

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner

Case: IPR2024-00331
U.S. Patent No. 11,526,886

**PATENT OWNER'S SUR-REPLY TO PETITIONER'S REPLY TO
PATENT OWNER'S RESPONSE**

TABLE OF CONTENTS

I. INTRODUCTION	1
II. GROUND 1: STONE COMBINED WITH HOYOS AND VARGHESE DOES NOT RENDER THE CHALLENGED CLAIMS OBVIOUS.	2
A. STONE-HOYOS-VARGHESE DOES NOT RENDER OBVIOUS THE CHALLENGED INDEPENDENT CLAIMS.	2
1. A POSITA would not have been motivated to combine Stone, Hoyos, and Varghese.	2
2. Stone-Hoyos-Varghese does not render obvious “wherein the virtual likeness of the face was selected by the account holder as part of an enrollment” as recited in limitation [1.2.2].	12
3. Stone-Hoyos-Varghese does not render obvious limitation [1.3.1].	15
4. Stone-Hoyos-Varghese does not render obvious limitation [1.5]: “a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.”	21
B. STONE-HOYOS-VARGHESE DOES NOT RENDER OBVIOUS THE CHALLENGED DEPENDENT CLAIMS.	23
III. GROUND 2: STONE COMBINED WITH THE FFIEC GUIDANCE DOES NOT RENDER THE CHALLENGED CLAIMS OBVIOUS.	24
A. A POSITA WOULD NOT HAVE BEEN MOTIVATED TO COMBINE STONE WITH THE FFIEC GUIDANCE.	24
B. STONE COMBINED WITH THE GUIDANCE DOES NOT RENDER ANY OF THE CHALLENGED CLAIMS OBVIOUS.	26
IV. 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.	26
V. CONCLUSION	26

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Intelligent Bio–Sys., Inc. v. Illumina Cambridge, Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	23
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	4
<i>NTP, Inc. v. Research in Motion, Ltd.</i> , 418 F.3d 1282 (Fed. Cir. 2005)	12

TABLE OF EXHIBITS

Exhibit	Description
2001	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 14 (Defendant’s Rule 12(b)(6) Motion to Dismiss the Complaint for Failure to State a Claim Under 35 U.S.C. §101) (W.D. Tex. May 24, 2023)
2002	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 30 (Plaintiff’s Response to Defendant’s Rule 12(b)(6) Motion to Dismiss the Complaint for Failure to State a Claim Under 35 U.S.C. §101) (W.D. Tex. June 1, 2023)
2003	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 31 (Defendant’s Reply Brief In Support of Motion to Dismiss for Failure to State Claim Under 35 U.S.C. §101) (W.D. Tex. June 28, 2023).
2004	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 64 (Defendant’s Opposed Motion to Stay Pending Transfer) (W.D. Tex. November 28, 2023)
2005	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 37 (Defendant’s Opposed Motion to Transfer (redacted)) (W.D. Tex. July 26, 2023)
2006	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 66 (Carbyne’s Response to Motion to Stay Pending Transfer) (W.D. Tex. December 5, 2023)
2007	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 50(Carbyne’s Response to Motion to Transfer Venue) (W.D. Tex. October 27, 2023)
2008	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 55 (Apple’s Reply In Support of Its Motion to Transfer Venue) (W.D. Tex. November 10, 2023)

2009	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 60 (Carbyne’s Surreply in Response to Motion to Transfer Venue) (W.D. Tex. November 16, 2023)
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)
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)
2015	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 73 (Apple’s Motion to Stay Pending The Court’s Written Order on Transfer) (W.D. Tex. January 17, 2024)
2016	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 79 (Carbyne’s Response to Motion to Stay Pending Written Order on Transfer) (W.D. Tex. January 24, 2024)
2017	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 80 (Apple’s Reply in Support of Motion to Stay Pending Court’s Written Order on Transfer) (W.D. Tex. January 24, 2024)
2018	<i>In Re Apple</i> , Case No. 2024-111, Dkt 2 (Apple’s Petition for Writ of Mandamus) (Fed. Cir. February 1, 2024)

2019	<i>In Re Apple</i> , Case No. 2024-111, Dkt. 13 (Carbyne’s Response to Writ of Mandamus) (Fed. Cir. February 20, 2024)
2020	<i>In Re Apple Inc.</i> , Case No. 2024-111, Dkt 15 (Apple’s Reply In Support of Petition for Writ of Mandamus) (Fed. Cir. February 27,
2021	<i>In Re Apple Inc.</i> , Case No. 2024-111, Dkt 18 (Order Denying Writ of Mandamus) (Fed. Cir., March 18, 2024)
2022	United States Patent and Trademark Office Memorandum Dated June 21, 2022 re: Interim Procedure for Discretionary Denials in AIA post-grant proceedings with Parallel District Court Litigation
2023	<i>Cloud of change, LLC v. Lightspeed POS Inc.</i> , Case NO. 6:21-cv-0102 Order Denying Lightspeed POS Inc’s Opposed Motion to Stay Pending Resolution of <i>Inter Partes</i> Review (W.D. Tex. Dated May 15, 2023)
2024	<i>Sonrai Memory Limited v. LG Electronics, Inc.</i> 2022 WL 2307475 (W.D. Tex. June 27, 2022)
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)
2026	Email Correspondence From Counsel Of Petitioner To Counsel of Patent Owner re <i>Sotera</i> Stipulations and <i>Carbyne Biometrics, LLC v. Apple Inc.</i> , 1:23-cv-0032 (W.D. Tex.)
2027	Email Correspondence From Counsel Of Petitioner To The Board re <i>Sotera</i> Stipulations for IPRs IPR2024-00329, -00330, -00331, -00332, -00333, -00334 and-00507
2028	U.S. Patent No. 5,164,992 (“Turk Patent”)
2031	CV of Dr. Michael Goodrich
2032	Declaration of Dr. Michael Goodrich

2033	<i>Carbyne Biometrics, LLC v. Apple Inc.</i> , Case No. 1:23-cv-00324, Dkt 155 (Apple Inc.’s Final Election of Asserted Prior Art) (W.D. Tex. October 23, 2024)
------	---

I. INTRODUCTION

Carbyne Biometrics LLC (“Patent Owner”) files this sur-reply responding to Apple Inc.’s (“Petitioner”) Reply to Patent Owner’s Response concerning U.S. Patent No. 11,526,886 (“the ’886 Patent”). Petitioner has failed to meet its burden to establish that any Challenged Claim of the ’886 Patent is obvious. Petitioner’s reply only highlights the shortcomings of its purported obviousness grounds.

First, Petitioner cannot establish that a POSITA would have been motivated to combine Stone with the secondary references for any of its obviousness grounds. Unlike the ’886 Patent, Stone is not directed to reducing fraud in electronic transactions, much less directed to eradicating spoofing of biometric authentication systems by employing techniques to ensure the user is alive as disclosed by Petitioner’s secondary references. *Second*, Petitioner has failed to show that its references disclose a virtual likeness of the face of the account holder rendered in a user interface and that was selected as part of an enrollment process as required by the ’886 Patent’s Challenged Claims. *Third*, Petitioner fails to show that a POSITA would have been motivated to implement Varghese’s location capture at the final step of Petitioner’s Stone-Hoyos-Varghese transaction model. *Finally*, Petitioner has failed to show that Stone discloses a memory coupled to a single processor that performs all the limitations required by claim 1, as the law requires.

For these reasons, the Board should uphold the patentability of '886 Patent's Challenged Claims.

II. GROUND 1: STONE COMBINED WITH HOYOS AND VARGHESE DOES NOT RENDER THE CHALLENGED CLAIMS OBVIOUS.

A. Stone-Hoyos-Varghese does not render obvious the challenged independent claims.

1. A POSITA would not have been motivated to combine Stone, Hoyos, and Varghese.

The Petition fails to identify a sufficient justification for why a POSITA would have been motivated to combine Stone, Hoyos, and Varghese. POR, 15-30; Ex. 2032 ¶¶ 54-77. Petitioner's reply arguments fare no better.

First, PO has not failed to rebut the Petition's reasons to combine Stone, Hoyos, and Varghese as Petitioner suggests. Pet. Reply, 2. The Petition's only stated reason for combining Stone with Hoyos is that "it was well-known that financial transactions of Stone had a need for authentication including fraud detection (e.g., with higher levels of security for some transactions)." Pet., 16. So in view of Stone's need to implement authentication with fraud detection, "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.* 16-17.

But as the POR explains, Petitioner’s justification for combining Stone and Hoyos is conclusory. POR, 15-18; Ex. 2032 ¶¶ 56-61. Petitioner overgeneralizes and presupposes the problem of electronic fraud and assumes a POSITA would apply a specific class of fraud detection techniques (aliveness detection) without explaining why a POSITA would apply these techniques over others. POR, 15-18. For one, Petitioner has provided no evidence “that financial *transactions of Stone* had a need for authentication including fraud detection.” Pet., 16 (emphasis added). Stone itself does not identify payment fraud as a problem that needs addressing. POR, 16-18, Ex. 2032 ¶¶ 57-59. The sources Petitioner cites identify a need for higher security authentication in high-risk banking and financial institution transactions over certain dollar amounts. *See* Pet., 16, citing Ex. 1010 (noting banks and financial institutions may want higher security authentication for transactions over a certain amount); Ex. 1016 (patent application assigned to Bank of America noting that “necessary authentication level is determined based on the transaction criteria based on factors such as value and type of transaction, as well as other factors”). Conversely, Stone is assigned to eBay and its figures depict PayPal transfers. Neither PayPal nor eBay is a bank or financial institution, and the example transaction in Stone is for a low-dollar amount. *See* Ex. 1008, Figure 2 (transfer for \$26.32). So Petitioner’s claim that it was “well-known” that the specific transactions of Stone—lower-dollar,

non-bank transactions—required fraud detection is not supported by record evidence.

But even if a POSITA believed Stone required additional authentication, Petitioner has given no reason why a POSITA would have implemented the specific techniques disclosed in Hoyos. Hoyos addresses the narrow problem of spoofing in biometric systems with a pointed solution: determining a user is a living person and not a printed photo or other inanimate object, for example. *See* Ex. 1013, [0011]-[0014], cl.1. Stone, for its part, never mentions fraud as a problem and never discusses any techniques for countering fraud, much less specific ways to counter spoofing attempts on biometric systems. Simply put, for a POSITA starting with Stone’s disclosure of a virtual currency display, the obvious question would not be how to improve fraud detection for Stone’s currency display, much less that Hoyos’ anti-spoofing techniques were an obvious solution. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 424-25 (2007).

Second, Stone is not analogous art to the ’886 Patent because it is not directed to improved techniques to prevent and detect fraud within electronic transactions. POR, 18-22. Petitioner’s proposed field of endeavor “electronic financial transactions,” Pet. 12-13, is too broad, such that it would be beyond what a POSITA would reasonably be expected to look for to find a solution to the problem facing the inventor, i.e., fraud detection. *See* POR, 19-22.

Third, Stone and Hoyos teach away from each other such that a POSITA would not have thought to combine their teachings because they require incompatible computing environments. POR, 22-30; Ex. 2032 ¶¶ 66-77. The currency display of Stone requires a server structure. POR, 23; Ex. 2032 ¶ 67. In Stone, the payment server stores all user account information needed to process a money transfer. POR, 23-24; Ex. 2032 ¶¶ 67-69. Petitioner does not dispute this. Hoyos, on the other hand, discloses implementation of biometric authentication techniques on a client device and never discusses implementing its techniques on a server. *Id.*

A POSITA starting with Stone would understand a server structure is required and would not consider implementing local (client-side) fraud detection techniques like those disclosed in Hoyos. POR, 24-25; Ex. 2032 ¶¶ 57-69. For one, local authentication would be redundant. *Id.* All user account information for processing transactions is stored on the payment server. Ex. 1008, [0045]-[0046]. Storing the same user account information on the user device would be a waste of device storage—antithetical to using a remote server. *Id.* Besides, local authentication can be problematic given variance among user devices in security, processing power, camera resolution, and biometric capabilities. *See* Ex. 1013, [0007]-[0009]. Running computationally intensive biometric analysis locally could lead to performance bottlenecks, especially on older or lower-end devices. *See, e.g.,* Ex. 1038, 64

(Systems using client-side matching “are not secure if the client device is not trusted; therefore additional cryptographic support is needed.”). Additionally, the more places sensitive information is stored, the more this sensitive information is exposed to breaches or loss. POR, 26; Ex. 2032 ¶¶ 70-72. So replicating verifications of the user on both client and server (the product of implementing Hoyos’ local authentication over Stone’s server structure) would actually decrease security in Petitioner’s proposed system, and increase the risk of identity theft and fraud. *Id.*

Nor would a POSITA implement Hoyos’ techniques over a remote server. POR, 25-26; Ex. 2032 ¶¶ 69-72. Hoyos does not disclose any remote server applications. It discloses its techniques are performed locally on a computer, connected to a camera. *See, e.g.,* Ex. 1013, [0018]-[0020], cls. 5-7, 13, 17-18. Employing Hoyos’ techniques over a remote server would also undermine the benefits of local authentication that Petitioner associates with Hoyos. *See* Ex. 1003 ¶ 70. For instance, it would increase latency by requiring communication with a server and decrease privacy and security of user information by requiring transfer of sensitive data over a network. *See* POR 25-26; Ex. 2032 ¶¶ 70-72. The additional transfer of sensitive data over the network would also greatly increase the security risk that the system and user’s biometric information could be comprised, which is contrary to the goals of Hoyos and the benefits of local authentication cited by Petitioner’s expert. Ex. 1013, [0015]; Ex. 1003 ¶ 73 (citing benefits of local-only

authentication as including, among other things, “enhanced privacy (by reducing the amount of data that needs to be transmitted to the server and minimizing potential privacy concerns)” and “improved security (where a malicious actor intends to compromise the user device system)”).

Ultimately, a POSITA starting with Stone’s currency display would not have implemented local authentication within Stone’s server structure and would not have applied Hoyos’ local authentication techniques using a remote server. *See id.*

A POSITA would not have been motivated to combine Varghese with Stone and Hoyos for largely the same reasons a POSITA would not have combined Stone and Hoyos. POR, 27-30, Ex. 2032 ¶¶ 73-77. Varghese, like Stone, requires a server structure for its location capture. *See* POR 27-30; Ex. 2032 ¶ 73. For the reasons stated above, a POSITA would not implement Hoyos’ localized biometric authentication in Stone’s server structure and would not have implemented Hoyos’ techniques using a remote server.

Petitioner’s reference to Dr. Goodrich’s writings recognizing the two broad approaches to authentication (client-side and server-side) is a red herring. Pet. Reply, 6-7. Dr. Goodrich has never disputed that authentication can be done either locally on a device or via a remote server. Rather, he explained in his declaration the reasons why a POSITA would have found these approaches *incompatible with Petitioner’s reference combinations*. Ex. 2032 ¶¶ 73-77.

PO and Dr. Goodrich's reference to Varghese's goal of providing a "purely software-based solution to identify theft that does not require hardware devices to be issued and maintained" merely emphasizes that Varghese is not concerned with implementing client-side authentication. POR, 27-30; Ex. 2032 ¶¶ 75-77. In criticizing PO's position, Petitioner provides no citation from Varghese referring to client-side authentication. Pet. Reply, 7-10.

Finally, Petitioner contends that PO's argument "incorrectly characterizes Varghese's 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." Pet. Reply, 8-9. According to Petitioner, Varghese, as shown in Table 10 and explained in [0109], "explicitly describes capturing real-time contextual information including capturing real-time physical location information in 'post-authentication.'" *Id.* Petitioner contends that Table 10 of Varghese further "further illustrates business policies using real-time location data for the authentication for completing the electronic transaction." *Id.* 9-10.

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

But Petitioner does not cite, and Varghese does not disclose, specific evidence that location information is actually collected *during* post-authentication (i.e., in-transaction). Pet., 21-23. For example, Table 10’s rule restricting a “money transfer request of a certain dollar amount by a user who is logged in from another country” also suggests that these rules apply location data that was already collected at login, not when a transaction was confirmed.

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

Paragraph 103 and Table 6A of Varghese, like paragraph 109 and Table 10 cited by Petitioner, are both associated with Figure 15.B's security policies. *See* Ex. 1010, [102]-[114]. Both discuss the use of location information within security policies and both address location associated with *user login*, indicating the login is the relevant collection point for location data, not transaction confirmation step as Petitioner's Stone-Hoyos-Varghese model suggests. Petitioner's reply ignores these sections of Varghese.

[0103] The security policy contains models involving decisions based on risk patterns associated with user, device and location information. The security models are based on known risk conditions and potentially risky behavior and are categorized into the following models. Tables 6A and 6B present illustrative security models.

TABLE 6A	
Restricted model	
Location based rules	Logins from restricted countries, (e.g. OFAC countries) Logins from restricted IP addresses Logins from restricted anonymizers and proxies
User based rules	Logins from restricted users list Multiple consecutive failures for the user
Device based rules	Logins from restricted devices Multiple consecutive failures from the device Device using stolen cookies User using the device for the first time

TABLE 6B

Hacker model	
Location based rules	User login from different geographical location (city, state or country) within a given time period Multiple logins from a given IP address within a given time period
User based rules	User login from different geographical location (city, state or country) within a given time period
Device based rules	User login from different device within a given time period Multiple failures from a given device within a given time period Multiple logins from a given device within a given time period Same device used from different geographical location within a given time period

Ex. 1010 at [0103], Tables 6A & 6B.

Varghese's collection of location data at user login and not at the step where a user confirms a transaction (as Petitioner's Stone-Hoyos-Varghese transaction model requires) undermines Petitioner's alleged motivation to combine these references in the manner Petitioner describes. POR, 27-30; Ex. 2032 ¶¶ 73-77.

2. Stone-Hoyos-Varghese does not render obvious “wherein the virtual likeness of the face was selected by the account holder as part of an enrollment” as recited in limitation [1.2.2].¹

Claim 1 of the '886 Patent claims “one or more processors configured to: render, in one or more interfaces, a virtual likeness of a face associated with an account holder, wherein the virtual likeness of the face was selected by the account holder as part of an enrollment.” Ex. 1001 at cl. 1. Based on this claim structure, *the* virtual likeness rendered in the interface and selected during enrollment must be the *same* virtual likeness. *See NTP, Inc. v. Research in Motion, Ltd.*, 418 F.3d 1282, 1306 (Fed. Cir. 2005) (noting use of “a” followed by use of “the” indicates reference to the same “destination processor”). The Petition does not identify, and Stone does not disclose, a virtual likeness of a face of an account holder that is both rendered in an interface and selected as part of an enrollment process. For the likeness rendered in the interface, Petitioner points to the personalized currency display on the sender’s device (below left) and the recipient photo 202 (below right).

¹ Limitation [1.2.2] is substantially similar to limitations [6.1.2] and [11.1.2]. Patent Owner’s arguments with respect to limitation [1.2.2] thus equally apply to limitations [6.1.2] and [11.1.2].

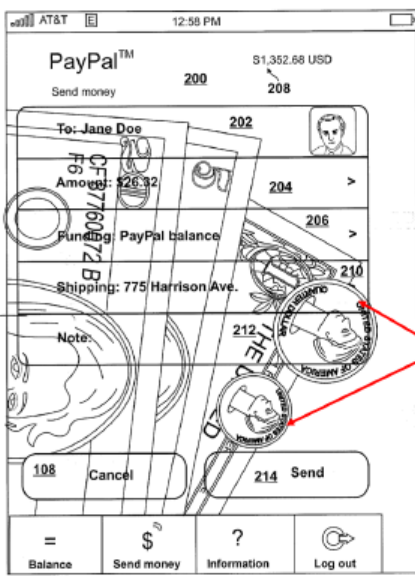


FIG. 2

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

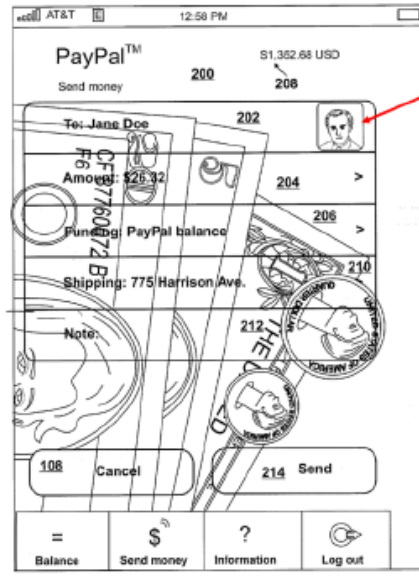


FIG. 2

APPL-1008, FIG. 2, annotated

Pet., 28-29.

Then, for the virtual likeness selected as part of the enrollment [1.2.2],
Petitioner points to user identifier 418, which may include a photo of the user. *See*
Ex. 1008, [0045].

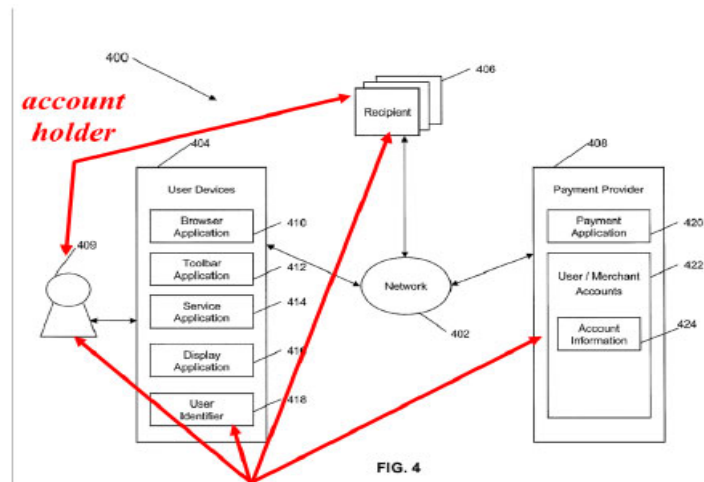


FIG. 4

enrollment

APPL-1008, FIG. 4, annotated

Pet. 30

But Petitioner does not allege, and does Stone disclose, that user identifier 418 is displayed in Stone's interface. *See* Ex. 1008, [0040]-[0048]. Nor does Stone disclose that the personalized currency or recipient photo 202 are the same photo as user identifier 418. In fact, Stone provides no link between user identifier 418, which Petitioner cites as the virtual likeness selected as part of enrollment, and any user likeness displayed in the interface. *See id.*

Petitioner understands there is no connection between what it cites in the Petition as disclosing the likeness rendered in the interface and likeness selected during enrollment. To address this problem, Petitioner states in its reply that the recipient image displayed in the interface is selected as part of the recipient establishing an account and that 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.’” Pet. Reply at 12-13. But Stone does not disclose an enrollment process, much less suggest that the recipient photo 202 would be selected as part of enrollment. Petitioner's support for the recipient photo 202 being selected during enrollment comes from a non-asserted reference and should be disregarded. *Id.* (citing Ex. 1009 – Chatterjee).

Petitioner also tries (and fails) to bridge the divide between user identifier 418 and the personalized currency image. Pet. Reply, 13-15. Petitioner now asserts it

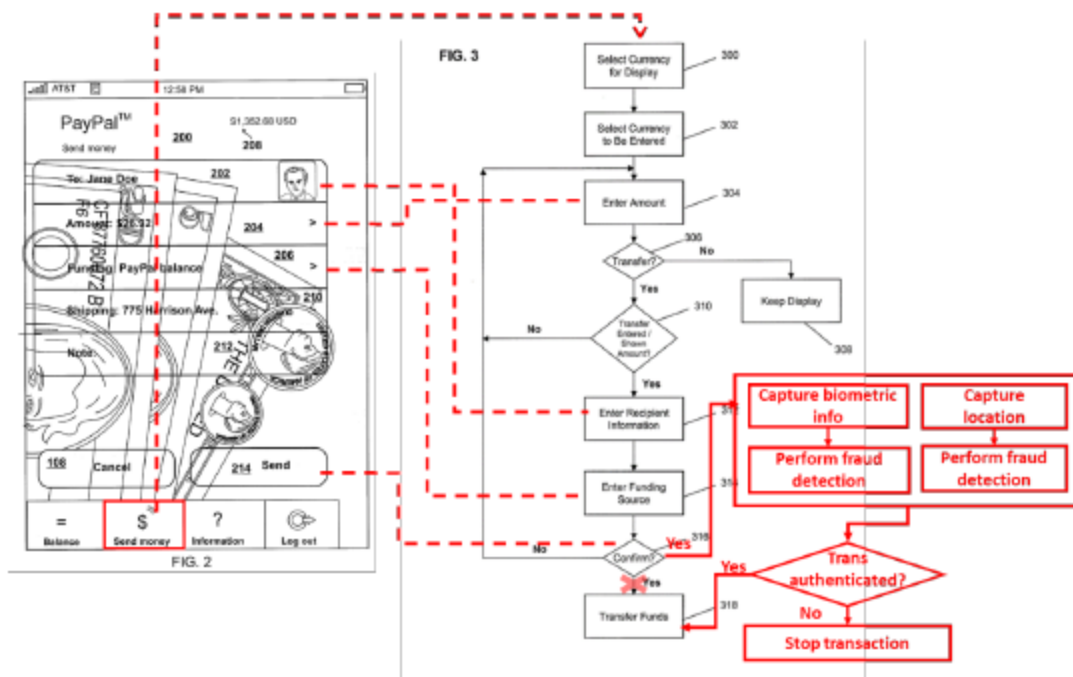
would have been obvious to use the user identifier 418 as the image of the user for the personalized currency display. *Id.* 14-15. But Stone does not teach this or anything to suggest a relationship between user identifier 418 and the personalized currency. Suggesting that the two images can be interchangeable is Petitioner grasping at straws to show obviousness by backfilling the deficiencies of Stone and its own Petition. This is classic hindsight bias, which the Board should reject.

3. Stone-Hoyos-Varghese does not render obvious limitation [1.3.1].²

As the POR explains, a POSITA would not have been motivated to implement Varghese's location capture at the final step of Petitioner's Stone-Hoyos-Varghese transaction model because Varghese teaches that the user device's geolocation would have already been collected at login. POR, 33-36; Ex. 2032 ¶¶ 84-87. 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." Petitioner asserts that the capture of location

² Limitation [1.3.1] is substantially similar to limitations [6.2.1] and [11.2.1]. Patent Owner's arguments with respect to limitation [1.3.1] thus equally apply to limitations [6.2.1] and [11.2.1].

information in its purported Stone-Hoyos-Varghese transaction model would occur after a user presses the send button (214) to complete the confirmation step (316). Pet., 38-39. But Varghese teaches that geolocation information, such as IP address, is collected during the pre-authentication phase (user logins) and not post-authentication (money transfers). POR at 36; Ex. 1010 at [0065], [0074], [0090-93], [0096], [0099].



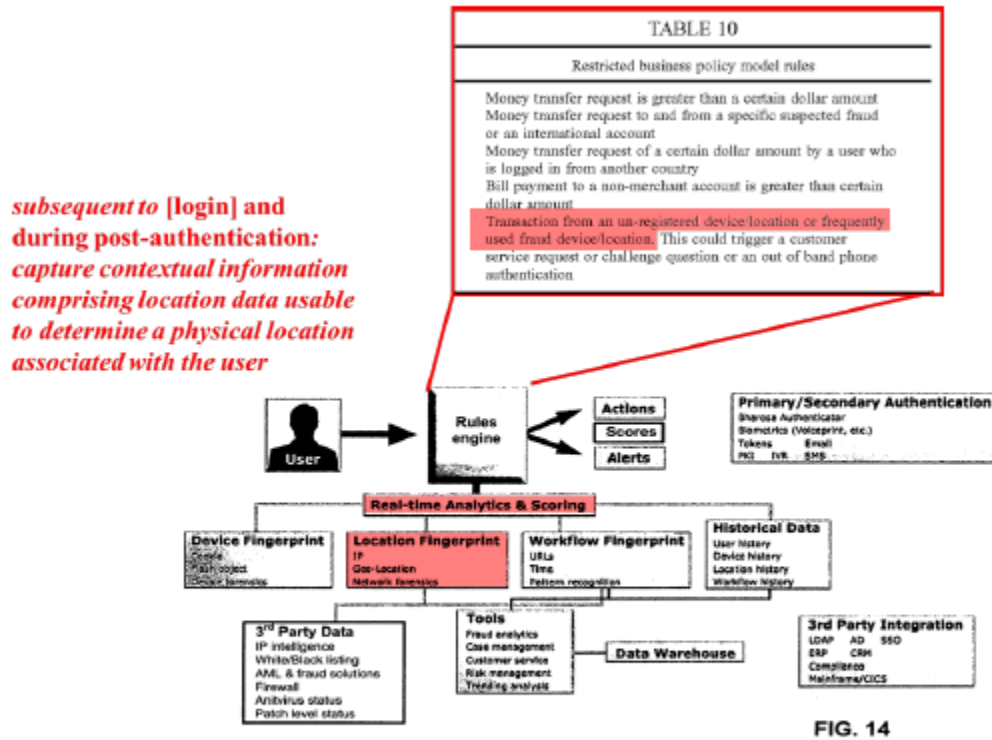
**Example of Stone-Hoyos-Varghese
(annotated based on APPL-1008, FIGS. 2 and 3)**

Pet., 38.

Petitioner contends that PO’s argument here “mischaracterizes Varghese as only collecting location data during the pre-authentication phase (e.g., user login)” and ignores Varghese’s “real-time analytics” capturing location information during

post-authentication “in-session transactions,” for example, a banking application applying the security rule “don’t allow (or challenge user for) money transfer request from an international IP address.” Pet. Reply at 17 (citing Ex. 1010, [0109]). But Varghese does not teach that the application of a security rule during a transaction requires collection of location data at *that* moment in time. In fact, Varghese teaches the opposite. Understanding Varghese’s delineation of pre- and post-authentication, by the time a user would attempt to complete a money transaction, location information (e.g., device IP address) has *already collected during the user’s login* (pre-authentication). See Ex. 1010, [0103], Tables 6A & 6B. The security rule applied during a transaction would then just use the location data that had *already been collected* at the time of the user’s login.

Petitioner points to Figure 14 together with Table 10 and [0109] from Varghese as supposedly showing the disclosure of the post-authentication (in-transaction) location capture.



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

Pet. Reply, 17.

But there are several problems with Petitioner’s diagram. First, Table 10 does not coincide with Figure 14 (preferred function configuration). It is associated with Figure 15.B (exemplary policy set and security model). *See* Ex. 1010, [0102]-[0111]. Table 10’s rule restricting a “money transfer request of a certain dollar amount by a user who is logged in from another country” also suggests that this rule and Varghese’s other security rules apply location data that was already collected at login, not location data collected when a transaction was confirmed, as Petitioner’s transaction model requires, *see* Pet., 38.

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

Paragraph 103 and Table 6A of Varghese, like paragraph 109 and Table 10 cited by Petitioner, are both associated with Figure 15.B's security policies. *See* Ex. 1010, [102]-[114]. Both discuss the use of location information within security policies and both address location associated with *user login*, indicating the login is the relevant collection point for location data, not the transaction confirmation step as Petitioner's Stone-Hoyos-Varghese model mandates. Petitioner's reply ignores these sections of Varghese. For this reason and those already discussed, Petitioner's Ground 1 fails to establish that the '656 Patent's Challenged Claims would have been obvious.

[0103] The security policy contains models involving decisions based on risk patterns associated with user, device and location information. The security models are based on known risk conditions and potentially risky behavior and are categorized into the following models. Tables 6A and 6B present illustrative security models.

TABLE 6A

Restricted model	
Location based rules	Logins from restricted countries, (e.g. OFAC countries) Logins from restricted IP addresses Logins from restricted anonymizers and proxies
User based rules	Logins from restricted users list Multiple consecutive failures for the user
Device based rules	Logins from restricted devices Multiple consecutive failures from the device Device using stolen cookies User using the device for the first time

TABLE 6B

Hacker model	
Location based rules	User login from different geographical location (city, state or country) within a given time period Multiple logins from a given IP address within a given time period
User based rules	User login from different geographical location (city, state or country) within a given time period
Device based rules	User login from different device within a given time period Multiple failures from a given device within a given time period Multiple logins from a given device within a given time period Same device used from different geographical location within a given time period

Ex. 1010 at [0103], Tables 6A & 6B.

4. Stone-Hoyos-Varghese does not render obvious limitation [1.5]: “a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.”

Stone-Hoyos-Varghese does not disclose “a memory coupled to the processor” as required by the ’886 Patent’s independent claims. POR at 14.

First, Petitioner’s client-side model fails because it is predicated on Stone’s processor on the user device 404 being configured to perform all the functionality of the ’886 Patent’s claim 1. But as just explained, the processor on user device 404 does not disclose all the limitations of the ’886 Patent’s claim 1, so it cannot be “*the* one or more processors” coupled to “a memory” for limitation [1.5]. *See* Section II.A.2.-3.

For the purported server-side implementation of Stone-Hoyos, a POSITA would not have been motivated to implement the biometric authentication techniques of Hoyos within a remote setup as explained above in Section II.A.1 (lack of motivation to combine Stone-Hoyos-Varghese). Petitioner also cannot point to multiple processors as disclosing all the limitations the one or more processors must be configured to perform. *See Salazar*, 64 F.4th at 1317.

Petitioner has also not identified for [1.5] a memory “coupled to” and “configured to provide the one or more processors with instructions.” Pet., 53-54. Petitioner alleges that memory 506 of the user device 404 discloses “a memory” that

is “coupled to a processor 504 in each device of the system including e.g., user devices 404, and the memory is configured to provide the processor with instructions (e.g., ‘instructions to create and display the proper currencies, convert currency, display various types of graphics showing transfer of currency, etc.’).” Pet., 54

But memory 506 fails to disclose the “memory” of the ’886 Patent’s claim 1 because it does not provide instructions to the claimed “one or more processors.” First, memory 506 only provides instructions to the processor 504 on the user device. A POSITA reading claim 1 of the ’886 Patent would understand the plain meaning of “provide the one or more processors with instructions” to include at least the instructions to perform the limitations of claim 1 (e.g., receive, associate in a data store, and render in an interface the virtual likeness of the face of the account holder). *See* Ex. 1050, Goodrich Tr. 59:3-59:8. Stone does not disclose that memory 506 on the user device provides any instructions to the payment provider server 408 where the association step [1.2.1] occurs in Petitioner’s server-side model, for example. *See* Pet., 26-29. In Petitioner’s client-side model, memory 506 does not provide the necessary instructions to perform the ’886 Patent’s claim 1 limitations because processor 504 on the user device does not perform these limitations. As a result, Petitioner’s Ground 1 fails to disclose or render obvious limitation [1.5].

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

Stone-Hoyos-Varghese does not render obvious any of the dependent Challenged Claims 2, 4-5, 7, 9-10, 12, 14-18, and 20-23 for the same reasons Stone-Hoyos-Varghese does not render obvious the independent claims. POR, 36-37. Stone-Hoyos-Varghese also does not disclose the dependent limitations of claims 3 and 8 (“wherein the icon represents a form of payment”).

Petitioner contends that PO has not rebutted that a POSITA would have been motivated to implement a graphical representation of payment form as the transaction icon. Pet. Reply, 18-20. But Petitioner has given no explanation *why* a POSITA would have implemented a transaction icon that includes a graphical representation of payment form. Petitioner has the burden to establish a motivation to combine and has failed to offer one. *Intelligent Bio-Sys., Inc. v. Illumina Cambridge, Ltd.*, 821 F.3d 1359, 1367-68 (Fed. Cir. 2016) (“It [i]s [petitioner’s] burden to demonstrate both ‘that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.’” (internal quotations and citations omitted)). Petitioner has thus failed to establish the obviousness of claims 3 and 8.

III. GROUND 2: STONE COMBINED WITH THE FFIEC GUIDANCE DOES NOT RENDER THE CHALLENGED CLAIMS OBVIOUS.

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

A POSITA, as defined in the Board’s Institution Decision, also would not have been motivated to combine Stone with the FFIEC Guidance when developing new methods for detecting fraud in electronic transactions. POR, 40-43; Ex. 2032 ¶¶ 95-101.

First, Petitioner’s claim that the record illustrates a POSITA’s interest in the Guidance are unavailing. Pet. Reply, 20-21. For starters, the FFIEC’s regulatory authority is limited to banks and financial institutions. Ex. 1037, 1. For the ’886 Patent, a POSITA as defined in the Board’s Institution Decision has no credentials or affiliation with the banking industry. *See* Paper [10], 11-12. Further, Stone, Petitioner’s primary reference, is assigned to eBay, which is not a bank or financial institution subject to the FFIEC’s authority. The three patent disclosures Petitioner cites as referencing the Guidance are also all assigned to financial institutions or expressly reference compliance requirements of financial institutions. *See* Pet. Reply, 21; Ex. 1003, ¶ 52. And Petitioner’s expert’s personal knowledge of and testimony about the Guidance’s “significance” is based on his work in standard setting organizations, which is far beyond a POSITA’s limited work experience (bachelor’s degree and two years’ experience in development of biometric

authentication techniques). Ex. 1049, 55:4-55:12 (“[T]hose of us in the standardization community paid great attention to it [FFIEC Guidance], so I've been familiar with it since.”).

Petitioner’s suggestion that PO’s arguments are contrary to Dr. Goodrich’s own practices is also false. Pet. Reply, 21-23. Dr. Goodrich’s patent application, WO 2008/020991, was developed specifically in response to EU privacy regulations. Ex. 1052 at [0011]. The ’886 Patent does not refer to any regulations, nor does it limit itself to the banking industry. *See generally* Ex. 1001. The ’886 Patent is focused solely on addressing technical problems with technical solutions. *Id.*

Dr. Goodrich’s class notes Petitioner cites are also irrelevant. Pet. Reply, 22. These notes pertain to copyright law, not patent law, and give an overview of basic copyright principles. Ex. 1051, 2-9. These class notes are not related to biometric authentication and reference no regulatory guidance. Finally, the chapter on Digital Rights Management in Dr. Goodrich’s textbook *Introduction to Computer Security* is eight pages and includes a single-page section on “Legal Issues” pertaining to copyrights that does not discuss regulatory guidance and bears no relevance to a POSITA’s knowledge or interest in regulatory guidance in relation to methods and techniques for fraud reduction in electronic transactions using biometrics. *See* Ex. 1054, 10.

B. Stone combined with the Guidance does not render any of the challenged claims obvious.

Petitioner's Ground 2 relies on the same elements of Stone it relied on in Ground 1 as disclosing limitations [1.2.2] and [1.3.1] and thus fails for the same reasons as Ground 1 above.

IV. 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.

Because claims 15-17 and 21-23 depend from the independent claims, Grounds 3 and 4 do not render these dependent claims obvious for the same reasons Grounds 1 and 2 do not render the independent claims obvious. POR, 44; Ex. 2032 ¶ 102.

V. CONCLUSION

For the reasons provided above, Patent Owner respectfully requests that the Board find all claims of the '886 Patent valid.

Dated: February 27, 2025

Respectfully submitted,

/s/Richard A. Kamprath
Richard A. Kamprath
Reg. No. 65,320
rkamprath@mckoolsmith.com
Bradley Jarrett (*pro hac vice*)
bjarrett@mckoolsmith.com
McKool Smith, P.C.
300 Crescent Court, Suite 1500
Dallas, Texas 75201
Telephone: (214) 978-4000
Facsimile: (214) 978-4044

George Fishback
Reg. No. 76,345
gfishback@mckoolsmith.com
McKool Smith, P.C.
303 Colorado Street, Suite 2100
Austin, Texas 78701
Telephone: (512) 692-8700
Facsimile: (512) 692-8744

*Counsel for Patent Owner, Carbyne
Biometrics, LLC*

CERTIFICATION OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned **PATENT OWNER'S SUR-REPLY TO PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE** specified in 37 C.F.R. §42.24 have 4,293 words, in compliance with the 5,600 word limit set forth in 37 C.F.R. §42.24(c)(4). This word count was prepared using Microsoft Word 2010.

Dated: February 27, 2025

Respectfully submitted,

/s/Richard A. Kamprath
Richard A. Kamprath
Reg. No. 65,320

CERTIFICATION OF SERVICE

The undersigned hereby certifies that a copy of this **PATENT OWNER'S SUR-REPLY TO PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE PURSUANT TO 37 C.F.R. § 42.10(b)** has been served on Petitioner via email on the following counsel of record for Petitioner:

David W. O'Brien
David.obrien.ipr@haynesboone.com

Kelly Gehrke Lyle
Kelly.lyle@haynesboone.com

Hong Shi
Hong.shi.ipr@haynesboone.com

Dated: February 27, 2025

Respectfully submitted,

/s/Richard A. Kamprath
Richard A. Kamprath
Reg. No. 65,320