates the associated feelings of guilt that a fraudster might experience. *See id.* 5:10-5:12 (“The more human the victim is made to be, the more guilty a fraudster might feel when perpetrating a fraud.”). The electronic environment makes it easier for the fraudster to go through with the fraud with less fear of reprisal. 5:8-5:34, 6:10-6:23, 6:52-6:64.

32. The '656 Patent seeks to deter electronic payment fraud by providing novel systems and methods that leverage the two primary fraud deterrents. *See* 4:24-4:26. For the first deterrent, the '656 Patent’s claimed invention increases a potential

fraudster's feelings of guilt by providing an improved interface that includes a virtual likeness of the face of an account holder whose account is engaged in an electronic transaction. *See id.* at 5:8-5:34. Forcing a potential fraudster to complete a transaction while looking at a photo or other likeness of the victim's face (or the potential recipient of illicit funds in a peer-to-peer cash transfer, *see id.* at 11:6-11:10) humanizes the transaction and makes it personal by emphasizing the identity of the victim, potential recipient, or account holder who will be impacted by the fraudulent transaction. *Id.* at 5:23-5:25. The figures below from the '656 Patent provide examples of a transaction interface that includes the virtual likeness of an account holder.



400 → **FIG. 4**

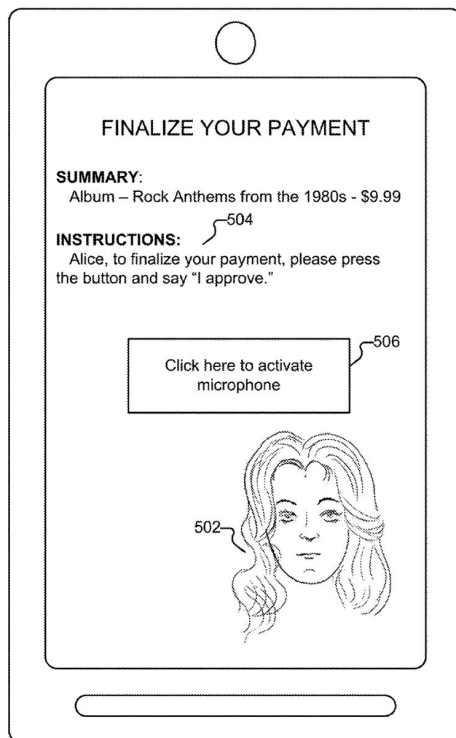


FIG. 6

33. The '656 Patent's claimed systems and methods also increase the
- 18

fraudster's risk of being caught—real or perceived—by employing biometric authentication techniques as part of a fraud detection analysis to determine that a user is alive. *See, e.g.*, Ex.1001, cl. 1. Specifically, the '656 Patent's claimed authentication process is as follows. The user interacts with a transaction icon in an interface containing a virtual likeness of the face of an account holder. *Id.* The user's biometric information is captured, and fraud detection analysis is performed to determine that the user is alive, based at least in part on the biometric information collected from the user. *See id.* The electronic transaction is then completed based at least in part on both the user interaction with the transaction icon in the interface and the fraud detection analysis. *See id.*

34. The collected biometric information can include images of the user or an audio recording. *Id.* at 8:51-9:6. For the collection of images, techniques for confirming the object captured in the images 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.” *Id.* at 8:61-66. “The application of various rules, such as requiring that a face be detected in the captured image or that a certain amount of flesh tone be present in the picture can also be implemented.” *Id.* 8:66-9:2. “Similar rules can be applied to other types of capture, such as requiring that a GPS be turned on prior to a transaction

taking place, or requiring that provided audio conform to general rules that define what human utterances sound like.” *Id.* 9:2-9:6.

35. In sum, the ’656 Patent provides a novel approach to preventing fraud in electronic transactions by coupling an interface incorporating the virtual likeness of an account holder to inspire feelings of guilt in a potential fraudster with biometric authentication techniques, specifically those to determine whether the user is alive, that increase the likelihood (real or perceived) that the fraud will be detected.

B. Petitioner’s Asserted Prior Art

36. Below is my description of Petitioner’s asserted prior art references.

1. Stone – U.S. Patent Pub. No. 2010/0042535 (Ex. 1008)

37. Petitioner’s “Stone reference” is titled “Currency Display” and assigned to eBay. *See* Ex. 1008. Stone discloses systems and methods for the electronic visual representation of currency or financial instruments. *Id.* [0002], [0006]. Embodiments of Stone’s disclosure “enable users to see a selected actual currency representing the amount entered by the user into a device with a display screen. *Id.* at [0016]. Providing a visual representation of the amount in a transaction reinforces the value of the amount of money in the transaction and provides the user with a “more visually rich interface.” *Id.* An aspect of the display envisioned by Stone is that it enables a user’s device to detect its location and use

the currency of that country. *Id.* at [0026]. If the user is a U.S. citizen traveling abroad in South Korea, for example, the device will detect the user's location, and the currency display will use South Korean won instead of U.S. dollars. *Id.* at [0026-30]. This feature allows a user in a foreign land to understand how much the user would be willing to pay for something when bartering with local merchants. *Id.* at [0030].

38. The display described in Stone can also include more than just a representation of currency. *Id.* at [0021]. Some embodiments of the display can include the name and picture of the recipient in a peer-to-peer transfer or the user's funding source and account balance before a transaction is initiated. *Id.* at [0024].

39. But Stone's primary focus is providing a "more visually rich interface" that gives the user a visual representation of the amount and denomination of currency subject to a transaction, particularly where foreign currencies are involved. *See id.* at [0016], [0026].

40. Stone does not identify electronic payment fraud or seek to address it. Stone is also not concerned with processing transactions, improving transaction processing or user authentication. *See, e.g.,* Stone at [0023] ("Note that transferring funds via a mobile phone is known, such as through PayPal in San Jose, Calif. Thus, details of how funds are transferred are not described here.").

2. Hoyos – US Patent Pub. No. 2010/0014720 (Ex. 1013)

41. Hoyos discloses systems and methods for biometric authentication in financial transactions. Ex. 1013 at [0002]. In one aspect, Hoyos discloses a method for authenticating financial transactions by acquiring biometric data from a person, calculating the probability of liveness of the person and probability of a match between the person and known biometric information. *Id.* at abstract and [0017]. Examples of the biometric inputs include photos capturing the subject's face and eyes or readings of finger and palm temperature. *Id.* at [0021]. In certain embodiments, the authentication decision is calculated using the collected biometric information to determine the probability of a match and probability of a live person based on a mathematical formula. *Id.* at [0016-22].

42. According to Hoyos, “in the prior art the decision to authorize a transaction does not separately consider a measure of liveness and a measure of match.” By match, Hoyos refers to the ability “to calculate the probability of a match between acquired biometric data from an individual or purported individual being authenticated and data acquired from known individuals.” Hoyos defines “liveness” as “whether the biometric data is being acquired from a live human rather than a fake due to a spoof attempt.” Ex. 1013 at [0012].

43. The prior systems and methods have not achieved significant

commercial success in the field of authenticating financial transactions due, in part, from the insufficient speed and accuracy from which prior biometric authentication systems for financial transactions suffered. More specifically, the current methods of basing a decision to perform a financial transaction on the measure of match means that many valid customers are rejected, due to the finite false reject rate.

44. While Hoyos describes techniques for biometric authentication, it does not suggest coupling these techniques with an improved digital interface. Nor does Hoyos even mention digital interfaces as being relevant to its claimed authentication techniques. Hoyos' proposed claims and specification focus mainly on the above-described probability calculations used for authenticating a user. Hoyos' proposed claims and specification focus mainly on the above-described probability calculations used for authenticating a user. Hoyos also does not disclose employing its methods or systems in a client-server environment, but rather is focused on providing local authentication on a client device. *See, e.g.*, Hoyos at cl. 4.

3. FFIEC Guidance (Ex. 1037)

45. The FFIEC Guidance reference is guidance published by the Federal Financial Institutions Examination Council (FFIEC). Ex. 1037 at 1. The FFIEC is a formal interagency body of five banking regulators established in 1979 and “empowered to prescribe uniform principles, standards, and report forms for the

federal examination of financial institutions.” *Id.* In 2005, the FFIEC issued “guidance” for “Authentication in an Internet Banking Environment” (“FFIEC Guidance” or the “Guidance”). *See id.* The 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.” *Id.* at 1. The Guidance suggests that single-factor authentication (such as typed passwords) is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. *Id.* The Guidance mentions high-level techniques and methodologies for multifactor authentication that fall into three broad categories: something a person knows (password or PIN), something a person has (a physical token or card), or something a person is (most commonly biometrics). *Id.* at 2.

46. Concerning biometrics, the FFIEC Guidance provides a basic description of fingerprint and facial recognition techniques and the benefits of employing these methods. But the Guidance stops short of “endors[ing] any particular technology” or explaining how to implement any techniques, specifically as part of a digital interface. *Id.* at 1. The Guidance mentions that “various biometric techniques and identifiers are being developed and tested, these include fingerprint

recognition, face recognition, voice recognition, keystroke recognition, handwriting recognition, finger and hand geometry, retinal scan, and iris scan.” Ex. 1037 at 10. Of these techniques, the FFIEC states that fingerprint and face recognition are gaining acceptance, *see id.*, but the FFIEC Guidance does not state that these techniques or any other technique mentioned in the Guidance was well known or in general user. The Guidance also does not discuss improvements or upgrades to digital displays in electronic transactions. *Id.* at 9-11.

4. Varghese – U.S. Patent Pub. No. 2006/0282660 (Ex. 1010)

47. Varghese generally relates to “systems and methods for providing protection against identity theft over a computer network.” Ex. 1010 at [0002]. It discloses multi-factor authentication for electronic transactions that uses a rules engine to score the transaction based on different criteria, including biometrics (voiceprint) and device “location fingerprint.” *Id.* at Fig. 14. Varghese describes both pre- and post-authentication procedures. *Id.* at [0090]; *see also id.* at Table 3. For “pre- authentication, the most common user request is a login request to access an application or system.” *Id.* at [0074]. “[R]equests usually handled by post-authentication services include, e.g., transaction requests involving large amounts of money.” *Id.* at [0074]; *see also id.* at [0099].

48. In the systems and methods Varghese discloses, authentication is

separated into two phases: pre- and post-authentication. Pre-authentication is employed for actions such as login requests. For pre-authentication, Varghese looks to identifying information of the device originating the request or information about the identity of the user. *Id.* at [0065]. Post-authentication is applied for authentication requests such as transaction requests for large amounts of money. *Id.* Post-authentication described by Varghese authenticates a transaction by looking at historic transaction information and workflow. *Id.*

49. Varghese identifies available security-relevant information related to a user request (the “request attributes”) as falling within related groupings or “criteria.” *Id.* at [0089]. For pre- and post-authentication, different criteria are available or of differing importance, depending on which authentication phase is being implemented. *Id.* For example, in pre-authentication, a user is seeking to log in to an application, so the user’s transaction history is unavailable. *Id.* But for post-authentication, when a user is making a transaction request (e.g., a transaction request for large amounts of money), criteria for initial authentication, such as location information for the user device or the device IP address, are typically not relevant, and the user’s transaction history is more important. *Id.*

50. Table 3 from Varghese presents a list of characteristics that can be used during pre-authentication and post-authentication. Notably, Petitioner’s Ground 1

relies on Varghese as disclosing the “location” limitations of Challenged Claims. Pet. 39-45, 65-68. As Table 3 (reproduced below) shows, location information is considered in pre-authentication, i.e., for user login requests. Location information characterizes the location of the device from which a request originates. Ex. 1010 at [0072]. Location can most easily be estimated from the device’s IP address and the hierarchy of networks linking the device to the internet. *Id.* at [0093].

TABLE 3

Example of Request Attributes		
Pre-authentication	Location information	City, State, Country information and confidence factors
		Connection type
		Connection speed
		IP address, routing type, and hop times
		Internet service provider flag
		Autonomous system number
		Carrier name
		Top-level domain
		Second-level domain
		Registering organization
		A list of anonymizing proxies
		Hostnames and routers
		Secure Cookies
		Flash Cookies
Post-authentication	Device information	Digitally signed device
		Device & display Characteristics:
		Operating System characteristics
		Browser Characteristics
	User information	User identifications
		Valid or not valid user
	Transaction information	Authentication status
		Key Value Pairs:
		Support multiples
		Keys can be defined using Regular Expressions
		Values can be defined in ranges
		Pages accessed
		Time spent on page
		Transactions sequences

5. Borovsky – U.S. Patent Pub. US 2010/0317335 (Ex. 1041)

51. Borovsky (U.S. Patent Pub. US 2010/0317335) is titled “Systems and

Methods for Remotely Configuring a Mobile Device.” Borovsky claims priority to U.S. Patent Appl. No. 12/483,149 filed June 11, 2009. *See* Ex. 1041. Borovsky generally relates to systems and methods for remotely configuring a mobile device. *Id.* at [0001]. The system and methods disclosed by Borovsky for remotely configuring a mobile phone using servers that store and remotely update configuration information for the mobile device. *See, e.g.,* Ex. 1041 at cls. 1, 7, 19. Borovsky provides for a remote computer that includes a user interface for managing configuration information for the user’s mobile device. *Id.* at [0010]. The user enters management information via the user interface presented at the remote computer and, subsequently, a management system updates configuration information at a database based on the management information. *Id.* The configuration information can include contact information for viewing or updating contacts of the user stored in the mobile device. *Id.* at cl. 3. The user interface displayable at the remote host computer may comprise a contacts interface that can enable a user to enter contact management information. *See, e.g., id.* at cl. 6. The contact management information may include display names corresponding to the user’s contacts, phone numbers for the contacts, addresses for the contacts, or photos corresponding to contacts of the user. *See, e.g., id.* at cl. 7.

VIII. The '656 Patent Is Not Invalid Based On Petitioner's Asserted Prior Art

52. The '656 Patent's Challenged Claims are not invalid in view of Petitioner's prior art references. Petitioner asserts three obviousness grounds in its Petition:

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

53. For the reasons I explain below, Petitioner's Grounds do not render the Challenged Claims obvious.

A. Ground 1 Does Not Render the Challenged Claims Obvious.

54. Petitioner's invalidity Ground asserts that independent claims 1, 10, and 19 and dependent claims 4-9 and 13-18 of the '656 Patent are rendered obvious under 35 U.S.C. §103(a) over Stone in view of Hoyos and Varghese. But as I explain below, the Stone-Hoyos-Varghese does not render the Challenged Claims obvious.

1. A POSITA would not have been motivated to combine Stone with Hoyos and Varghese and would not have had a reasonable expectation of success.

55. A POSITA would not have been motivated to combine Stone with

Hoyos and Varghese, and Petitioner has offered nothing but conclusory, hindsight-based justifications to support its alleged combination.

56. Petitioner's stated reasons supporting the Stone-Hoyos-Varghese combination do not explain why a POSITA would have combined these references, specifically, Stone and Hoyos, to reach the '656 Patent's claims.

57. Petitioner's explanation for why a POSITA would have combined Stone and Hoyos is essentially the following: "[I]t was well-known that financial transactions of Stone had a need for authentication including fraud detection (e.g., with higher levels of security for higher-risk transactions)." Pet. at 16. And "[a] POSITA would have been motivated to implement Hoyos' spoofing-resistant biometric authentication for fraud detection in the system of Stone for 'improved deterrent against attempted fraudulent transactions, and decreased rejection of valid customers.'" *Id.*

58. These justifications do not offer a sufficient reason why a POSITA would have been motivated to combine the references. Stone does not state that electronic fraud is a problem that needs to be solved. It never mentions fraud, nor does it discuss any techniques for preventing fraud, like those described in Hoyos. Stone is concerned with and discloses an improved currency display. *See* Stone at [0002] and [0016]. Stone is also not concerned with the actual processing of

transactions; thus, a POSITA would not have been motivated to apply Hoyos's authentication techniques to Stone's teachings. *See* Stone at [0023] ("Note that transferring funds via a mobile phone is known, s through PayPal in San Jose, Calif. Thus, details of how funds are transferred are not described herein.").

59. Stone states that user identifier 418 "may include attributes related to the user, such as personal information (e.g., a username, 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.). *See* Stone at [0045]. Yet, Stone does not say that user identifier 418 is used to perform user authentication or fraud detection, specifically fraud detection analyzing user biometrics.

60. Stone discloses that user identifier 418 may include a "biometric id" or "security information," but Stone does not disclose that either is used to authenticate a transaction. In reference to the transfer of funds, Stone states: "Note that transferring funds via a mobile phone is known, such as through PayPal in San Jose, Calif. Thus, details of how funds are transferred are not described herein." Stone at [0023]. This further emphasizes that Stone is not concerned with the actual process of transferring funds, but focused on the user interface. Declining to explain how funds are transferred, much less providing ways to improve this process, such as

ways to reduce fraud, further proves that Stone is not concerned with fraud detection or the processing of electronic transactions.

61. Hoyos also includes nothing to suggest a POSITA would combine its disclosure with that of Stone. Hoyos is narrowly focused on improving biometric authentication by combining known biometric matching techniques with a method to determine the probability that the subject is alive. Ex. 1013 at [0016]-[0022]. By creating a sliding scale that considers both the probability that a user is a biometric match with a stored template and the probability of liveness (i.e., “whether the biometric data is being acquired from a live human rather than a fake due to a spoof attempt.”). *Id.* at [0012]. Hoyos is not concerned with improving a user display, specifically an electronic currency display (like that of Stone), or improving a user’s experience based on providing a richer interface (like Stone). Nothing in Hoyos would lead a POSITA to combine its biometric authentication methods with an interactive interface, particularly a currency display like the one Stone provides.

62. The sum total of Petitioner’s motivation to combine Stone with Hoyos for Ground 1 is that fraud in electronic transactions was a known problem, and the Stone and Hoyos consist of known elements that were within a POSITA’s skill level to combine. But this not accurate, as it overlooks that Stone was not concerned with processing or improving the processing of electronic transactions. And even if it

were, known elements and a known problem without more are insufficient to establish a motivation to combine. Essentially, Petitioner is looking back in hindsight to reconstruct the claims of the '656 Patent using its asserted references.

63. It is also my opinion that a POSITA would also not have been motivated to combine Stone with Hoyos and Varghese because Stone is not analogous art. It is my understanding that to be analogous a reference must be in the same field of endeavor or reasonably pertinent to the particular problem with which the inventor is involved.

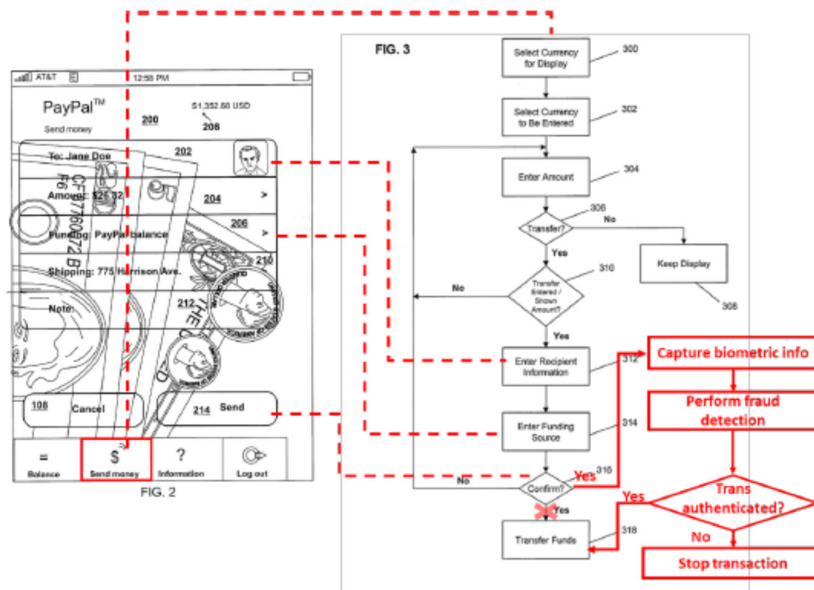
64. Stone is not in the same field of endeavor. It is my understanding that to determine the field of endeavor one may look at the patent, for example, the background of the invention. Here, the background of the invention of the '656 Patent states that the claimed invention relates to improved techniques to prevent and detect fraud, particularly within electronic transactions.

65. The '656 Patent's claims are also solely focused on detecting and preventing fraud—by increasing feelings of guilt and the likelihood a perpetrator will be caught—as are the specification and the disclosed embodiments. *See generally* Ex. 1001. Stone is only concerned with providing an improved currency display. *See* Stone at Abstract. It “relates to electronic visual displays, and in particular, to such displays that show a visual representation of financial

instruments.” *Id.* at [0002]. And a primary goal of Stone’s claimed invention is to provide a “more visually rich interface.” *Id.* at [0016]. It is not in the field of electronic fraud prevention. Stone never mentions fraud.

66. To the extent Petitioner may argue the relevant field of endeavor is electronic financial transactions, this is not correct. As noted, Stone is not concerned with the actual processing of financial transactions or improving the processing of financial transactions. *See* Stone at [0023]. To the extent Stone mentions financial transactions, this is tangential to Stone’s primary purpose—improving a user display.

67. Stone and Hoyos teach away from each other in material ways that would prevent a POSITA from combining them. The figure below from the Petition illustrates Petitioner’s Stone-Hoyos electronic transaction model. The Stone interface is on the left (Fig. 2); the transaction flow chart from Stone is to the right (Fig. 3), and the biometric “authentication process” from Hoyos is inserted into the flowchart represented by the red text on the far right.



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

Pet. at 37.

68. There are several problems with Petitioner's Stone-Hoyos transaction model. First, Stone and Hoyos teach away from each other and are incompatible because they are directed to different computing environments. Stone requires a client-server structure, *see* Ex. 1008 at [0040]-[0048] and Fig. 4, and Hoyos's disclosed authentication methods are employed locally on the device, with no mention of a server structure. *See, e.g.*, Hoyos cl. 4; *see also id.* at [0016]-[0022].

69. While Petitioner suggests that biometric authentication can be performed using either a server or client device, *see* Pet. at 22, Stone provides no basis for applying Hoyos's authentication techniques locally because Stone discloses

only a client-server structure for implementing its currency display. *See* Ex. 1008 at [0045]-[0048] and Fig. 4. Stone discloses that the payment server maintains the user accounts, account information, and payment applications. *See id.* So for the system of Stone to perform a transaction, communication with the server is required.

70. Employing local biometric authentication within Stone’s client-server structure also does not make sense. For one, this would be redundant. As Stone Figure 2 shows, the user’s account balance (208) is displayed on the interface before the user completes the transaction. Displaying an account balance would require some communication with the payment server where the user’s account information must be stored, *see* [0047]-[0048] and Fig. 4, well before the end of the transaction where Petitioner inserts the Hoyos “authentication process.” Inserting the Hoyos client-only authentication process as the final step before completing the transaction would then require on-device authentication after the device has already transferred information in communication with payment server 408, which is redundant.

71. Requiring local authentication in addition to requiring communication with a server to associate a user with their account and obtain necessary account information would also increase latency within the transaction, which undermines a primary goal of Hoyos (transaction speed) to address a problem that Stone does not even identify as a concern (electronic payment fraud), *see* Ex.1013, [0009], [0011],

and would unnecessarily occupy processing resources on the user device that the client-server structure conserves.

72. A POSITA also would not have been motivated to implement the aliveness determination and matching techniques from Hoyos on a client-server structure. Doing so would undermine Hoyos's stated goals of improving speed, accuracy, and security of biometric authentication. Petitioner's expert, Dr. Jones, concedes as much by listing a series of benefits derived from local authentication as Hoyos discloses. These benefits include "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 intends 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)." Ex. 1003 at ¶ 68.

73. In my opinion, every one of these benefits provided by local

authentication, like that envisioned by Hoyos, is undermined by employing a server structure. Latency is increased due to the time communicating with the server. There would be no offline capability. Privacy would not be improved, given the possibility of a data breach of the server where a user's biometric information would be stored. Resources would not be efficiently used as processing power on the device would be sacrificed.

74. It is also my opinion that a POSITA would not have been motivated to combine Varghese with Stone and Hoyos. For one thing, a POSITA would understand that Varghese amplifies the disconnect between Stone and Hoyos regarding the server and client distinction. Varghese, like Stone, employs a client-server structure, requiring transfer of information from the client to the server for authentication. *See* Ex. 1010 at [0005-06]. So for the reasons just explained for Stone and Hoyos, a POSITA would also not be motivated to combine techniques performed using a client-server structure (Varghese) with techniques performed only on a client device (Hoyos) to achieve the fraud analysis provided for in the '656 Patent's claims.

75. Additionally, a POSITA would understand that a goal of Varghese is to provide a "purely software-based solution to identify theft that does not require hardware devices to be issued and maintained." Ex. 1010 at [0022]. The system

envisioned by Varghese is centered around “device-based fraud monitoring” that includes “a repository of information for identifying legitimate and fraudulent users based on a more reliable and robust fingerprinting of the user device that can be integrated with other repositories of security tracking information.” Varghese at [0017] and [0021]. Varghese acknowledges that these systems and methods were “currently lacking in the art” at the time. *Id.* at [0016]. The software-only solution proposed by Varghese requires implementation through a client-server structure. Varghese is also concerned with using information from the user’s device itself rather than the user for fraud detection, *see* Varghese at [0017] and [0021]-[0022], and not concerned with implementing or improving sensor-based biometrics, such as fingerprints and facial biometrics, on the user device that require hardware implementations (e.g., fingerprint scanners and forward-facing cameras). *See* Ex. 1013 at Fig. 2, [0018-19], [0034-36] (using camera to collect images of user for biometric authentication), [0022] (noting probability of biometric match can be calculated by “iris recognition, fingerprint image recognition, finger vein image recognition, or palm vein image recognition”).

76. The hardware-based biometrics collection and authentication techniques described in Hoyos do not support Varghese’s stated goal of providing a “purely software based solution to identify theft” (i.e., fraud detection), so a POSITA

would not have been motivated to look to Hoyos to improve or alter the system disclosed by Varghese, specifically to reach the claimed solution of the '656 Patent claims.

77. Petitioner has also not established that a POSITA would have been motivated to add Varghese's collection of location information to the transaction flow laid out in Stone, particularly at the final confirmation stage. Varghese specifically teaches against applying a location check as one of the final steps of the '656 Patent's claimed fraud detection analysis. Varghese discloses a multifactor authentication framework divided into pre-authentication and post-authentication stages. Ex. 1010 at [0074] and [0090]. Pre-authentication deals with collection of information related to the user and the user's device to authenticate a user logging into a web application—focusing heavily on information collected from the user's device (e.g., device fingerprint that involves collection of IP address information, among other things.) *Id.* at [0074]. A user login is not depicted in Petitioner's combined transaction model shown above. But it would undoubtedly occur at a stage before the first step listed in the flowchart of Stone Fig. 3, as well as before the interface in Stone Fig. 2 would be presented to a user.

78. But perhaps most problematic for Petitioner, Varghese teaches that post-authentication is for completing monetary electronic transactions, which are

authenticated using a user's transaction history and historic workflow. Ex. 1010 at [0065] ("User workflow sequences are authenticated (referred to herein as 'post-authentication') using a user's transaction history."). And "when a user is engaged in requesting transactions [post-authentication], criteria related to initial authentication [e.g., pre-authentication location data] are usually less important." Ex. 1010 at [0089]. Based on Varghese's teaching, a POSITA would not have been motivated to collect location data (a pre-authentication technique for user login requests) to authenticate an electronic transaction [post-authentication request], particularly as the last step of a transaction as Petitioner claims.

2. Stone-Hoyos-Varghese does not disclose or render obvious limitation [1.2].

79. It is my opinion that Stone-Hoyos-Varghese does not disclose limitation [1.2] "receive biometric information associated with an account holder; store, in a data store, the received biometric information, wherein the biometric information is associated with an account of the account holder." According to Petitioner, "Stone describes receiving from an account holder (user 409), biometric information (to be stored as 'biometric id') associated with the account holder (user 409); and storing the biometric information as 'biometric id' in a data store (storage component 508) of user device 404, where the stored 'biometric id' is a user attribute

of user identifier 418 associated with an account (account 422) of the account holder (user 409).” Pet. at 31 (citing Ex. 1008 at [0045]).

80. However, Petitioner does not establish that Stone discloses biometric information that is associated with an account of the account holder as required by limitation [1.2].

81. Petitioner points to figures 4 and 5 of Stone and the related descriptions in the specification as disclosing limitation [1.2]. Both figures are reproduced below for reference. First, for the claim element “receive biometric information associated with an account holder” Petitioner points to the user identifier 418, which “may include attributes related to the user, such as personal information (e.g.,...biometric id).” *See* Pet. at 31 (citing Ex. 1008 at [0045]). Petitioner states the user’s (i.e., account holder’s) “biometric id” is stored in a data store (storage component 508) of the user’s device 404, in a data store (storage component 508) of user device 404, where the stored “biometric id” is a user attribute of user identifier 418 associated with an account (account 422) of the account holder (user 409).” Pet. at 31 (citing Ex. 1008 at [0045]). However, Stone does not disclose any association of a user identified 418 with a user’s account 422 that occurs on the user’s device 404. Any association that may occur of a user identifier with a user account occurs on the payment server 408, not a data store on the user device.

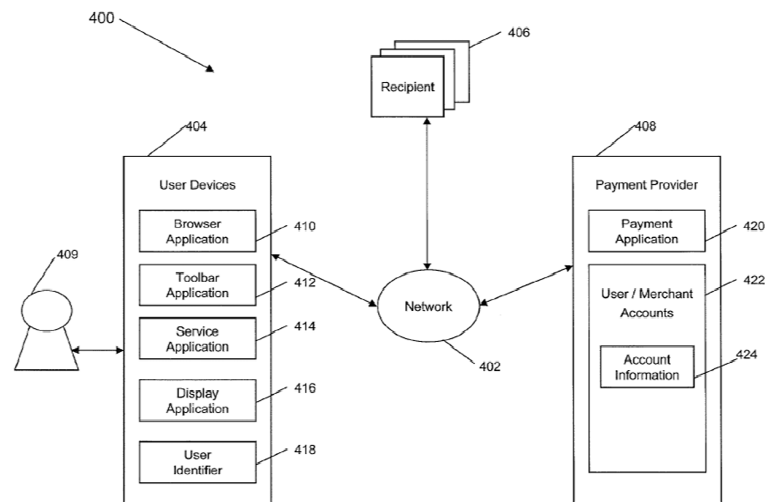


FIG. 4

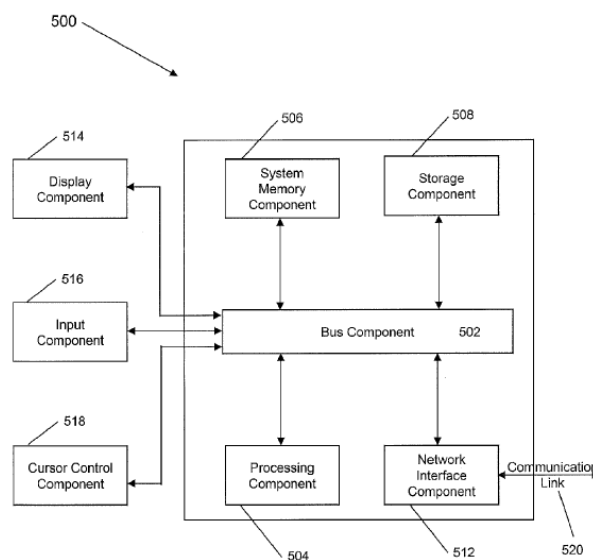
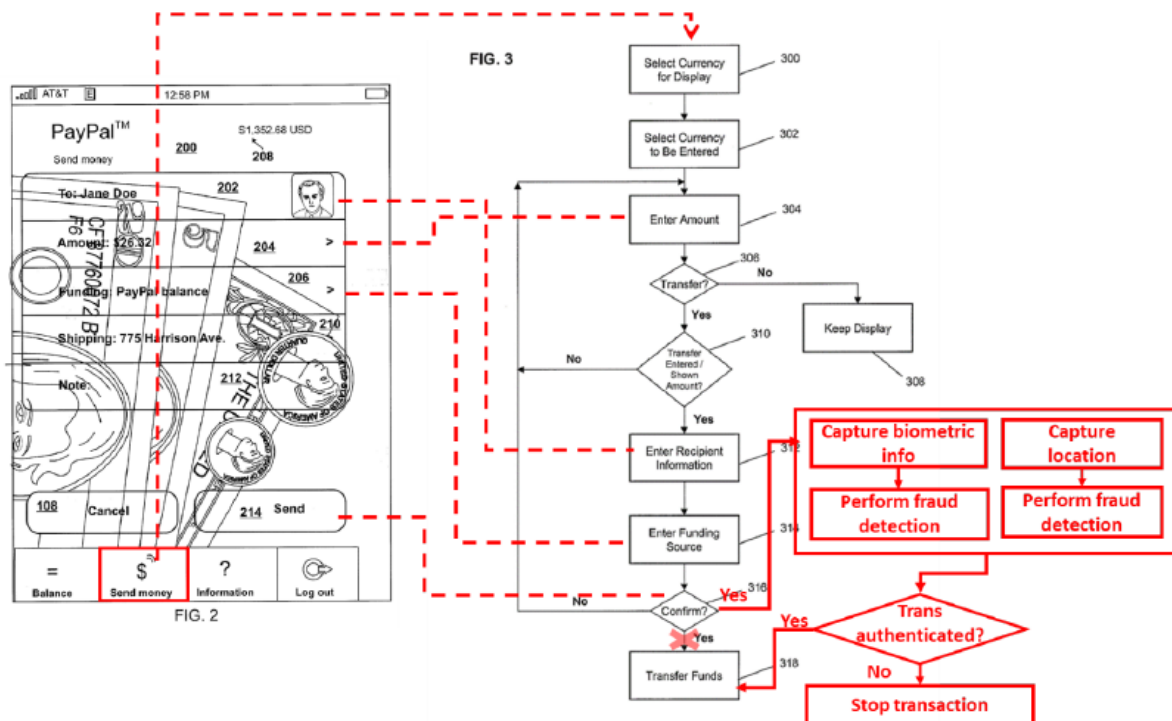


FIG. 5

82. Moreover, the payment server cannot disclose the “association” element of the claim because the “association” must occur *within* the data store after the biometric information is stored. *See* limitation [1.2] (“store, in a data store, the

received biometric information, wherein the biometric information is associated with an account of an account holder” (emphasis added)). Stone describes the “association” of user identifier 418 (e.g., biometric id) with an account as occurring in the payment server: “user identifier 418 may be passed request to payment provider server with a user money transfer 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.” Ex. 1008 at [0045]. Stone provides no other disclosure for “associating” a user identifier with an account other than within the payment provider server.



Example of Stone-Hoyos-Varghese

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

83. Even if Petitioner were to suggest that the association step occurring in the payment provider server discloses limitation [1.2], this would conflict with the '656 Patent's claimed transaction flow. The independent claims of the '656 Patent include a timing requirement for the transaction flow. *See* Pet. 39-51 and "Listing of Challenged Claims" at vii-viii.

84. The "capture" of "biometric information and location data associated with the user," and "fraud detection analysis" comprising "performing a comparison

based at least in part on the stored biometric information and the captured biometric information” must occur after the account holder’s biometric information is stored and associated with the account of the account holder in limitation [1.2]. If not, no stored biometric information is available to be used for comparison. But Stone only discloses possibly associating the biometric id with a user’s account “with a user money transfer request to the payment provider server,” Ex. 1008 at [0045], i.e., after the user has completed the “confirm” step 316 in the graphic above. So this not only conflicts with the ’656 Patent’s claimed transaction flow, but Stone’s failure to disclose stored biometric information associated with a user prior to the time a transaction request is submitted to the server further highlights that a POSITA would not have sought to implement Hoyos’s (local) authentication techniques after Stone’s “confirmation” step as the ’656 Patent’s claims require. This further proves that Petitioner’s Ground 1 is rooted in hindsight bias.

85. Petitioner also argues that “to the extent Stone does not explicitly describe ‘biometric id’ as the reference biometric information for comparison in authentication, Hoyos expressly describes receiving and storing biometric information during enrollment, and the stored biometric information is used for comparison with subsequent captured biometric data during transaction authentication.” Pet. at 33 (citing Ex. 1003, ¶94; Ex. 1013 (“Hoyos”) at [0003]).

Hoyos, however, does not teach receiving, storing, and associating with an account biometric information in a data store as claimed by the '656 Patent's limitation [1.2]. The paragraph of Hoyos that Petitioner cites as disclosing limitation [1.2] is a generic description of the biometric matching technology known in the art at the time the Hoyos application was filed. *See* Pet. at 33 (citing Hoyos at [0003] ("Biometric identification and authentication systems . . . are known to be useful for [] **comparing** biometric data acquired from an individual to **stored sets of biometric data of known "enrolled" individuals**")). Besides not disclosing limitation [1.2], a POSITA would not have been motivated to combine Hoyos's local authentication with Stone's client-server structure, particularly in terms of the "association" step that occurs on the payment server 408 in Stone.

3. Stone-Hoyos-Varghese does not disclose or render obvious limitation [1.9].

86. Limitation [1.9] recites "a memory coupled to the processor and configured to provide the processor with instructions." Petitioner contends that "Stone discloses a memory (e.g., system memory component 506 of FIG. 5) coupled to a processor 504 in each device of the system, and the memory is configured to provide the processor with instructions for various processes for an electronic transaction." Pet. at 51. However, Petitioner has not identified "a memory coupled

to the processor and configured to provide the processor with instructions,” as required by the claim 1 of the ’656 Patent. The embodiment of system 500 depicted in Figure 5 of Stone may be a part of a cell phone, personal computer, and/or a network server. See Stone at [0049]. Stone states that “system 500 performs specific operations by processor 504 executing one or more sequences of one or more instructions contained in the system memory component 506.” Stone at [0050]. Figure 4 and Figure 5 of Stone are reproduced below.

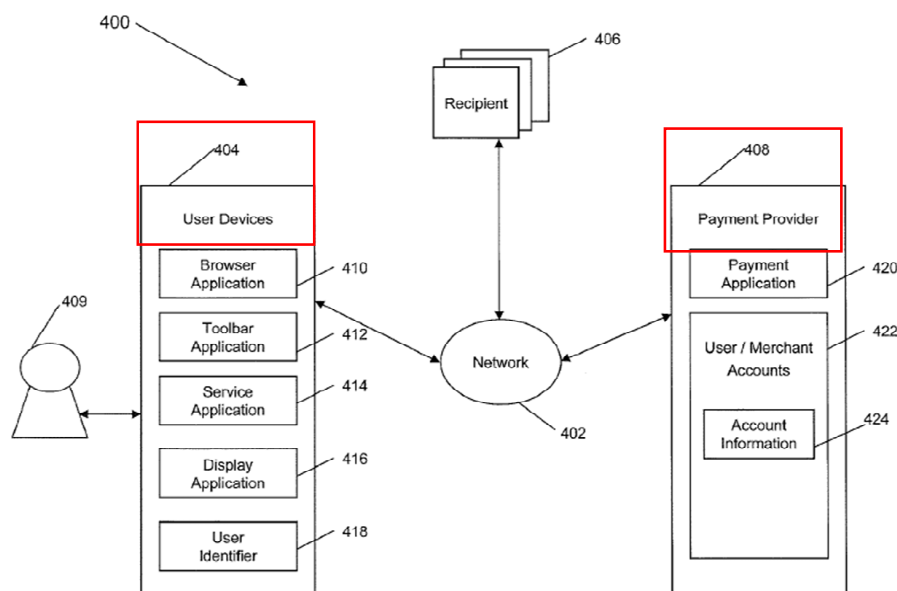


FIG. 4

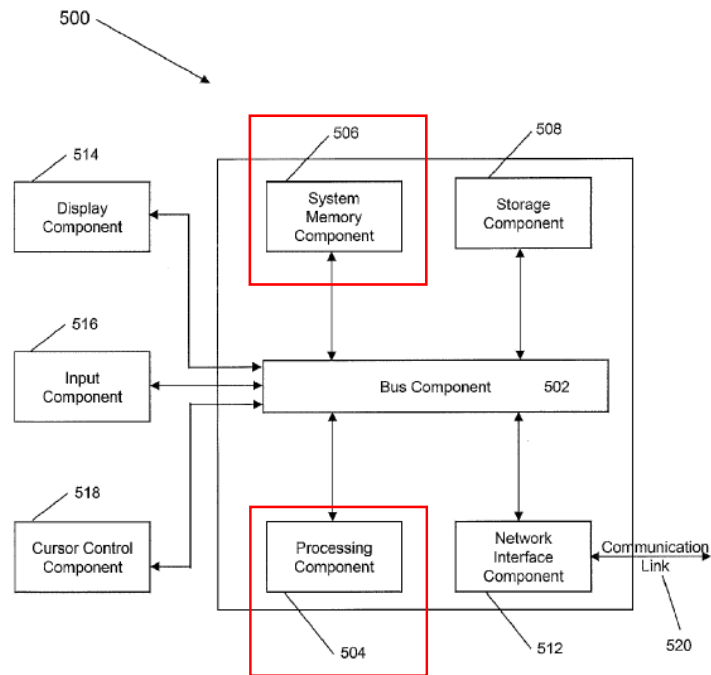


FIG. 5

87. For the disclosure of “a processor” in limitation [1.1], Petitioner identifies in Stone “processor 504 in user device 404 alone, or in combination with other processors including the processor 504 of other devices” as being “configured to perform processes for a transaction.” Pet. at 29-30. Based on the antecedent basis rule, “the processor” in limitation [1.9] refers to the processor identified in limitation [1.1], which performs the other claim limitations in claim 1. For the storing and “association” of the biometric information with the account of the account holder required by limitation [1.2], this is done by the payment server 408 as described in my analysis of that limitation. As limitation [1.9] requires “a memory coupled to the

processor,” to disclose limitation [1.9] under Petitioner’s theory, the “memory” must be at least coupled to the payment server 408 since the payment server must perform the association step. But since Petitioner only identifies the “processor” for limitation [1.1] as the processor on user device 404, Petitioner fails to identify “a memory coupled to *the* processor” as limitation [1.9] requires.

4. Stone-Hoyos-Varghese does not render the dependent challenged claims obvious.

88. Petitioner has not shown that Stone-Hoyos-Varghese renders obvious independent claims 1, 10, and 19. Because the dependent Challenged Claims depend from these independent claims, Stone-Hoyos-Varghese does not render obvious any of the dependent Challenged Claims 4-9 and 13-18 for the same reasons Stone-Hoyos-Varghese does not render obvious the independent claims. In addition, as I explain below, the Stone-Hoyos-Varghese does not disclose the dependent limitations of claims 5, 8, 14, and 17.

89. Dependent claims 5 and 14 require the system of claim 1 (for claim 5) and the method of claim 10 (for claim 14) “wherein the transaction icon comprises a graphical representation of a payment form.” Neither Stone nor Hoyos discloses that a transaction icon can be a payment form. Petitioner states simply that “a POSITA would have been motivated to implement the funding source selection

using a form of payment icon (e.g., ‘the specific card, such as a PayPal card, Visa, MC, AMEX’) for improved visual presentation.” Pet. at 53-54. But Petitioner provides no explanation why this would be obvious other than hindsight bias to reach the ’656 Patent’s claims.

90. Dependent claims 8 and 17 require the system of claim 1 (for claim 8) and the method of claim 9 (for claim 17) “wherein the virtual likeness of the face of the recipient comprises an avatar of the recipient.” Neither Stone nor Hoyos or Varghese discloses the use of an avatar to represent an account holder. Rather, Petitioner merely states that an “avatar is a well-known alternative of a picture for a user icon renders this element obvious.” Pet. at 55-57. But the fact that a claim element is well known does not render it obvious. Besides being supposedly “well known” for use on social networking sites, Petitioner provides no justification why it would be obvious to use an avatar for an electronic payment system—besides hindsight bias—to reach the invention of the ’656 Patent’s claim 6.

B. Ground 2 Does Not Render the Challenged Claims Obvious.

91. Petitioner asserts that Stone in view of the FFIEC Guidance renders obvious independent claims 1, 10, 19 and dependent claims 4-9 and 13-18 of the ’656 Patent. As explained below the Stone-FFIEC Guidance combination does not render the Challenged Claims obvious.

1. Stone-FFIEC Guidance does not disclose or render obvious limitations [1.2] or [1.9].

92. Ground 2 relies on Stone as supposedly disclosing limitations [1.2] and [1.9] for the same reasons described in Ground 1. Therefore, Ground 2 fails to render these limitations obvious for the same reasons I explain in Ground 1.

2. A POSITA would not have been motivated to combine Stone with the FFIEC Guidance.

93. For the reasons I explained in Ground 1, Stone is not analogous art. For this reason alone, Petitioner's alleged motivation to combine Stone and the FFIEC Guidance fails.

94. Additionally, it is my opinion that the Stone-FFIEC Guidance fails because Petitioner's alleged motivation to combine these references is conclusory. Petitioner's alleged motivation to combine consists of four boilerplate paragraphs. *See* Pet. at 62-63. For instance, Petitioner states that a POSITA would have understood based on the Guidance that multifactor authentication can reduce fraud and improve customer protection. *Id.* at 63. Based on this understanding, Petitioner then states that "a POSITA would have been motivated to apply, multifactor, real-time, risk-based authentication taught by the Guidance." *Id.*

95. Considering this, Petitioner then states that "a POSITA would have been motivated to apply Guidance's teaching of multifactor, real-time, contextual-

based and risk-based authentication in Stone for the benefits of improved security and boosted customer confidence for service providers, and the additional benefits of FFIEC compliance for federal supervised financial institutions.” Pet. at 62.

96. Petitioner’s alleged justifications are conclusory and do not actually explain why a POSITA would have combined Stone and the FFIEC Guidance. Petitioner assumes that Stone had a need for authentication for fraud detection, even though Stone does not identify electronic fraud as a problem needing to be addressed. However, Stone is not concerned with security of transactions. Rather, it is concerned with providing an improved display for the user and “richer interface” that provides a currency display. Ex. 1008 at [0016]. Stone also does not view fraud as a problem that needs to be addressed, with increased security, nor does it even mention electronic payment fraud. Petitioner never once cites the Stone reference when stating that it was known that the transactions of Stone require additional security. *See, e.g.*, Pet. at 63.

97. The FFIEC Guidance is also not concerned with what Stone is concerned with. Stone is directed to facilitating the transfer of funds and providing visual representations of currency or providing a digital interface. The FFIEC Guidance is not directed to improving an interface, for example. The Guidance addresses biometrics and security at a general, regulatory level, not an

implementation level. Ex. 1037 at 1-2, 9-11. The Guidance, for example, never discusses using multifactor or biometric authentication with a digital interface, or combining these components in an ordered manner like the claims of the '656 Patent. So like Stone and Hoyos, Stone and the FFIEC Guidance are directed to separate objectives.

98. The FFIEC Guidance is also not something that would be of interest to a POSITA per the Petitioner's own definition, which defines a POSITA as someone with 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." Pet. at 4. Based on this definition, a POSITA would not be interested in high-level regulatory guidance when seeking to develop and implement improved technical solutions for fraud detection and prevention.

99. For the reasons just discussed, it is my opinion that Petitioner's argument is a hindsight combination of these references to reach the limitations of the '656 Patent's independent claims without giving anything more than perfunctory statements for why a POSITA would have combined them. *See* Pet. at 62-63.

3. Stone-FFIEC Guidance does not render the dependent claims obvious.

100. Petitioner has not shown that Stone-FFIEC Guidance renders obvious independent claims 1, 10, and 19. Because the dependent Challenged Claims depend from these independent claims, Stone-FFIEC Guidance does not render obvious any of the dependent Challenged Claims 4-9 and 13-18 for the same reasons Stone-FFIEC Guidance does not render obvious the independent claims. In addition, the Stone-Hoyos-Varghese does not disclose the dependent limitations of claims 5, 8, 14, and 17 for the same reasons I explained in my analysis of Ground 1.

C. Grounds 3 and 4 Do Not Render the Challenged Claims Obvious.

101. Petitioner asserts that Stone in view of the Hoyos, Varghese, and Borovsky (Ground 3) or Stone in view of the FFIEC Guidance and Borovsky (Ground 4) render obvious dependent claims 2-3 and 11-12 of the '656 Patent. Petitioner states that Ground 3 relies on the same analysis and evidence provided for Ground 1 (Stone-Hoyos-Varghese), except where additional analysis is provided for the dependent limitations for the respective claims, and Ground 4 relies on the same analysis and evidence provided for Ground 2 (Stone-FFIEC Guidance), except where additional analysis is provided for the dependent limitations of each claim. Because Grounds 3 and 4 rely on the same evidence as Grounds 1 and 2 respectively, Grounds 3 and 4 do not render obvious any of these dependent claims for the same

reasons Grounds 1 and 2 do not render the independent claims obvious.

102. Moreover, a POSITA would not have been motivated to combine Stone and Borovsky as Petitioner claims. Petitioner states that “Stone has the need to obtain for display on the user device, pictures of other users connected to a network with the user.” Pet. at 78; Ex. 1003 at ¶ 278. Petitioner further states that “[f]acing the need of Stone, a POSITA would have been motivated apply Borovsky’s teaching of providing contact photo obtained from social network sites for user device contact display as icons for network-connected users on user device, especially in the case that the other user did not profile a profile icon, for the benefits of enhanced user experience with helpful visuals, increased transaction confidence and efficient identification.” *Id.* But Petitioner does not state why a social networking site would be the obvious source for obtaining a user photo in Stone. For example, Stone does not discuss using social networks to populate any information for the disclosed interface. The source of information is all directly provided by the user (e.g. user identifier 418) and/or banking or credit card information from the payment server 408. *See* Ex. 1008 at [0020], [0036], [0045-48]. Nothing in Stone suggests introducing another third-party server to Stone’s existing client-server. The only motivation for doing would be hindsight bias.

IX. Conclusion

103. For the reasons discussed above, it is my opinion that all Challenged Claims of the '656 Patent are valid.

Dated: October 24, 2024

By:



Michael T. Goodrich, Ph.D.