

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 PETITIONER'S REPLY**

TABLE OF CONTENTS

I.	INTRODUCTION	2
I.	LEVEL OF ORDINARY SKILL IN THE ART.....	3
II.	GROUND 1: COMBINATION OF STONE, HOYOS AND VARGHESE (STONE-HOYOS-VARGHESE) RENDERS THE CHALLENGED CLAIMS OBVIOUS.....	3
A.	Stone-Hoyos-Varghese renders obvious the challenged independent claims.....	3
1.	A POSITA would have been motivated to combine Stone, Hoyos, and Varghese.	3
2.	Stone in view of Hoyos and Varghese renders obvious “wherein the virtual likeness of the face was selected by the account holder as part of an enrollment” as recited in [1.2.2]..	12
3.	Stone in view of Hoyos and Varghese renders obvious [1.3.1].	18
B.	Stone in view of Hoyos and Varghese renders obvious the challenged dependent claims.....	20
III.	GROUND 2: STONE IN VIEW OF FFIEC RENDERS THE CHALLENGED CLAIMS OBVIOUS.....	22
A.	A POSITA would have been motivated to combine Stone and FFIEC.	22
B.	Stone-Guidance renders obvious limitation [1.2.2].	26
C.	Stone-Guidance renders obvious limitation [1.3.1].	26
D.	Stone-Guidance renders obvious the challenged dependent claims. ..	28
IV.	FOUNDATIONS 3 AND 4: COMBINATION OF STONE, HOYOS, VARGHESE, AND CAMPBELL (GROUND 3) AND COMBINATION OF STONE, GUIDANCE, AND CAMPBELL (GROUND 4) RENDER OBVIOUS CLAIMS 15-17 AND 21-23.	28
V.	DECLARATION	30

I. Introduction

1. I, Creed Jones, previously submitted a declaration as APPL-1003 in this proceeding. The terms of my engagement, my background, qualifications and prior testimony, and the legal standards and claim constructions I am applying are set forth in my previous CV and declaration. *See* APPL-1003; APPL-1004. I offer this declaration in reply to the Response the Patent Owner filed in this proceeding. In forming my opinion, I have considered the materials noted in my previous declaration, as well as the following additional materials:

Ex.2028	U.S. Patent No. 5,164,992 (“Turk Patent”)
Ex.2031	CV of Dr. Michael Goodrich
Ex.2032	Declaration of Dr. Michael Goodrich
APPL-1049	Deposition transcript of Dr. Creed Jones (October 11, 2024)
APPL-1050	Deposition transcript of Dr. Michael Goodrich (January 7, 2025)
APPL-1051	CS 201P - Computer Security, Notes (https://ics.uci.edu/~goodrich/teach/cs201P/notes/ and https://ics.uci.edu/~goodrich/teach/cs201P/notes/Ch10-DRM.pdf)
APPL-1052	WO App. Pub. 2008/020991 to Goodrich et al.
APPL-1053	Deposition transcript of Dr. Michael Goodrich (January 8, 2025)
APPL-1054	Goodrich et al., “Introduction to Computer Security” (October 15, 2010)
APPL-1055	M.J. Atallah, K.B. Frikken, M.T. Goodrich, and R. Tamassia, “Secure Biometric Authentication for Weak Computational Devices,” 9th Int. Conf. on Financial Cryptography and Data Security, Springer, Lecture Notes in Computer Science 3570, 357-371, 2005

II. Level of Ordinary Skill in the Art

2. I was informed that in the Institution Decision, the Board adopted Petitioner's POSITA standard "except for the language 'at least' that qualifies the experience level and allows the experience level to encompass an expert's level of skill." ID, 21. I apply the standard as clarified by the Board. The analysis of my declaration (APPL-1003) remains the same, applying this clarified level of skill for a POSITA.

III. Ground 1: Combination of Stone, Hoyos and Varghese (Stone-Hoyos-Varghese) Renders the Challenged Claims Obvious.

A. Stone-Hoyos-Varghese renders obvious the challenged independent claims.

1. A POSITA would have been motivated to combine Stone, Hoyos, and Varghese.

3. PO states, "Petitioner's explanation for the alleged motivation to combine is conclusory," "Stone is not analogous art to the '886 Patent," and "Stone and Hoyos teach away from each other." POR, 15. PO's arguments are contrary to the record, and are incorrect technically.

a. PO fails to rebut Petition's reasons to combine Stone, Hoyos, and Varghese.

4. PO fails to rebut any of Petition's reasons to combine Stone, Hoyos, and Varghese, which are fully supported by the evidence. Pet. 16-23 (citing numerous supporting references and my prior declaration). Instead, PO's arguments

mischaracterize the prior art and disregard the Petition's explanation regarding a POSITA's understanding of the prior art disclosure.

5. Specifically, PO's arguments mischaracterize Stone as only disclosing "an enhanced currency display," and as "not concerned with the actual processing of transactions" or fraud prevention, by completely disregarding how a POSITA would have understood Stone. POR, 16. PO does not dispute that Stone discloses attributes including "user name," "password," "biometric id." POR, 16 (citing APPL-1008, Stone, [0045]). Further, PO does not dispute that it was well-known that ID/password is used for authentication for electronic transactions, (Pet. 12, citing APPL-1037, 1-2), and does not dispute that it was well-known that "biometric identifiers are most commonly used as part of a multifactor authentication system" for electronic transactions (Pet. 31, 44, citing APPL-1037, 10). *See also* POR, 16-17. As such, PO's assertion that Stone is not concerned with fraud detection for electronic transactions completely disregards Stone's explicit disclosure as would have understood by a POSITA.

6. PO further completely disregards Stone's numerous express disclosures of electronic financial transactions. *See, e.g.*, APPL-1008, Stone, [0004] (describing in related art "Internet commerce" with examples of a consumer transferring funds (e.g., a transaction between "parties in the United States and Russia")), [0005] (describing in related art online bidding where for an accepted bid, "the consumer's

funds are transferred to the seller's account”), [0020] (“the user may simply drag the currency to the other user's icon to **transfer the funds** to the other user”), [0023] (describing display “[w]hen the funds are transferred” and stating that “transferring funds via a mobile phone is known, such as through PayPal in San Jose, Calif.”), FIG. 3, [0035] (“**the shown funds are transferred** to the desired recipient in step 318”); *see* POR 17.

7. A POSITA would have understood that Stone omitted “details of how funds are transferred” (APPL-1008, Stone, [0023]), because such details were well-known in the art. As such, contrary to PO’s assertion that Stone’s omission of the details of how funds are transferred “proves that Stone is not concerned with fraud detection or the processing of electronic transactions,” (POR, 17), Stone expressly discloses that it is concerned with the processing of electronic transactions including fraud detection, and merely omits details of how funds are transferred that were well-known in the art.

8. PO also incorrectly characterizes Hoyos as containing “nothing to suggest a POSITA would apply its teachings to Stone.” POR, 17. Specifically, Hoyos expressly discloses that by using its biometric authentication “combining in one algorithm the live-person result with the match result,” various advantages are achieved, including spoofing prevention; reducing iterative attacks by eliminating clear feedback; reducing “the reject rate of true authentications”; providing “an enormous

deterrent to criminals;" and providing "a means to perform customer redress." APPL-1013, [0024], [0026], [0027], [0029].; Pet., 17. A POSITA would have been aware of the added security offered by spoofing prevention in biometric applications where the biometric sample capture is unsupervised, such as biometric authentication of an online financial transaction. As such, contrary to PO's arguments, Hoyos itself provides express advantages that would have motivated a POSITA to incorporate Hoyos' biometric authentication teachings in Stone.

b. Stone is analogous art.

9. As I discuss in ¶¶5-7, above, Stone is concerned with electronic transactions including fraud prevention for electronic transactions, and as such is in the same field of endeavor as the '886 Patent. APPL-1008, Stone, FIG. 2 (illustrating that a user logged in "PayPal" with a balance displayed). PayPal was a widely used online payment platform allowing users to send and receive money and transfer funds between bank accounts or credit cards.

10. Stone is also pertinent to the particular problem of making an electronic financial transaction seem "more concrete" because "physical cash is a concrete, tangible item while a digital payment for a digital good is a more abstract concept." APPL-1001, 4:28–30, 4:62–67, 5:16–18; APPL-1008, Figs. 1–2 (displaying the "actual currency" for an electronic financial transaction); APPL-1003, ¶122.

c. PO's teaching away arguments are meritless.

i. Stone and Hoyos do not teach away from each other.

11. PO states, "Stone and Hoyos teach away from each other in material ways such that a POSITA would not have been motivated to combine them," because "Stone requires a client-server structure," and Hoyos does not mention a server structure. POR, 23-24. I disagree.

12. Dr. Goodrich appears to apply an improper teaching away standard when references merely include different disclosures or preferences. *See, e.g.,* Ex2032, ¶¶66-67. I understand that a reference teaches away "when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken" in the claim. I understand that a reference that "merely expresses a general preference for an alternative invention but does not criticize, discredit, or otherwise discourage investigation into" the claimed invention does not teach away. Therefore, Dr. Goodrich's teaching away arguments in his declaration should be rejected as he applies the wrong standard.

13. Dr. Goodrich does not show or argue that the references "criticize, discredit, or otherwise discourage investigation into" the claimed invention. In many cases, he appears to merely assume that because a reference discloses one thing, it teaches away from using anything else.

14. As explained by the Petition and supported in my prior declaration, Stone's client-server model and Hoyos' authentication methods are complementary. A POSITA would adapt Hoyos' biometric methods to function within Stone's system (either on the client or on a server), achieving secure authentication without undermining the system's architecture. Pet., 22; APPL-1003, ¶¶67-68 (citing APPL-1016, [0040], [0042] (describing that fraud detection can "be performed locally or by transmission of []data to a remote source"), [0076]; APPL-1015, FIG. 3, 4:4-10; APPL-1038, 64). PO's own expert, Dr. Goodrich, explains for biometric authentications, "[t]here are two broad approaches: The one where the comparison is done at the remote server, and **the one where the comparison is done at the client end** (the portable device where the biometric measurement is done). Most of the recent work has focused on the second category." APPL-1054, 2 (cited as C-101 in Dr. Goodrich's declaration Ex. 2032, paragraph 9).

15. A POSITA would have been aware that biometric authentication in a client-server architecture could be performed on a server or on a client, and that either approach had advantages and disadvantages in specific applications. "Biometric authentication can be implemented through systems performing the matching either on the server or on the client side. Depending on whether the matching of the biometric template is executed - at the server or at the client - different security problems arise." APPL-1038, 64. The authentication methods of

Hoyos are applicable in a client-server model of Stone, either on the client or remotely on a server.

ii. A POSITA would have been motivated to combine Varghese with Stone and Hoyos

16. PO states, “a POSITA would not have been motivated to combine Varghese with Stone and Hoyos,” because “Varghese amplifies the disconnect between Stone and Hoyos regarding the server and client distinction.” POR, 27. I disagree. PO’s arguments fail for the same reasons that I discuss in ¶¶12-15, because there is no disconnect between Stone and Hoyos regarding the server and client distinction, and because a POSITA would have applied Hoyos’ biometric methods to function within Stone’s system (either on the client or on a server), achieving secure authentication without undermining the system’s architecture. Pet., 22; APPL-1003, ¶¶67-68 (citing APPL-1016, [0040], [0042] (describing that fraud detection can “be performed locally or by transmission of []data to a remote source”), [0076]; APPL-1015, FIG. 3, 4:4-10; APPL-1038, 64).

17. PO then states that 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’.” POR, 28. PO’s arguments mischaracterize Varghese and I disagree. Varghese describes a “purely software based solution to identify theft that ***does not require hardware devices to be issued and maintained***”, APPL-1010, Varghese, [0022]. Varghese does not exclude

sensors for capturing biometrics, because its description of “*does not require hardware devices to be issued and maintained*” refer to tokens associated with the “something the user has” factor (e.g., password-generating token). *See, e.g.*, APPL-1037, FFIEC Guidance, APPL-1037, 8-9. Contrary to PO’s assertion, Varghese explicitly describes use of sensor-based biometrics including “obtaining biometric identification information (e.g., fingerprints, retinal scans, or the like).” APPL-1010 Varghese, [00079].

18. PO characterizes Varghese’ collecting location data as **only** a pre-authentication technique for user login requests, and not a technique for the post-authentication for completing monetary electronic transactions. POR, 30. This is incorrect for the reasons described below.

19. As shown in Table 10 below, Varghese explicitly describes capturing real-time contextual information including capturing real-time physical location information in “post-authentication.” APPL-1008, Varghese, [0109] (“**Business policies** generally include rules (referred to as “transaction rules”) that evaluate parameters of individual in-session transactions for the likelihood of fraud or malicious intent. Accordingly, business policies are generally application **during post-authentication** are generally specific to the field or to the business of the service provider and service provider application. For example, in a banking application, specific transaction rules can be directed to specific banking

transactions, e.g. bill pay, transfer funds, and the like. Transaction models can be used in conjunction with security rule, e.g. don't allow (or challenge user for) **money transfer request from an international IP address.**").

20. Contrary to PO's arguments, Table 10 of Varghese further illustrates business policies using real-time location data for the authentication for completing the electronic transaction:

TABLE 10

Restricted business policy model rules
Money transfer request is greater than a certain dollar amount
Money transfer request to and from a specific suspected fraud or an international account
Money transfer request of a certain dollar amount by a user who is logged in from another country
Bill payment to a non-merchant account is greater than certain dollar amount
Transaction from an un-registered device/location or frequently used fraud device/location. This could trigger a customer service request or challenge question or an out of band phone authentication

APPL-1008, Varghese, TABLE 10, annotated.

2. Stone in view of Hoyos and Varghese renders obvious “wherein the virtual likeness of the face was selected by the account holder as part of an enrollment” as recited in [1.2.2].¹

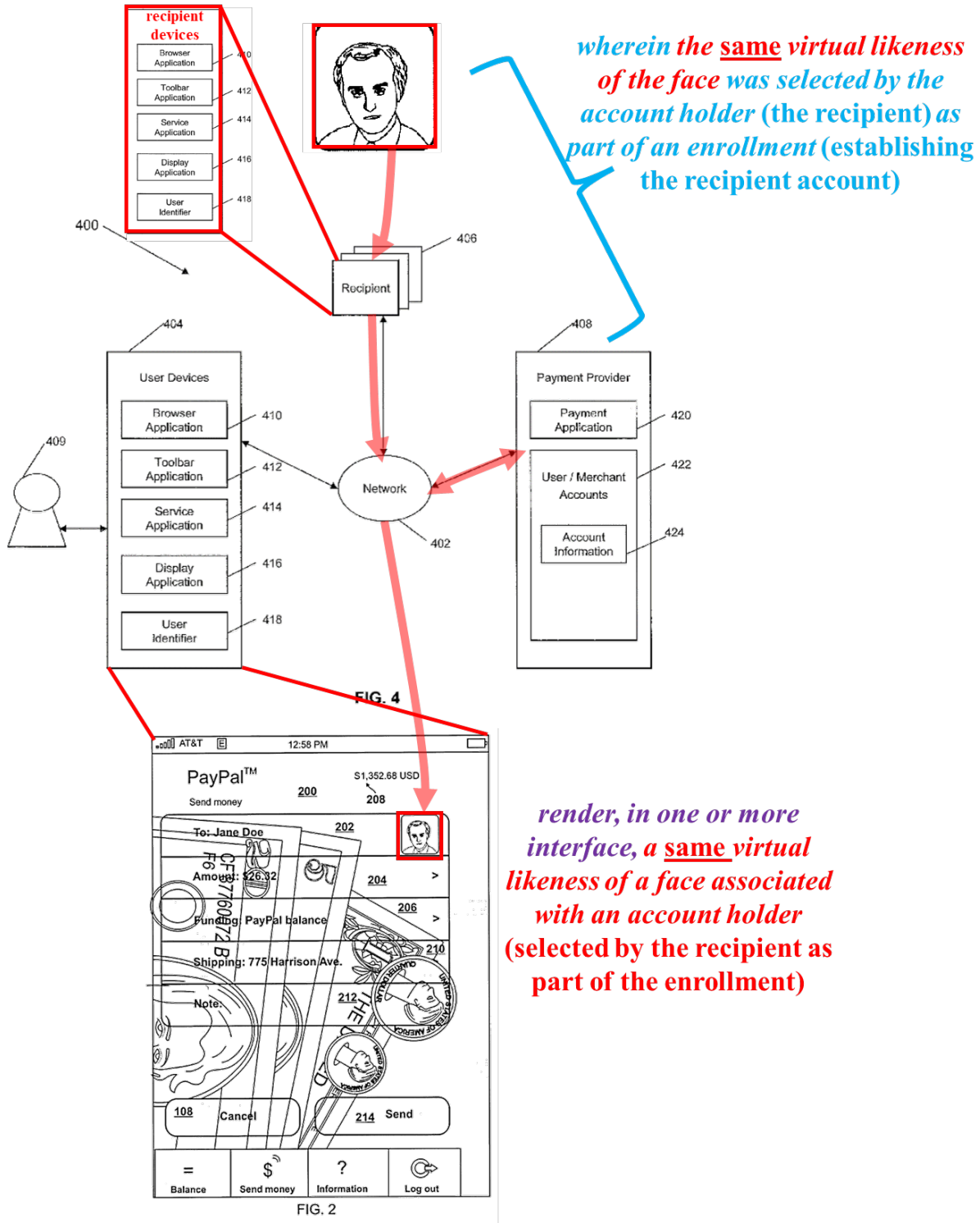
21. PO argues, Stone in view of Hoyos and Varghese does not render obvious “*wherein the virtual likeness of the face was selected by the account holder as part of an enrollment,*” because “Stone does not disclose any enrollment or registration procedure.” (POR, 31). PO’s arguments are meritless and for the reasons given below, I disagree.

a. Stone’s recipient icon renders obvious “the virtual likeness of the face...selected by the account holder as part of an enrollment”.

22. As shown in FIGS. 2 and 4 below, Stone discloses *an enrollment* or registration procedure (the procedure for establishing a recipient account of the recipient with payment server), where the recipient icon displayed on FIG. 2 was selected by the recipient during the enrollment/registration for display. APPL-1008, Stone, [0046] (“Each of the one or more recipient may need to **establish an account** with payment provider server 408 so that payment server provider 408 is able to process money transfers from user 409 with payment provider server”). A POSITA would have understood that such a selected recipient icon, which is associated with

¹ My arguments with respect to limitation [1.2.2] similarly apply to limitations [6.1.2] and [11.1.2].

the recipient account so established, can be stored on the recipient device 406 and/or the payment provider server 408, and would be provided through network 402 such that “user device 404 may be able to access recipient attributes, such as icon information, for display or use by user device 404.” APPL-1008, Stone, [0046].



APPL-1008, Stone, FIGS. 2 and 4, Composited and Annotated.

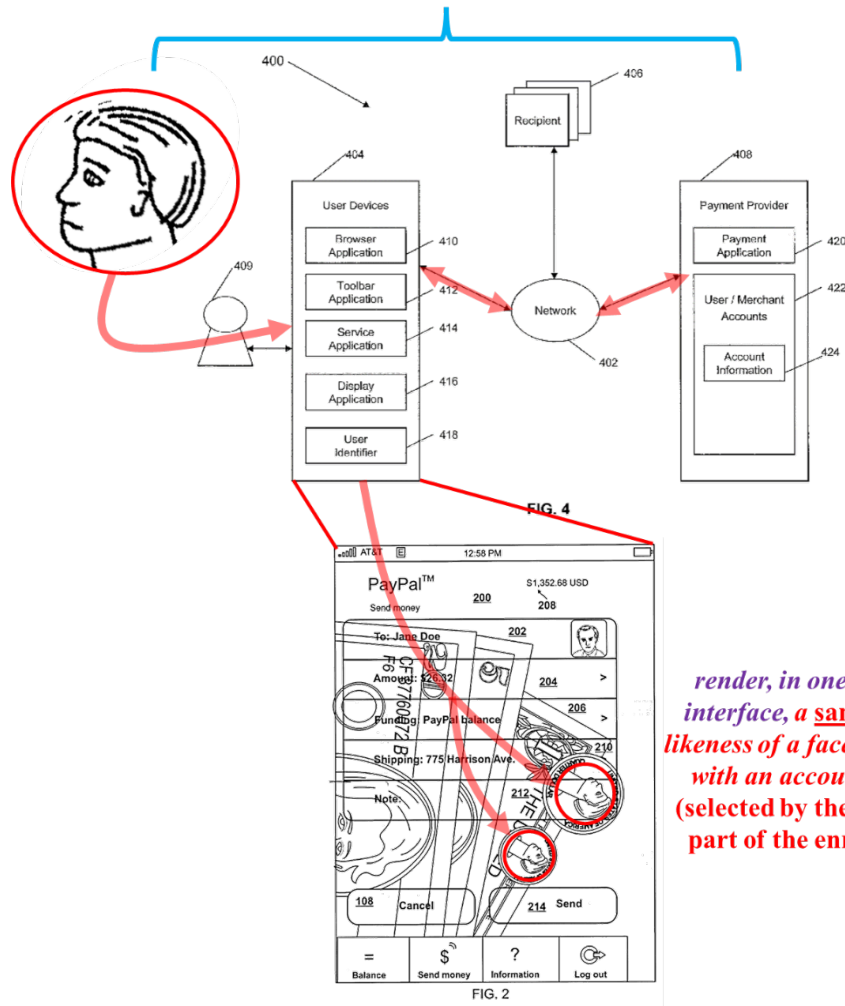
23. As explained in Petition, Stone's electronic transaction system provides a well-known social networking aspect for connecting people. APPL-1008, FIG. 2, [0020] (describing the social media aspect of the transaction application, "[w]hen the user is connected to a network with other users, the user display may visually show other users"), [0036] (describing that "an appropriate icon" of a selected recipient or "multiple icons" of the recipient may be displayed). As such, in Stone combined with Hoyos and Varghese, a POSITA would have been motivated to provide a user (the recipient) an option to select a profile icon, which the user can "designate[] as available to other users for purposes of presenting the user," thereby allowing "the user to select an online identity to connect with others." APPL-1009, 1:20-28, 15:15-27.

b. Stone's sender icon renders obvious "the virtual likeness of the face...selected by the account holder as part of an enrollment".

24. As shown in FIGS. 2 and 4 below, and similar to the recipient account enrollment discussed above at III.A.2.b (§§22-23, above), Stone discloses *an enrollment* or registration procedure (the procedure for establishing a sender account of the sender with payment server), where the sender icon displayed on FIG. 2 was selected by the sender during the enrollment/registration for display. APPL-1008, Stone, [0046], [0045] ("user account maintained by payment provider server 408" which is generated with the enrollment procedure), [0048] ("payment provider

server 408 may be configured to maintain plurality of user and recipient accounts 422," which are established as part of the enrollment/registration procedure).

*wherein the same virtual likeness of the face
was selected by the account holder (the sender)
as part of an enrollment (establishing the
sender account)*



APPL-1008, Stone, FIGS. 2 and 4, Composited and Annotated.

25. In Stone-Hoyos-Varghese, a POSITA would have been motivated to use the sender photo selected by the sender during enrollment (stored either in the user device or in the payment provider, whichever design option is chosen), because

that photo would already be stored in the system. Use of the already stored photo would be understood to be efficient and reliable and avoid redundancy and unnecessary user effort, compared to a new separate user photo to be provided by the user. Additionally, using the same user icon that the sender selects as online identity for display for other users on its own device provides various benefits including, e.g., providing the sender confirmation that its chosen image is being displayed correctly, consistency between the image shown to the sender and the other users, and increasing the user's trust in the platform where the sender is ensured that its selected profile image is presented as intended.

c. PO disregards the fundamental knowledge that biometric authentication, such as that in Stone combined with Hoyos and Varghese, includes an enrollment stage and an authentication stage.

26. PO disregards fundamental knowledge of biometric authentication well-known in the art. Specifically, Stone discloses biometric ID and performs the biometric authentication process. Further, Hoyos and Varghese each disclose biometric authentication. However, PO argues that Stone-Hoyos-Varghese does not teach enrollment, which completely disregards a POSITA's fundamental knowledge that biometric authentication—such as that in Stone-Hoyos-Varghese—performs a comparison based at least in part on the stored biometric information (obtained and stored during its enrollment stage) and the captured biometric information (e.g. captured through live scan at its transaction authentication stage). Pet., 69-70; APPL-

1003, ¶209; APPL-1014, [0009]; APPL-1021, Abstract; APPL-1023, 8:3-9:39; APPL-1013, [0003]; APPL-1024, 3:6-11; APPL-1033, FIG. 3; APPL-1037, 9-10.

3. Stone in view of Hoyos and Varghese renders obvious [1.3.1].

27. Limitation [1.3.1] recites, “*one or more processors configured to . . . 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.*” PO argues that “a POSITA would not have been motivated to implement Varghese’s location capture at the final step of the above transaction model,” because PO asserts that the “device’s geolocation would have **already been** collected during the pre-authentication phase” of Varghese. POR, 36. PO mischaracterizes Varghese as **only** collecting location data during the pre-authentication phase (e.g., user login).

28. As shown in FIG. 14 and Table 10 below, contrary to PO’s arguments, Varghese disclose “**real-time** analytics” including capturing real time location data for post-authentication for “in-session transactions.” APPL-1010, Varghese, FIG. 14; [0109].

*subsequent to [login] and
during post-authentication:
capture contextual information
comprising location data usable
to determine a physical location
associated with the user*

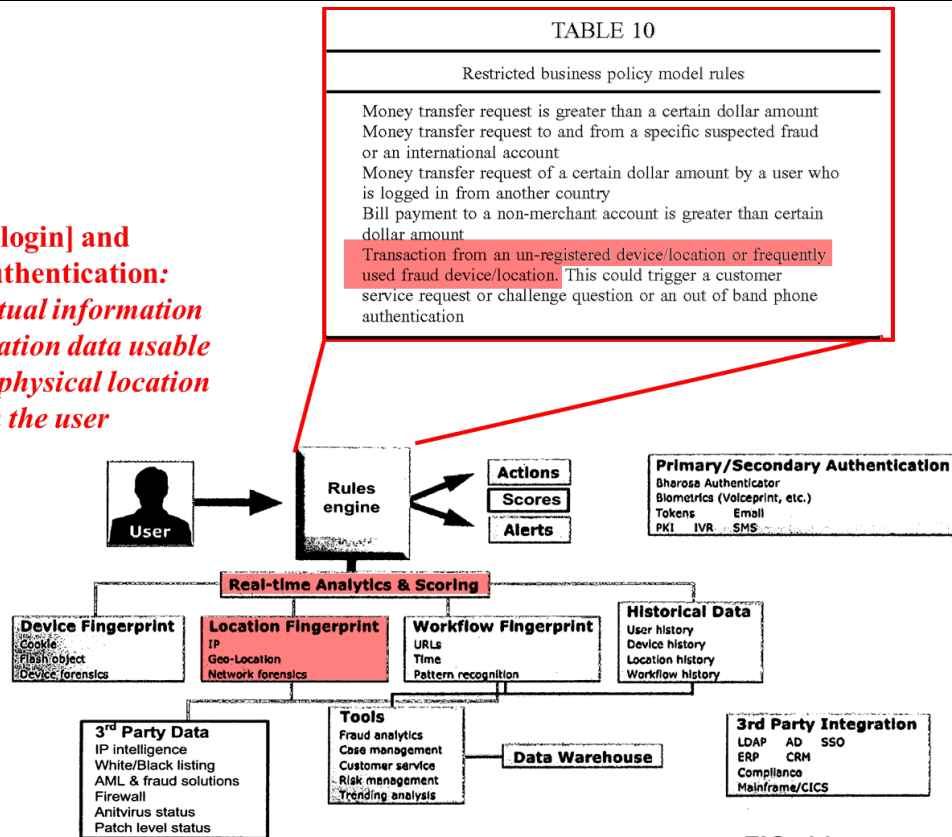


FIG. 14

APPL-1010, Varghese, FIG. 14 and Table 10, annotated.

29. Specifically, Varghese describes that “**real-time analytics & scoring**” can be applied to business policies, which “generally include rules (referred to as “transaction rules”) that evaluate parameters of **individual in-session transactions** for the likelihood of fraud or malicious intent. Accordingly, business policies are generally application [sic] during post-authentication [and] are generally specific to the field or to the business of the service provider and service provider application.” APPL-1010, Varghese, [0109]. As an example, “in a banking application, specific transaction rules can be directed to specific banking

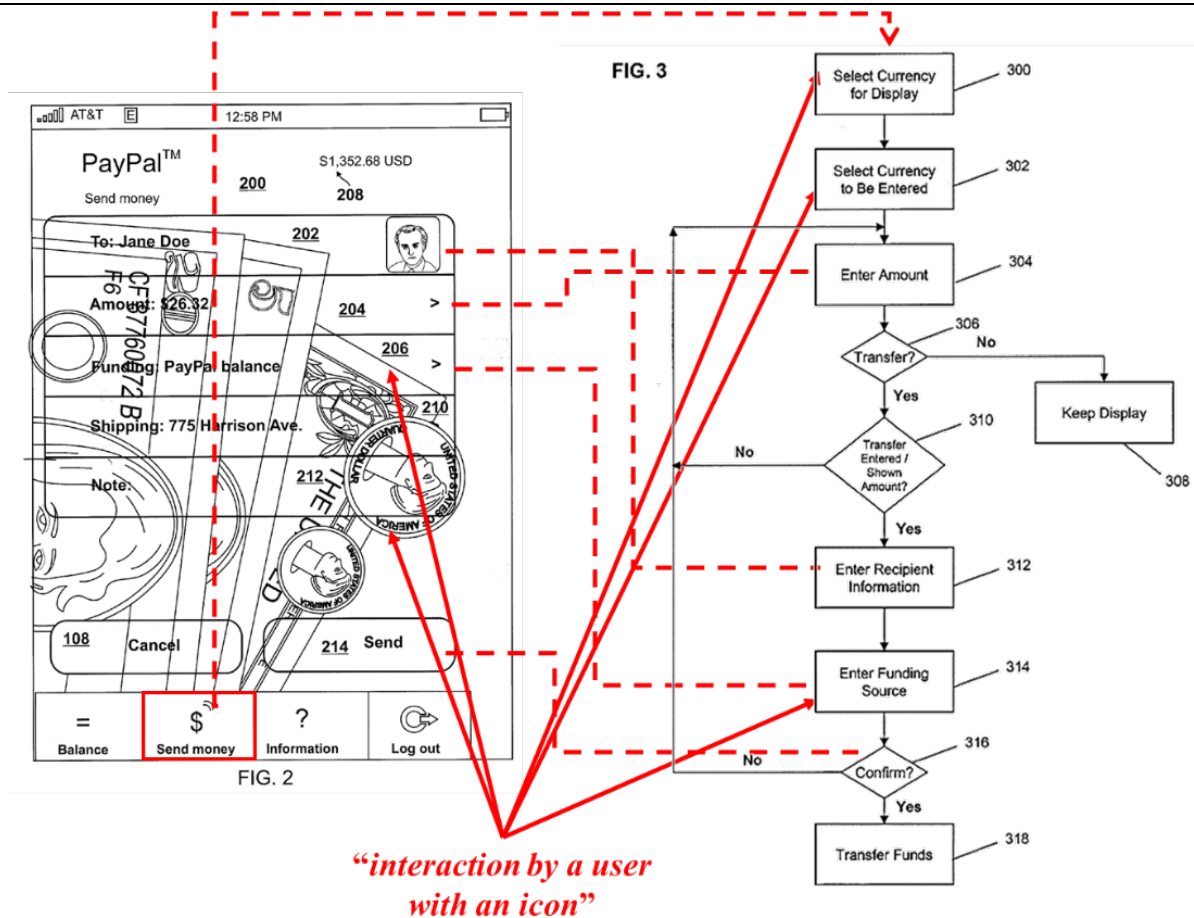
transactions, e.g. bill pay, transfer funds, and the like. Transaction models can be used in conjunction with security rules, e.g. don't allow (or challenge user for) money transfer request from an **international IP address.**"). *Id.*

B. Stone in view of Hoyos and Varghese renders obvious the challenged dependent claims.

30. Stone in view of Hoyos and Varghese renders obvious the limitations of dependent claims 2, 4-5, 7, 9-10, 12, 14-18, and 20-23.

31. PO's arguments for dependent claim limitations are limited to "*wherein the icon represents a form of payment*" in claims 3 and 8, alleging that "Stone and Hoyos do not disclose that a transaction icon can be a payment form." POR, 36-37. I disagree. PO's arguments misrepresent Petitioner's combination and are contrary to the disclosure of the prior art. Pet., 55-58; APPL-1003, ¶¶150-154.

32. Stone teaches a *transaction icon* associated with a funding source ("funding source box 206" on FIG. 2 to implement the step 314 "Enter Funding Source"), as shown in the annotated FIGS. 2-3 of Stone below.



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

33. Stone teaches *graphical representation of payment form* of funding sources (display of “specific card, such as a PayPal card, Visa, MC, AMEX, etc.”). APPL-1008, [0038].

34. A POSITA would have been motivated to implement *a graphical representation* related to a specific user transaction for a user interface item (*transaction icon*) related to that specific user transaction.

35. A POSITA would have been similarly motivated to use payment form icons (e.g., type of currency) associated with blocks 300 and 302 for selecting types of currency.

IV. Ground 2: Stone in view of FFIEC Renders the Challenged Claims obvious.

A. A POSITA would have been motivated to combine Stone and FFIEC.

36. I understand that PO does not dispute that Guidance is analogous art to the '886 Patent. I also understand that PO does not dispute that a POSITA “could have accessed” the Guidance. POR, 44. Instead, PO argues that the “Guidance is outside a POSITA’s area of interest” because a POSITA “**would not have been inclined to** look to high-level and non-technical regulatory guidance directed to the banking industry to develop precise technical solutions for electronic fraud.” POR, 42-43. I disagree. PO’s arguments are contrary to my own experience, contrary to the record illustrating a POSITA’s interest in the Guidance, contrary to its own expert’s practices, and contrary to the law as it has been explained to me.

37. As discussed at Section II above, the POSITA standard I apply is 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 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.

38. Based on my own experience as a professor and an engineer, and based on my own experience as a supervisor of students and engineers who were POSITAs, it is my opinion that a POSITA would have been interested in the Guidance. In other words, the Guidance is within a POSITA's area of interest, and persons interested in the subject matter or art of biometric authentication can locate it exercising reasonable diligence.

39. At the time that the Guidance was issued, 2005, I was a project engineer at Sagem Morpho, involved in the design of fingerprint-based identification systems, some of which were used for financial authentication. I was also heavily engaged in the development of national and international standards for the use of biometric identification, as the chair of the ANSI-accredited INCITS M1.3 subcommittee on biometric data interchange formats and a member of the US delegation to ISO/IEC JTC1 SC37, the international committee on biometric standardization. I first became aware of the FFIEC Guidance document in the standardization arena, and we in M1 and SC37 considered it carefully. It represented valuable input from the financial community on the requirements for biometric authentication of financial transactions, and standards for data storage and transmission, interoperability, API standardization and biometrics use were all developed with this Guidance in mind.

40. At Sagem Morpho, I was a supervisor to engineers who were POSITAs, and it was my own experience that the Guidance was within the interested subject matter of a POSITA. It was my personal experience that POSITAs in the engineering staff at Sagem Morpho were interested in the Guidance, and further used the Guidance as part of our approach of providing biometrics subsystems for use in financial applications. It was also my personal experience that POSITAs in the development staff of our parent company, SAGEM SA, who developed fingerprint sensors and biometric terminals, were interested in the Guidance.

41. PO's arguments are contrary to the record illustrating a POSITA's interest in the Guidance. Pet., 11-12; APPL-1003, ¶¶50-52 (citing APPL-1039, APPL-1040, Google Scholar cites, archive.org links, and patent disclosures referencing Guidance as the driver for multifactor authentication in financial transactions); APPL-1049, 54:19-57:9 (I explained during deposition the significance of the Guidance in the biometrics industry and my personal knowledge of the Guidance).

42. A POSITA working in the field of biometric authentication would have recognized the importance of understanding regulatory frameworks that guide industry best practices, even if the guidance itself is not technical in nature because these frameworks influence the design and deployment of security technologies in real-world applications where regulatory compliance is crucial.

43. PO's arguments are contrary to its own expert, Dr. Goodrich's own practices. For example, in his own patent application, WO 2008/020991, Dr. Goodrich describes that technical solutions are developed in response to regulatory guidelines. APPL-1052, [0010] ("In the past decade, the European Union and its member states have implemented a legal framework to provide guidance on processing of personal data with the specific aim to restore citizens' control over their data. To complement the legal framework, Camenisch et al. presented the architecture of PRIME (Privacy and Identity Management for Europe), which implements a technical framework for processing personal data."). Similarly, Dr. Goodrich' class notes for computer security, which is a course for undergraduates, include an entire chapter for "Digital Rights Management," covering "U.S. Copyright History" including "US Constitution," "Copyright Act of 1790," "Copyright Act of 1976," "Faire Use Doctrine," "Sony vs. Universal Studios," "Digital Millennium Copyright Act (DMCA). APPL-1051, 2-9; APPL-1053, 13:4-7, 23-24 (Dr. Goodrich testifying that for the "computer security course," "the goal was to design it for freshmen and sophomores," and "I was going for undergraduates for that class."); APPL-1054, 10 (Dr. Goodrich's textbook "Introduction to Computer Security" used for his undergraduate class includes an entire section on "Legal Issues" in Digital-Rights Management). As such, a student at the undergraduate level (a threshold which a POSITA has met) would have understood

that the integration of technical knowledge with regulatory compliance is standard practice to ensure that products meet both technical specifications and legal requirements. A POSITA would therefore be interested in the Guidance.

B. Stone-Guidance renders obvious limitation [1.2.2].

44. Stone-Guidance renders obvious limitation [1.2.2] for the same reasons discussed above at III.A.2. *See* ¶¶21-25, above (discussing Stone).

C. Stone-Guidance renders obvious limitation [1.3.1].

45. PO states, “Stone-FFIEC Guidance fails to disclose limitation [1.3.1] ‘one or more processors configured to . . . 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,’” because the “Guidance does not disclose the *timing* of when the allegedly disclosed authentication is performed.” POR, 38-39. The gist of PO’s argument appears to be that a POSITA would not have understood that Guidance discloses that the capturing of the contextual information for the authentication to complete a financial transaction is performed after a user interaction with the interface. I disagree. PO’s arguments are contrary to the record and Petitioner’s combination.

46. Contrary to PO’s assertion, a POSITA would have understood that the Guidance discloses the **timing** of when the authentication is performed, because a POSITA would have understood that Guidance discloses “real-time” authentication

with a level appropriate to the risk associated with a financial transaction, where the risk associated with a financial transaction is determined **after** the user provides the value and type of the transaction (e.g., by interacting with an icon as taught in Stone). Pet. 75-76; APPL-1037, 1-2 (requiring multifactor authentication for “high-risk transactions,” and authentication methods should depend upon risk assessment), 6 (“The level of authentication used by the financial institution should be appropriate to the risks associated with those products and services”), 10 (using “live-scan process” for biometrics), 12 (performing location authentication “in a real-time environment”).

47. Such POSITA's understanding of the Guidance's teaching is consistent with the well-known knowledge in the art. APPL-1016, [0036] (“increased authentication requirements as the value of the transaction increases,” where the value of the transaction is provided by user interaction), [0043] (determining a higher authentication level for “significant transactions having high value,” where the high value of the transaction is provided by a user), [0073] (“different authentication levels may be necessary for different transactions, based on factors such as value and type of transaction, as well as other factors,” where value and type of transaction are provided by a user); Pet. 75-76.

48. Furthermore, a POSITA's understanding of the Guidance's teaching, including applying its real-time authentication after receiving transaction

information from user interaction, is consistent with the knowledge in the art that authentication techniques are performed for user logon and transaction completion after user logon. *See, e.g.*, APPL-1010, Varghese, generally (describing applying authentication for both pre-authentication (user logon) and post-authentication (transaction after user logon)), FIG. 14, [0091], TABLE 10; APPL-1016, [0036] (“increased authentication requirements as the value of the transaction increases,” where the value of the transaction is provided by user interaction), [0043] (determining a higher authentication level for “significant transactions having high value,” after the value of the transaction is provided by user interaction).

D. Stone-Guidance renders obvious the challenged dependent claims.

49. PO relied upon its arguments in Ground 1 and argued that Stone-Guidance does not render the challenged dependent claims obvious. POR, 40-46. PO's arguments fail for the same reasons that they fail for Ground 1 as explained above. *See* ¶¶3-35, above (relative to Ground 1).

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

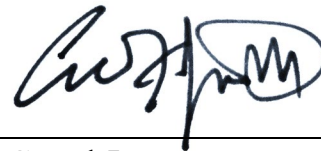
50. I understand that PO does not dispute that Campbell teaches the limitations of claims 15-17 and 21-23. Instead, PO simply states that because “claims 15-17 and 21-23 depend from the independent claims, Grounds 3 and 4 do not [sic] these dependent claims obvious” for the same reason it stated relevant to Grounds 1

and 2. POR, 44. PO's arguments fail for the same reasons discussed at Grounds 1 and 2 above. *See* ¶¶3-49, above (relative to Grounds 1 and 2).

VI. DECLARATION

51. 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 16, 2025

A handwritten signature in black ink, appearing to read 'Creed Jones', is written over a horizontal line.

Dr. Creed Jones