

**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

---

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

**TABLE OF CONTENTS**

|                                                                                                                                                                                                                                                                                                                       |           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>I. INTRODUCTION.....</b>                                                                                                                                                                                                                                                                                           | <b>1</b>  |
| <b>II. GROUND 1: THE COMBINATION OF STONE, HOYOS, AND VARGHESE DOES NOT RENDER THE CHALLENGED CLAIMS OBVIOUS.....</b>                                                                                                                                                                                                 | <b>2</b>  |
| A. STONE COMBINED WITH HOYOS AND VARGHESE DOES NOT RENDER OBVIOUS THE CHALLENGED INDEPENDENT CLAIMS. ....                                                                                                                                                                                                             | 2         |
| 1. Petitioner fails to establish that a POSITA would have combined Stone, Hoyos, and Varghese and would have had a reasonable expectation of success in doing so.....                                                                                                                                                 | 2         |
| 2. Stone-Hoyos-Varghese does not disclose or render obvious “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” as recited in limitation [1.2]. .... | 11        |
| 3. Stone-Hoyos-Varghese does not disclose or render obvious “a memory coupled to the processor and configured to provide the processor with instructions” as recited in limitation [1.9]. ....                                                                                                                        | 15        |
| B. STONE-HOYOS-VARGHESE DOES NOT RENDER OBVIOUS THE CHALLENGED DEPENDENT CLAIMS.....                                                                                                                                                                                                                                  | 17        |
| 1. Stone-Hoyos-Varghese does not disclose or render obvious “wherein the transaction icon includes a graphical representation of payment form” in claims 5 and 14. ....                                                                                                                                               | 17        |
| 2. Stone-Hoyos-Varghese does not disclose or render obvious “wherein the virtual likeness comprises an avatar selected by the account holder” in claims 8 and 17. ....                                                                                                                                                | 18        |
| <b>III. GROUND 2: STONE COMBINED WITH THE FFIEC GUIDANCE DOES NOT RENDERS THE CHALLENGED CLAIMS OBVIOUS .....</b>                                                                                                                                                                                                     | <b>18</b> |
| A. A POSITA WOULD NOT HAVE BEEN MOTIVATED TO COMBINE STONE WITH THE FFIEC GUIDANCE. ....                                                                                                                                                                                                                              | 18        |
| B. STONE COMBINED WITH THE GUIDANCE DOES NOT RENDER ANY OF THE CHALLENGED CLAIMS OBVIOUS. ....                                                                                                                                                                                                                        | 20        |
| <b>IV. GROUNDS 3 AND 4: THE COMBINATION OF STONE, HOYOS, VARGHESE, AND BOROVSKY (GROUND 3) AND COMBINATION OF</b>                                                                                                                                                                                                     |           |

|                                                                                                                |           |
|----------------------------------------------------------------------------------------------------------------|-----------|
| <b>STONE, THE FFIEC GUIDANCE, AND BOROVSKY (GROUND 4) DO<br/>NOT RENDER OBVIOUS CLAIMS 2-3 AND 11-12 .....</b> | <b>20</b> |
| <b>V. CONCLUSION.....</b>                                                                                      | <b>21</b> |

**TABLE OF AUTHORITIES**

| <b>Cases</b>                                                                                            | <b>Page(s)</b> |
|---------------------------------------------------------------------------------------------------------|----------------|
| <i>Intelligent Bio–Sys., Inc. v. Illumina Cambridge, Ltd.</i> ,<br>821 F.3d 1359 (Fed. Cir. 2016) ..... | 17             |
| <i>KSR Int’l Co. v. Teleflex Inc.</i> ,<br>550 U.S. 398 (2007) .....                                    | 4              |
| <i>Salazar v. AT&amp;T Mobility LLC</i> ,<br>64 F.4th 1311 (Fed. Cir. 2023) .....                       | 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. 10,713,656 (“the ’656 Patent”). Petitioner has failed to meet its burden to establish that any Challenged Claim of the ’656 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 ’656 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 reference combinations disclose a processor configured to receive, store, and associate an account holder’s biometric information with the account holder’s account as required by the ’656 Patent’s claim 1. *Finally*, Petitioner has failed to show that Stone discloses a memory coupled to a single processor that performs all the limitations required by the ’656 Patent’s claim 1, as the law requires.

For these reasons, the Board should uphold the patentability of ’656 Patent’s Challenged Claims.

**II. GROUND 1: THE COMBINATION OF STONE, HOYOS, AND VARGHESE DOES NOT RENDER THE CHALLENGED CLAIMS OBVIOUS**

**A. Stone combined with Hoyos and Varghese does not render obvious the challenged independent claims.**

**1. Petitioner fails to establish that a POSITA would have combined Stone, Hoyos, and Varghese and would have had a reasonable expectation of success in doing so.**

The Petition fails to identify a sufficient justification for why a POSITA would have been motivated to combine Stone, Hoyos, and Varghese. POR, 16-31; Ex. 2032 ¶¶ 55-78. 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.

But as the POR explains, Petitioner’s justification for combining Stone and Hoyos is conclusory. POR, 16-19; Ex. 2032 ¶¶ 57-62. 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, 16-19. 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, 17-18, Ex. 2032 ¶¶ 58-60. 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 '656 Patent because it is not directed to improved techniques to prevent and detect fraud within electronic transactions. POR, 19-23. Petitioner's proposed field of endeavor "computer network applications for 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, 20-21.

***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, 23-31; Ex. 2032 ¶¶ 67-78. The currency display of Stone requires a server structure. POR, 24; Ex. 2032 ¶ 68. In Stone, the payment server stores all user account information needed to process a money transfer. POR, 24-25; Ex. 2032 ¶¶ 68-69. 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, 31-32; Ex. 2032 ¶¶ 80-81. 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 the 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, 26-27; Ex. 2032 ¶¶ 71-73. 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 ¶ 68. 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 27; Ex. 2032, ¶¶ 71-73. 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 ¶ 68 (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, 27-31, Ex. 2032 ¶¶ 74-78. Varghese, like Stone, requires a server structure for its location capture. *See* POR 27-31; Ex. 2032 ¶ 74. For the reasons explained 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, 6-8. 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 ¶¶ 74-78.

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, 27-31; Ex. 2032 ¶¶ 76-78. In criticizing PO’s position, Petitioner provides no citation from Varghese referring to client-side authentication. Pet. Reply, 8-10.

Finally, Petitioner contends that PO’s argument “mischaracterize[s] 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, 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.* 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., 24-26. 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)<br>Logins from restricted IP addresses<br>Logins from restricted anonymizers and proxies           |
| User based rules     | Logins from restricted users list<br>Multiple consecutive failures for the user                                                                            |
| Device based rules   | Logins from restricted devices<br>Multiple consecutive failures from the device<br>Device using stolen cookies<br>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<br>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<br>Multiple failures from a given device within a given time period<br>Multiple logins from a given device within a given time period<br>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

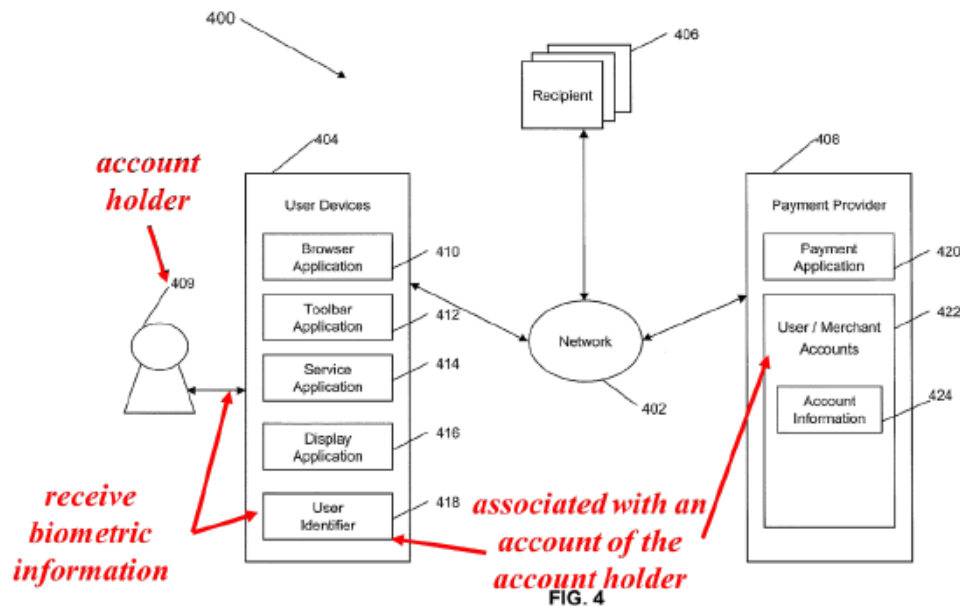
model requires) undermines Petitioner’s alleged motivation to combine these references in the manner Petitioner describes. POR, 27-31; Ex. 2032 ¶¶ 74-78.

2. **Stone-Hoyos-Varghese does not disclose or render obvious “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” as recited in limitation [1.2].<sup>1</sup>**

Stone does not disclose any association between user identifier 418 (what Petitioner identifies as the user biometric) and user account 422 (account of an account holder) that occurs on the user device 404. The only association of user identifier 418 with an account occurs on the payment provider server 408, where all user account information is stored. Ex. 1008 at [0045]-[0046]. In the Petition, Petitioner appears to identify the payment provider server 408 as “associating” the user identifier with user account 422.

---

<sup>1</sup> Limitation [1.2] is substantially similar to limitations [10.1] and [19.1]. Patent Owner’s arguments for limitation [1.2] thus equally apply to limitations [10.1] and [19.1]. Because limitations [10.1] and [19.1] are not disclosed or rendered obvious by Petitioner’s prior art references, Petitioner has failed to show that independent claims 1, 10, and 19 are rendered obvious by any of Petitioner’s Grounds.



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

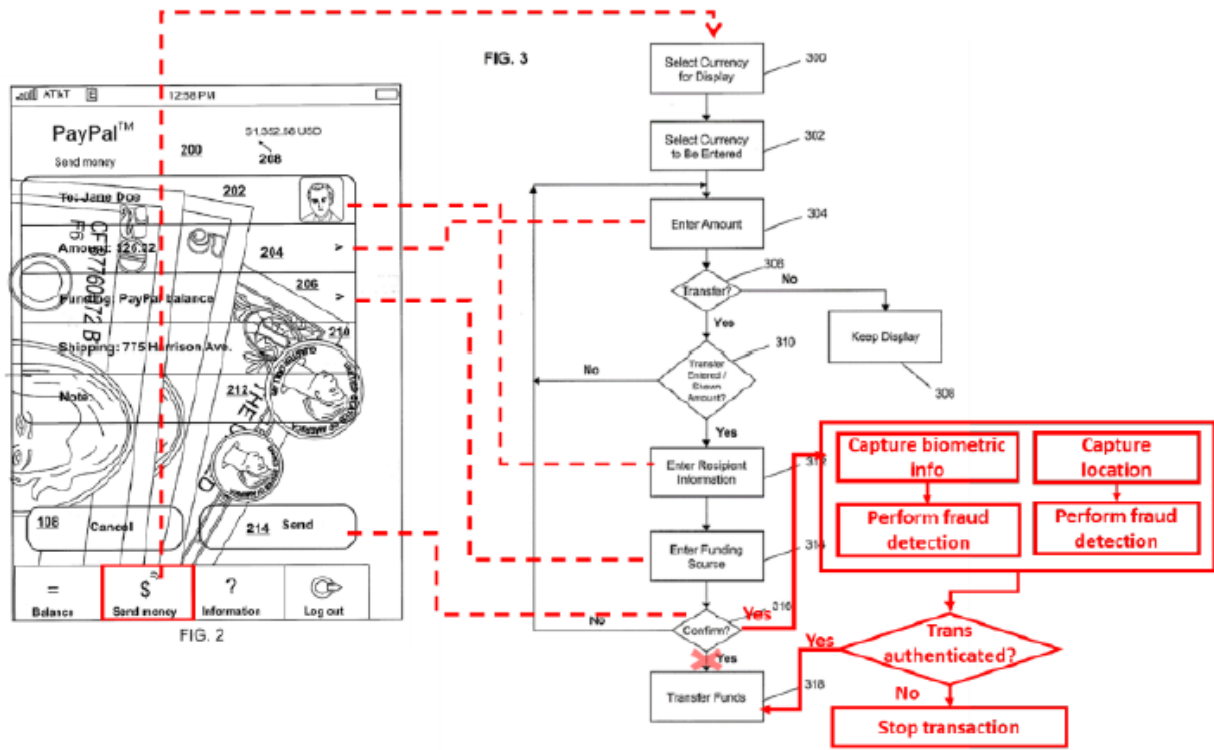
Pet., 33. But association of the user identifier with a user account on the payment provider server cannot disclose [1.2]. The association of the user biometric (user identifier 418) with an account must occur on the *same* processor that receives, stores, and associates the user biometric (user identifier 418) with a user account. *See Salazar v. AT&T Mobility LLC*, 64 F.4th 1311, 1317 (Fed. Cir. 2023) (holding that a claim to “a microprocessor” (meaning “one or more microprocessors”) “require[s] that at least one microprocessor be capable of performing each of the claimed functions.”).

Petitioner in its reply, concedes that Stone does not disclose the association required for [1.2] as occurring on user device 404. Instead, Petitioner now states that “POSITA would have been motivated to implement in the system of Stone *combined*

*with Hoyos and Varghese client-side biometric authentication*, in which the reference biometric information received during enrollment is associated with the user account in the biometric storage.” Pet. Reply, 12. But as already explained, a POSITA would not have been motivated to implement local authentication as taught by Hoyos on Stone’s server structure, given wide variance among user devices in security requirements, processing power, camera resolution, and biometric capabilities and because running computationally intensive biometric analysis locally could lead to performance bottlenecks, especially on older or lower-end devices. *See* Section II.A.1.

Petitioner is also incorrect to say for local authentication in a system employing Stone-Hoyos-Varghese that the association is not required to occur on the payment server. Pet. Reply, 14. Petitioner’s Stone-Hoyos-Varghese local-authentication model presupposes that account information for associating a user with the user’s account will be stored on the user device and not require communication with the payment server. *Id.* This is contrary to Stone’s teaching that the information for associating a user with their account is stored exclusively on the payment server and the association of the user identifier 418 with an account occurs only when a transaction is submitted to the payment provider server for processing. Ex. 1008, [0045]-[0046]. And Petitioner’s position here is supported only by the conclusory statement of Petitioner’s expert that biometric authentication can be

implemented “either on the server or on the client side” and a string citation to a smattering of Petitioner’s exhibits that support the general idea that biometric authentication, *in the abstract*, can be completed locally on a user device or remotely on a server. Pet. Reply, 15.



### Example of Stone-Hoyos-Varghese

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

Pet. at 23.

Petitioner’s contention that [1.2] would be completed during an enrollment phase is also unavailing. Stone never discloses an enrollment phase. *See, e.g.*, Ex. 1008, Fig. 3 & 4. Stone’s only disclosure of association of the user identifier 418

(biometric id) with a user's account occurs "with a user money transfer request to the payment provider server." *Id.* [0045]. Petitioner's addition of an enrollment step based on "fundamental knowledge" of biometric authentication is conclusory and an attempt to alter the teachings of Stone in hindsight to fit the '656 Patent's claims, and the Board should reject this argument. Pet. Reply, 18-19.

**3. Stone-Hoyos-Varghese does not disclose or render obvious "a memory coupled to the processor and configured to provide the processor with instructions" as recited in limitation [1.9].**

For limitation [1.9], Petitioner contends that the combination of Stone-Hoyos-Varghese implementing Hoyos' authentication locally on the processor of user device 404 discloses "a memory coupled to the processor and configured to provide the processor with instructions." Pet. Reply, 19-20. But Petitioner's client-side implementation of Stone-Hoyos-Varghese fails to disclose this limitation because it is predicated on Stone's processor on user device 404 being configured to perform all the functionality of the '656 Patent's claim 1. But as just explained, the user device processor 404 does not disclose all the limitations of the '656 Patent's claim 1. Specifically, the user device processor *does not associate* the user identifier 418 (biometric) with a user account 422. *See* Section II.A.2. Stone discloses that the association of the user identifier with account information occurs only on payment server 408. Ex. 1008, [0045]. Therefore, the processor on the user device cannot be "*the processor*" coupled to "a memory" for limitation [1.9].

To the extent Petitioner contends that Hoyos discloses the receipt, storage, and association of biometric information with the account of an account holder, this is incorrect. *See* Pet., 33. But Hoyos does not make up for Stone’s shortcomings, specifically its lack of association of biometrics with a specific account. Petitioner does not cite, and Hoyos does not disclose, association of biometric information with a specific account of an account holder. In fact, Hoyos does not mention accounts at all. *See* Ex. 1013. So even relying on Hoyos, Petitioner’s Stone-Hoyos-Varghese combination still fails to disclose or render obvious “*the* processor” coupled to “a memory” for limitation [1.9].

In its reply, Petitioner contends that “PO’s arguments fail because they rely upon the incorrect and unsupported premise that ‘[f]or 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 the analysis of that limitation.” Pet. Reply, 19. Petitioner offers no support for its argument, simply stating that “PO’s premise is incorrect.” *Id.* But, again, as just shown above, neither Stone nor Hoyos discloses any association of biometric information with a user account that occurs on a processor in a user device. Petitioner’s Ground 1 therefore fails to disclose limitation [1.9].

**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 4-9, 13-18 for the same reasons Stone-Hoyos-Varghese does not render obvious the independent claims. POR, 41-42. Stone-Hoyos-Varghese also does not disclose the dependent limitations of claims 5, 8, 14, and 17.

**1. Stone-Hoyos-Varghese does not disclose or render obvious “wherein the transaction icon includes a graphical representation of payment form” in claims 5 and 14.**

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, 22-24. But Petitioner gives 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 5 and 14.

**2. Stone-Hoyos-Varghese does not disclose or render obvious “wherein the virtual likeness comprises an avatar selected by the account holder” in claims 8 and 17.**

Petitioner contends that it would have been obvious to use an avatar for the virtual likeness of claim 1 simply because an avatar is a “well-known alternative of a picture for a user icon.” Pet. Reply at 24. However, Petitioner provides no reason for why a POSITA would have been motivated to replace any of the user images Petitioner relies on from Stone (recipient photo 202, personalized currency, user identifier 418) as disclosing the “virtual likeness” of the ’656 Patent’s claims with an avatar.

**III. GROUND 2: STONE COMBINED WITH THE FFIEC GUIDANCE DOES NOT RENDERS 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, 44-47; Ex. 2032 ¶¶ 93-99.

*First*, Petitioner’s claim that the record illustrates a POSITA’s interest in the Guidance is unavailing. Pet. Reply, 25-26. For starters, the FFIEC’s regulatory authority is limited to banks and financial institutions. Ex. 1037, 1. For the ’656 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, 25; Ex. 1003, ¶ 50. 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, 26. Dr. Goodrich's patent application, WO 2008/020991, was developed specifically in response to EU privacy regulations. Ex. 1052 at [0011]. The '656 Patent does not refer to any regulations, nor does it limit itself to the banking industry. *See generally* Ex. 1001. The '656 Patent is focused solely on addressing technical problems with technical solutions. *Id.*

Dr. Goodrich's class notes Petitioner cites are also irrelevant. Pet. Reply, 26-27. 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] and [1.9] and thus fails for the same reasons as Ground 1 above.

**IV. GROUNDS 3 AND 4: THE COMBINATION OF STONE, HOYOS, VARGHESE, AND BOROVSKY (GROUND 3) AND COMBINATION OF STONE, THE FFIEC GUIDANCE, AND BOROVSKY (GROUND 4) DO NOT RENDER OBVIOUS CLAIMS 2-3 AND 11-12**

Petitioner's Grounds 3 and 4 fail to render obvious the dependent claims for the same reasons Grounds 1 and 2 fail to render obvious the independent claims. Further, Petitioner's reply offers no further reason to combine Borovsky's teachings with Stone, Hoyos, and Varghese beyond the conclusory justification offered in the

Petition and thus fails to offer a sufficient motivation to combine as well. *See* POR, 48-50.

## V. CONCLUSION

For the reasons provided above, Patent Owner respectfully requests that the Board find all claims of the '656 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 3,879 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](mailto:David.obrien.ipr@haynesboone.com)

Kelly Gehrke Lyle  
[Kelly.lyle@haynesboone.com](mailto:Kelly.lyle@haynesboone.com)

Hong Shi  
[Hong.shi.ipr@haynesboone.com](mailto:Hong.shi.ipr@haynesboone.com)

Dated: February 27, 2025

Respectfully submitted,

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