

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

CARBYNE BIOMETRICS, LLC,

Patent Owner

IPR2024-00330

U.S. Patent No. 10,713,656

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

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	LEVEL OF ORDINARY SKILL IN THE ART.....	1
III.	GROUND 1: STONE IN COMBINATION WITH HOYOS AND VARGHESE RENDERS OBVIOUS THE CHALLENGED CLAIMS	2
A.	Stone combined with Hoyos and Varghese renders obvious the challenged independent claims.....	2
1.	A POSITA would have been motivated to combine Stone, Hoyos, and Varghese	2
2.	Stone combined with Hoyos and Varghese renders 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 [1.2].....	11
3.	Stone combined with Hoyos and Varghese renders obvious “a memory coupled to the processor and configured to provide the processor with instructions” as recited in [1.9].....	19
B.	Stone combined with Hoyos and Varghese renders obvious the challenged dependent claims.....	21
1.	Stone combined with Hoyos and Varghese renders obvious “wherein the transaction icon includes a graphical representation of payment form” in claims 5 and 14.....	22
2.	Stone combined with Hoyos renders obvious “wherein the virtual likeness comprises an avatar selected by the account holder” in claims 8 and 17.....	24
IV.	GROUND 2: STONE COMBINED WITH FFIEC GUIDANCE (GUIDANCE) RENDERS THE CHALLENGED CLAIMS OBVIOUS.	25
A.	A POSITA would have been motivated to combine Stone and Guidance.....	25
B.	Stone combined with Guidance renders obvious the challenged claims.....	27

V. GROUND 3 AND 4: COMBINATION OF STONE, HOYOS,
 VARGHESE, AND BOROVSKY (GROUND 3) AND COMBINATION
 OF STONE, GUIDANCE, AND BOROVSKY (GROUND 4) RENDER
 OBVIOUS CLAIMS 2-3 AND 11-12. 28

VI. CERTIFICATE OF WORD COUNT 30

CERTIFICATE OF SERVICE 31

PETITIONER'S EXHIBIT LIST

Updated: January 16, 2026

APPL-1001	U.S. Patent No. 10,713,656 to Jakobsson ("656 patent")
APPL-1002	Prosecution File History of U.S. App. No. 15/948744 (issued as '656 patent) ("744 App")
APPL-1003	Declaration of Dr. Creed Jones ("Jones Decl.")
APPL-1004	CV of Dr. Creed Jones
APPL-1005	Prosecution File History of U.S. Prov. App. 61/332,140 ("140 App")
APPL-1006	Prosecution File History of U.S. App. No. 13/099,981 (issued as U.S. Patent No. 8,458,041) ("981 App")
APPL-1007	Prosecution File History of U.S. App. No. 13/875,245 (issued as U.S. Patent No. 9,972,010) ("245 App")
APPL-1008	U.S. Pub. No. 2010/0042535 to Stone ("Stone")
APPL-1009	U.S. Patent No. 8,386,620 to Chatterjee ("Chatterjee")
APPL-1010	U.S. Pub. No. 2006/0282660 to Varghese et al. ("Varghese")
APPL-1011	U.S. Pub. No. 2009/0135188 to Ding et al. ("Ding")
APPL-1012	U.S. Patent No. 8,355,530 to Park et al. ("Park")
APPL-1013	U.S. Pub. No. 2010/0014720 to Hoyos et al. ("Hoyos")
APPL-1014	U.S. Pub. No. 2006/0158307 to Lee et al. ("Lee")
APPL-1015	U.S. Patent No. 8,150,772 to Mardikar et al. ("Mardikar")
APPL-1016	U.S. Pub. No. 2009/0157560 to Carter et al. ("Carter")
APPL-1017	U.S. Patent No. 5,164,992 to Turk et al. ("Turk")
APPL-1018	U.S. Patent No. 7,814,332 to Beenau et al. ("Beenau")
APPL-1019	U.S. Patent No. 10,373,173 to Winner et al. ("Winner")
APPL-1020	U.S. Patent No. 7,856,472 to Arav ("Arav")
APPL-1021	Heusch, et al., "Local Binary Patterns as an Image Preprocessing for Face Authentication," IDIAP Research Institute Report, November 2005 ("Heusch")

APPL-1022	Oracle-Bharosa Acquisition Announcement, 2007, https://www.oracle.com/us/corporate/acquisitions/bharosa/oracle-bharosa-faq-072369.pdf (retrieved January 17, 2024) (“Oracle-Bharosa Acquisition Announcement”)
APPL-1023	U.S. Patent No. 7,779,268 to Draper et al. (“Draper”)
APPL-1024	U.S. Patent No. 5,930,804 to Yu et al. (“Yu”)
APPL-1025	Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (June 21, 2022) (“Director Memo”)
APPL-1026	Preliminary Constructions, Carbyne Biometrics, LLC v. Apple Inc., WDTX-1:23-cv-00324 (December 11, 2023)
APPL-1027	United States District Courts—National Judicial Caseload Profile (September 30, 2023), https://www.uscourts.gov/statistics/table/na/federal-court-management-statistics/2023/09/30 (retrieved Dec. 14, 2023)
APPL-1028	Scheduling Order, Carbyne Biometrics, LLC v. Apple Inc., WDTX-1:23-cv-00324 (July 14, 2023)
APPL-1029	Carbyne Preliminary Infringement Contentions, Carbyne Biometrics, LLC v. Apple Inc., WDTX-1:23-cv-00324 (June 21, 2023)
APPL-1030 - APPL-1032	RESERVED
APPL-1033	J. P. Campbell, “Speaker Recognition: a Tutorial,” in Proceedings of the IEEE, vol. 85, no. 9, pp. 1437-1462, Sept. 1997 (“Campbell”)
APPL-1034	U.S. App. Pub. No. 2009/0288012A1 to Hertel et al. (“Hertel”)
APPL-1035	U.S. Patent No. 8,533,485 to Bansal et al. (“Bansal”)
APPL-1036	U.S. App. Pub. No. 2006/0271460A1 to Hanif (“Hanif”)
APPL-1037	Federal Financial Institutions Examination Council, FFIEC Press Release and FFIEC Guidance - Authentication in an Internet Banking Environment, Oct 12, 2005, https://www.ffiec.gov/pdf/authentication_guidance.pdf (retrieved January 17, 2024), accessible through hyperlinks in

	https://www.ffiec.gov/press/pr101205.htm (APPL-1040) and https://www.fdic.gov/news/inactive-financial-institution-letters/2005/fil10305.html (APPL-1039) ("Guidance")
APPL-1038	Bhargav-Spantzel et al., "Privacy Preserving Multifactor Authentication with Biometrics," DIM'06, November 3, 2006 ("Bhargav-Spantzel")
APPL-1039	FDIC Financial Institution Letter, FFIEC Guidance Authentication in an Internet Banking Environment, FIL-103-2005, October 12, 2005, https://www.fdic.gov/news/inactive-financial-institution-letters/2005/fil10305.html (retrieved January 17, 2024), including hyperlink for APPL-1037 ("FIL-103-2005")
APPL-1040	Federal Financial Institutions Examination Council, FFIEC Guidance Press Release, Oct 12, 2005, https://www.ffiec.gov/press/pr101205.htm (retrieved January 17, 2024), including hyperlink for APPL-1037 ("FFIEC Guidance Press Release")
APPL-1041	U.S. App. Pub. No. 2010/0317335A1 to Borovsky ("Borovsky")
APPL-1042	Ekler et al., "Similarity Management in Phonebook-Centric Social Networks," 2009 Fourth International Conference on Internet and Web Applications and Services, Venice/Mestre, Italy, 2009, pp. 273-279, doi: 10.1109/ICIW.2009.46 ("Ekler")
APPL-1043	U.S. Patent No. 8,954,500 to Marlow et al. ("Marlow")
APPL-1044	Kollreider et al., "Verifying liveness by multiple experts in face biometrics," 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, Anchorage, AK, USA, 2008, pp. 1-6, doi: 10.1109/CVPRW.2008.4563115 ("Kollreider")
APPL-1045	Narayanan et al., "De-anonymizing Social Networks," 2009 30th IEEE Symposium on Security and Privacy, 2009 ("Narayanan")
APPL-1046	U.S. App. Pub. No. US2008/0270038A1 to Partovi et al. ("Partovi")
APPL-1047	Vasalou et al., "Avatars in Social Media: Balancing Accuracy, Playfulness and Embodied Messages," International Journal of Human-Computer Studies Volume 66, Issue 11, November 2008, Pages 801-811 ("Vasalou")

APPL-1048	Sotera Stipulation dated April 17, 2024
(New) APPL-1049	Deposition transcript of Dr. Creed Jones (October 11, 2024)
(New) APPL-1050	Deposition transcript of Dr. Michael Goodrich (January 7, 2025)
(New) 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)
(New) APPL-1052	WO App. Pub. 2008/020991 to Goodrich et al.
(New) APPL-1053	Deposition transcript of Dr. Michael Goodrich (January 8, 2025)
(New) APPL-1054	Goodrich et al., "Introduction to Computer Security" (October 15, 2010)
(New) 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
(New) APPL-1056	Supplemental Declaration of Dr. Creed Jones ("Jones Suppl. Decl.")

I. Introduction

Carbyne Biometrics (“Patent Owner” or “PO”), in its Patent Owner’s Response (“POR”), cannot dispute that the claims are rendered obvious by the prior art. So, to avoid a clear finding of unpatentability, it attempts to distort the teachings of the prior art, misrepresent the Petition’s combinations, and misapply the law. The Board should disregard these arguments and find the challenged claims unpatentable.

II. Level of Ordinary Skill in the Art

In the Institution Decision, the Board adopted Petitioner’s POSITA standard “with the exception of the phrase ‘at least’ which injects potential ambiguity into the level of skill.” ID, 11-12. Petitioner applies the standard as clarified by the Board. The analysis of the Petition remains the same, applying this clarified level of skill for a POSITA. APPL-1056, ¶2 (Dr. Jones explaining that his analysis in the original declaration APPL-1003 remains the same).

III. Ground 1: Stone in Combination with Hoyos and Varghese Renders Obvious the Challenged Claims

A. Stone combined with Hoyos and Varghese renders obvious the challenged independent claims

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

PO states, “Petitioner’s explanation for the alleged motivation to combine is conclusory,” “Stone is not analogous art to the ’656 Patent,” and “Stone and Hoyos teach away from each other.” POR, 15. PO’s arguments are contrary to the record, are incorrect both legally and technically, and should be rejected. APPL-1056, ¶3.

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

PO fails to rebut any of Petition’s reasons to combine Stone, Hoyos, and Varghese, which are fully supported by the evidence. *See* Pet. 16-23 (citing numerous supporting references and Dr. Jones’ testimony). Instead, PO’s arguments mischaracterize the prior art, disregard the Petition’s explanation regarding a POSITA’s understanding of the prior art disclosure, and should be rejected. APPL-1056, ¶4.

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 disregarding how a POSITA would have understood Stone. POR, 16; APPL-1056, ¶5. 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 information/"biometric id" as described in Stone is typically received and stored on user device 404 during an enrollment/registration process, and is also referred as 'enrollment data' used for subsequent comparison with the later captured data to provide an authentication decision" for electronic transactions. Pet. 32; *see* POR, 16-17. As such, PO's assertion that Stone is not concerned with fraud detection for electronic transactions disregards Stone's explicit disclosure as it would have been understood by a POSITA, and thus should be rejected. APPL-1056, ¶5.

PO further 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”); APPL-1056, ¶6; *see* POR 17.

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. APPL-1056, ¶7.

PO’s arguments should also be rejected because they incorrectly characterize 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. As such, and contrary to PO’s arguments, Hoyos itself provides express advantages

that would have motivated a POSITA to incorporate Hoyos' biometric authentication teachings in Stone. APPL-1056, ¶8.

b. Stone is analogous art

PO's arguments that Stone is not analogous art are meritless and should be rejected. APPL-1056, ¶9.

First, as discussed at III.A.1.a above, Stone is analogous art, because Stone explicitly describes its implementation in the context of PayPal, which is in the same field of endeavor of the '010 Patent. *See, e.g.*, 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. APPL-1056, ¶10.

Second, Stone is analogous art because it is 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-1056, ¶11.

Accordingly, Stone is analogous art. APPL-1056, ¶12.

c. PO's teaching away arguments are meritless

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

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.

First, PO's arguments are contrary to the law, because they fail to identify anything in prior art that criticizes, discredits, or otherwise discourages the claimed invention, and should be rejected. *See In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994). APPL-1056, ¶¶13-14.

Second, as explained by the Petition and supported by Dr. Jones' declarations, 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., 20-21; APPL-1003, ¶¶67-68; APPL-1016, [0040], [0042] (describing that fraud detection can "be performed locally or by transmission of []data to a remote source"); [0076]; APPL-1038, 64 ("Biometric authentication can be implemented through systems performing the matching either on the server or on the client side," where describing "security and privacy problems" and CPU-intensiveness of server side implementation, and "relatively

simple and cheap” with security and privacy benefits of client side implementation); APPL-1056, ¶15. 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-1055, 2 (cited as C-101 in Dr. Goodrich’s declaration Ex. 2032, ¶9). APPL-1056, ¶15.

A POSITA would have been aware that biometric authentication in a client-server architecture could be performed on a server or on a remote 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. As such, the authentication methods of Hoyos are applicable in a client-server model, as described in Stone. In a system of Stone modified with Hoyos, a POSITA would have been motivated to implement the biometric authentication on the client for the benefits of improved security and privacy, and “[s]uch an approach is convenient as it is relatively simple and cheap to build biometric authentication systems supporting biometric storage at the client end able to support local matching.” APPL-1038, 64; APPL-

1056, ¶16.

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

First, 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. PO’s arguments fail for the same reasons discussed at III.A.1.c.i, 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., 20-21; APPL-1003, ¶¶67-68; APPL-1056, ¶17.

Second, 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 should be rejected. 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*” refers 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]. Further, some biometric modalities can make use of sensors that are already part of the client system, such as webcams, microphones and fingerprint sensors for local login. As such, PO's arguments should be rejected. APPL-1056, ¶18.

Third, PO mischaracterizes 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. APPL-1056, ¶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 [sic] during post-authentication [and] 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.**"). APPL-1056, ¶20.

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.

Thus, PO's arguments mischaracterize the prior art and should be rejected.

APPL-1056, ¶¶21-22.

2. **Stone combined with Hoyos and Varghese renders 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 [1.2]**¹

PO states, “Petitioner fails to show that Stone discloses biometric information that is associated with an account of the account holder as limitation [1.2] requires,” because “Stone **does not** disclose any association of a user identified 418 with a user's account 422 that **occurs on the user's device 404.**” POR, 33-34. This is incorrect. APPL-1056, ¶23.

As explained in the Petition, a POSITA would have been motivated to implement the biometric authentication as taught by Hoyos on the client (user device 404) of the client-server system of Stone, for the benefits of improved security and privacy, and “[s]uch an approach is convenient as it is relatively simple and cheap to build biometric authentication systems supporting biometric storage at the client end able to support local matching.” Pet. 20-21; APPL-1003, ¶68 (citing APPL-1015, FIG. 3, 4:4-10; APPL-1016, [0040], [0042], [0076], APPL-1038, 64). PO's own expert, Dr. Goodrich, explains in his paper that for biometric authentications, “[t]here are two broad approaches: The one where the comparison is done at the

¹ The analysis with respect to limitations [1.2] similarly apply to limitations [10.1] and [19.1].

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); APPL-1050, 75:17-20 (Dr. Goodrich testifying that C-101 is related to applications “for financial transactions, such as with a bank”), 74:10-19 (Dr. Goodrich testifying that whether to perform computations for biometric authentication including “convert[ing] biometric raw data into a template” on client or server is a well-known design choice, taking into consideration of the computational power of the client device). APPL-1056, ¶24.

Accordingly, a 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, which supports subsequent local matching during the live-scan process of the biometric authentication. APPL-1037, Guidance, 9-10 (explaining that biometric authentication includes an enrollment process and a live-scan process). APPL-1056, ¶25.

a. Stone combined with Hoyos and Varghese renders obvious that a processor of a user device performs all steps of [1.2]

Specifically, as shown in an example of a system of Stone combined with Hoyos and Varghese with client-side authentication below, Stone combined with Hoyos and Varghese renders obvious that *a processor* (a processor of user device 404 alone) *is configured to:*

receive (by user device 404 during biometric enrollment process) *biometric information* (a reference biometric information) *associated with an account holder* (user 409);

store (by user device 404 during biometric enrollment process), *in a data store* (storage component 508 of user device 404), *the received biometric information* (the reference biometric information), *wherein the biometric information* (the reference biometric information, to be stored as “biometric id” associated with a user account, e.g., in a database in a form of a template, the original raw biometric information, or some form of processed biometric information) *is associated with an account* (a user account) *of the account holder* (user 409). APPL-1056, ¶26.

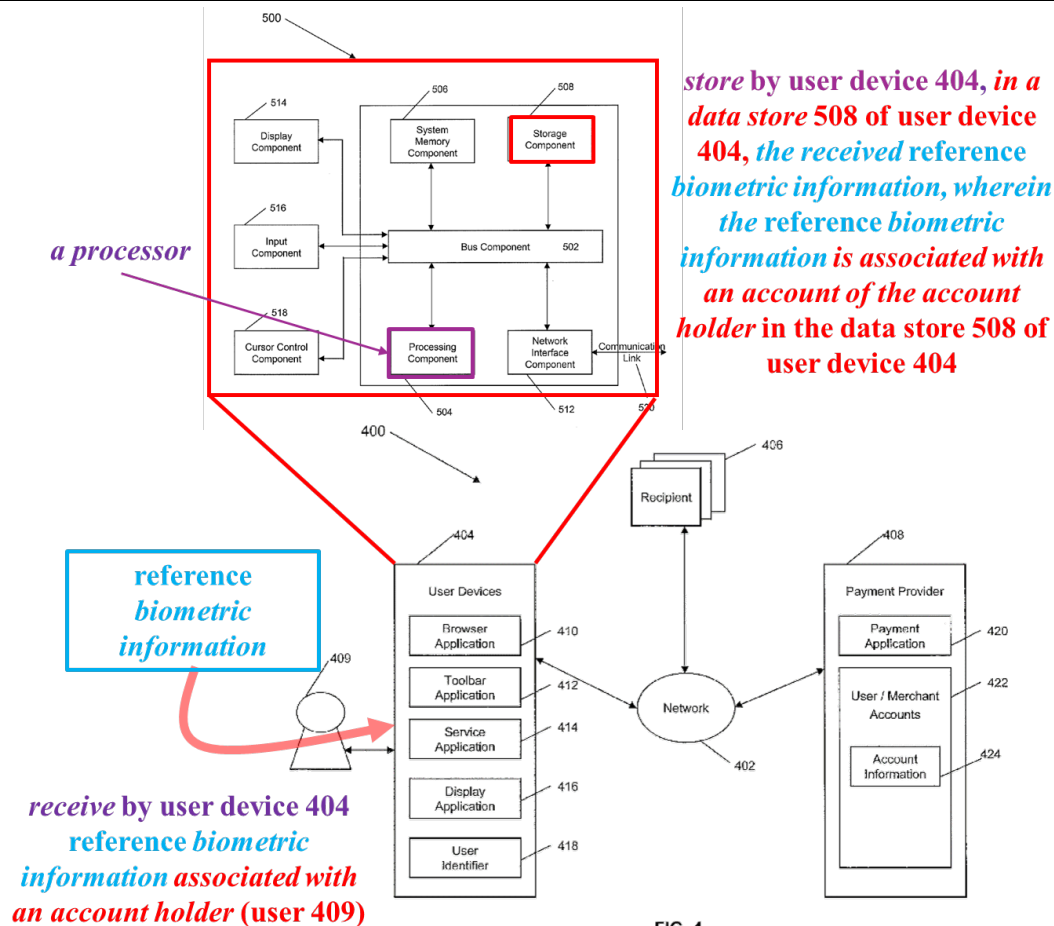


FIG. 4

Example of Stone Combined with Hoyos and Varghese (annotated based on APPL-1008, Stone, FIGS. 4 and 5).

PO appears to argue that because the payment server 408 maintains the user accounts 422, the association of the reference biometric information with a user account **has to** be performed by the payment server 408. This is incorrect. In the system of Stone combined with Hoyos and Varghese where the biometric authentication is performed locally on the user device, the reference biometric information is stored **locally** and is associated with a user account for comparison later on, which provides enhanced privacy and improved security. Pet. 20-21; APPL-

1003, ¶68 (citing APPL-1015, FIG. 3, 4:4-10; APPL-1016, [0040], [0042], [0076], APPL-1038, 64); APPL-1016, [0040], [0042], [0076]; APPL-1038, 64 (stating that “[b]iometric authentication can be implemented through systems performing the matching either on the server or on the client side,” and describing that “security and privacy problems” and CPU-intensiveness of server side implementation, and “relatively simple and cheap” with security and privacy are benefits of client side implementation). APPL-1056, ¶27.

In the system of Stone combined with Hoyos and Varghese where the biometric authentication is performed locally on the user device, user device 404 receives the user account through network 402 from the payment provider 408, and associates the received reference biometric information with the user account in its storage component, e.g., for performing a client-side biometric authentication process later on. *See* APPL-1055, 2 (explaining that 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-1056, ¶28.

b. Stone combined with Hoyos and Varghese renders obvious that the processor of the user device performs [1.6]-[1.8] after [1.2]

PO states, “[e]ven if Petitioner were to suggest that the association step occurring in the payment provider server discloses limitation [1.2], this would conflict with the ’656 Patent’s claimed transaction flow” shown in [1.6]-[1.8] that need to be “*subsequent*” to [1.2]. POR, 35. PO’s arguments fail because they ignore the Petition’s explanation that the processor of the user device in Stone combined with Hoyos and Varghese performs [1.2] during enrollment/registration. PO’s arguments also fail because they are premised on a mischaracterization of Stone as “only disclos[ing]...associating the biometric id with a user’s account [in the context of] a user money transfer request to the payment provider server.” See POR, 36. APPL-1056, ¶29.

Contrary to PO’s argument, in the system of Stone combined with Hoyos and Varghese where the biometric authentication is performed locally on the user device, the reference biometric information is received and stored on user device 404, associated with a user account, during an enrollment/registration process. Pet., 32. APPL-1037, Guidance, 9 (“The process of introducing people into a biometrics-based system is called ‘enrollment.’ In enrollment, samples of data are taken from one or more physiological or physical characteristics; the samples are converted into a mathematical model, or template; and the template is registered

into a database on which a software application can perform analysis.”). Biometric matching alone cannot determine or authenticate identity; one of the biometric templates must have an identity associated with it, and if the match is successful (to a sufficient confidence) then the other template is identified or authenticated. Thus, any system performing biometric authentication must have an enrollment process where templates with asserted person identities are added to a storage or database. After enrollment, a user would “interact with the live-scan process of the biometrics technology,” which is also referred to as the “authentication process” of biometric authentication, and the stored reference biometric information is used to be compared with the results of the live scan for authentication. APPL-1037, Guidance, 10 (“The live scan is used to identify and authenticate the customer. The results of a live scan, such as a fingerprint, are compared with the registered templates stored in the system. If there is a match, the customer is authenticated and granted access.”). APPL-1056, ¶30.

Moreover, Stone combined with Hoyos and Varghese renders obvious that the processor of the user device performs [1.6]-[1.8] (including [1.7.2] reciting *a comparison based at least in part on **the stored biometric information***) after [1.2], because *the processor* (e.g., processor 504 in user device 404 alone) *is configured to:*

[1.6] *subsequent to receiving the indication of the action taken by the user, capture (by user device 409 after confirm step 316) contextual information associated with the electronic transaction, the captured contextual information comprising captured biometric information and location data associated with the user;*

[1.7.1] *..., wherein performing the fraud detection analysis comprises:*

[1.7.2] *performing (by user device 404) a comparison based at least in part on the stored biometric information (the reference biometric information of [1.2] stored in the user device 404) and the captured biometric information ...*

[1.8] *based at least in part on both the user interaction with the transaction icon rendered in the interface (of user device 404) and performing the fraud detection analysis, complete (by user device 404) the electronic transaction.*

Accordingly, Stone combined with Hoyos and Varghese renders obvious that the processor of the user device performs [1.6]-[1.8] **after** [1.2]. APPL-1056, ¶¶31-32.

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

Further, PO's arguments fail because they disregard fundamental knowledge of biometric authentication well-known in the art. Specifically, PO does not dispute that Stone discloses biometric ID and performs the biometric authentication process.

Further, PO does not dispute that Hoyos and Varghese each disclose biometric authentication. However, PO argues that Stone combined with Hoyos and Varghese does not teach enrollment, which disregards the fundamental knowledge that biometric authentication—such as that in Stone combined with Hoyos and 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., 32; 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; APPL-1056, ¶33.

3. Stone combined with Hoyos and Varghese renders obvious “*a memory coupled to the processor and configured to provide the processor with instructions*” as recited in [1.9].

PO states, “Petitioner fails to identify in Stone ‘*a memory coupled to the processor and configured to provide the processor with instructions.*’” POR, 38. However, PO’s arguments misrepresent the Petition’s combination, and should be rejected. APPL-1056, ¶34.

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.” POR, 40

(providing no support other than “*See* III.A.1.b,” which also does not provide substantive support). PO's premise is incorrect. As discussed above at III.A.2.a, Stone combined with Hoyos and Varghese renders obvious [1.2], where *a processor* (processor of user device 404) performs all the steps of [1.2], including the receiving, the storing and the association as claimed. APPL-1056, ¶35.

As shown in the example of Stone combined with Hoyos and Varghese with client-side authentication below, Stone combined with Hoyos and Varghese renders [1.9] obvious, because the processor of user device 404 is configured to perform all the steps of claim 1, and *a memory* (system memory component 506) of the user device 404 *is coupled to the processor and configured to provide the processor instructions*. APPL-1056, ¶36.

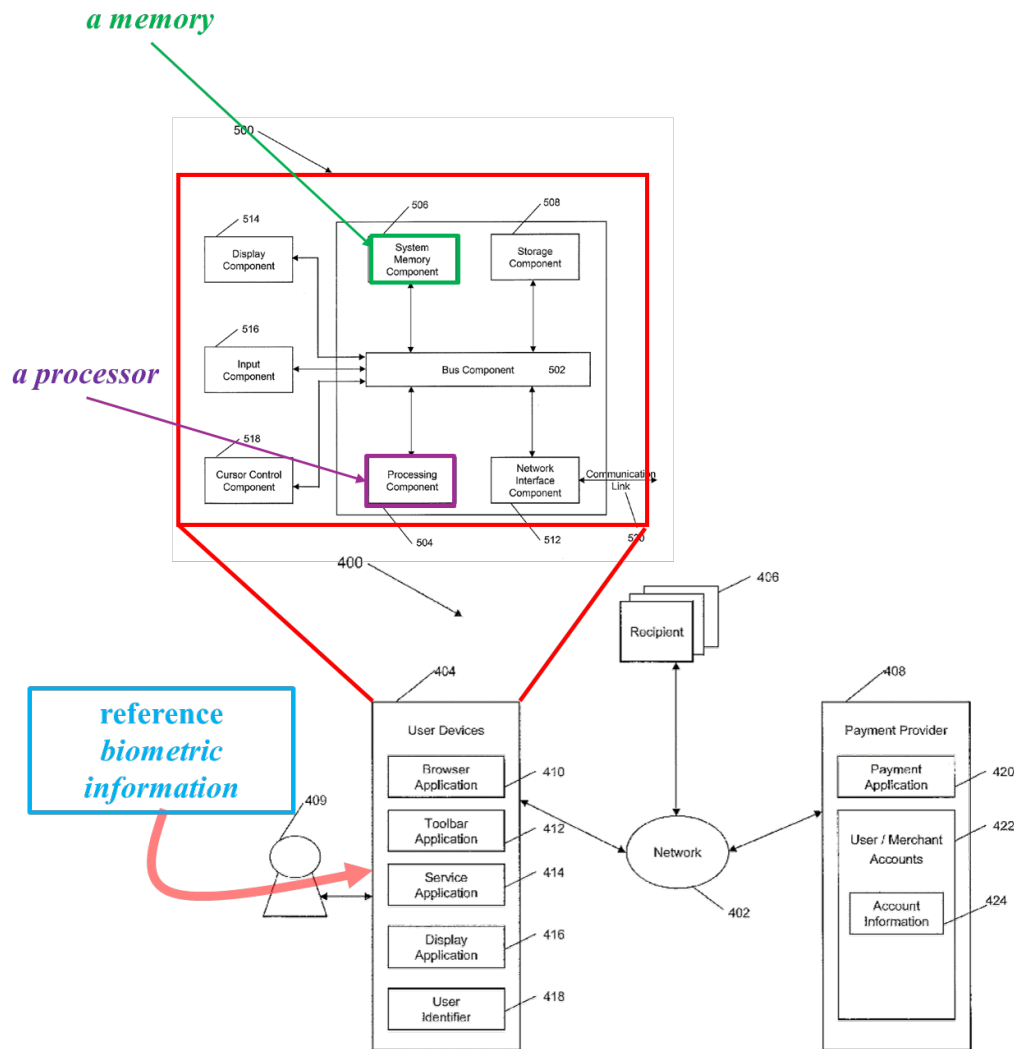


FIG. 4

**Example of Stone Combined with Hoyos and Varghese
(annotated based on APPL-1008, Stone, FIGS. 4 and 5).**

B. Stone combined with Hoyos and Varghese renders obvious the challenged dependent claims.

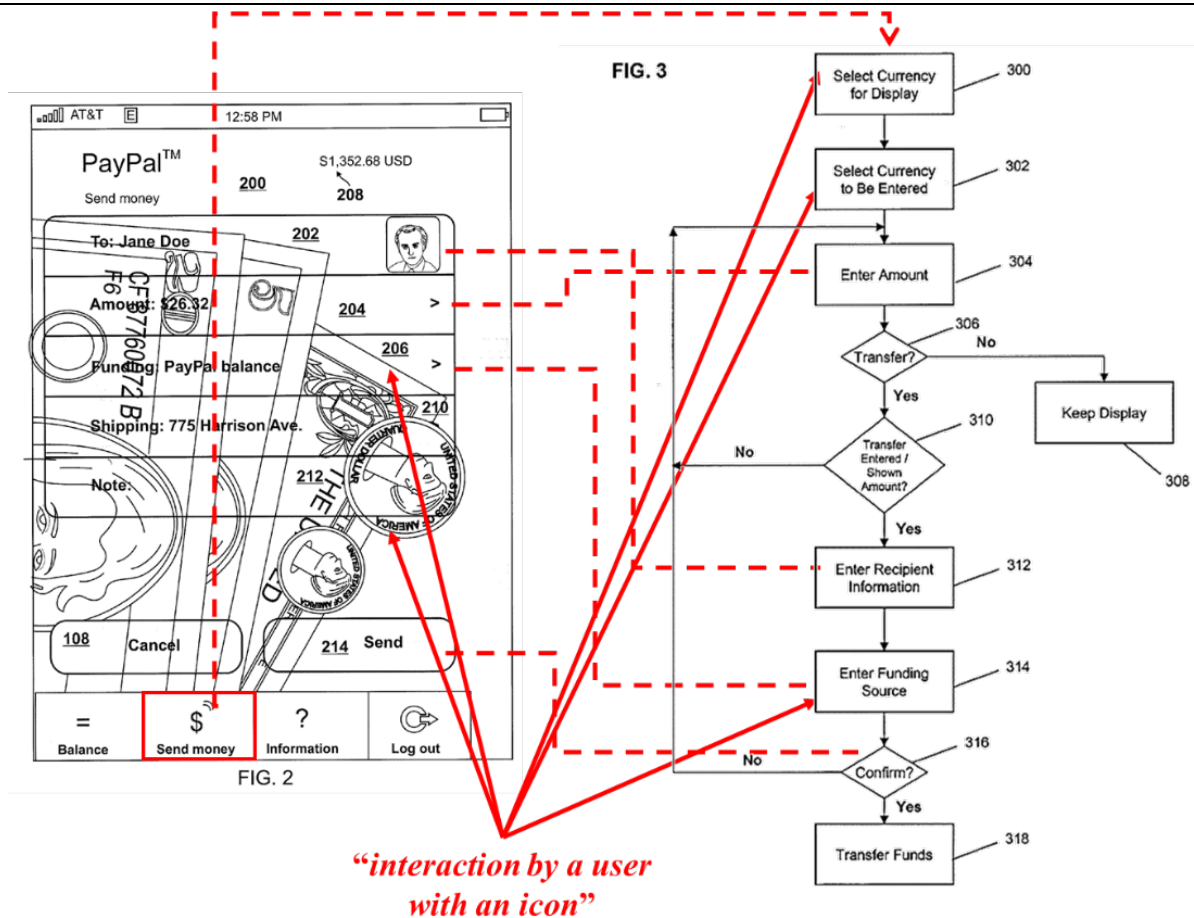
PO does not dispute that Stone combined with Hoyos and Varghese renders obvious the limitations of dependent claims 4-9, 13-18. POR, 41-42. PO's arguments for dependent claim limitations are limited to "*wherein the transaction icon includes a graphical representation of payment form*" in claims 5 and 14, and "*wherein the*

virtual likeness comprises an avatar selected by the account holder” in claims 8 and 17. *Id.* PO's arguments should be rejected, because they are contrary to the disclosure of the prior art. APPL-1056, ¶37.

1. Stone combined with Hoyos and Varghese renders obvious “*wherein the transaction icon includes a graphical representation of payment form*” in claims 5 and 14.

Regarding claims 5 and 14, PO states, “[n]either Stone nor Hoyos discloses that a transaction icon can be a payment form,” and “Petitioner provides no explanation why this would be obvious without working backward from claim 4 [sic] of the '656 Patent using hindsight.” POR, 41. This is incorrect. APPL-1056, ¶38.

PO's arguments should be rejected because they are conclusory and fail to rebut the explanation provided by the Petition. **First**, PO does not dispute that 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-1056, ¶39.



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

Second, PO does not dispute that Stone teaches a *graphical representation of payment form* of funding sources (display of “specific card, such as a PayPal card, Visa, MC, AMEX, etc.”). APPL-1008, [0038]. **Third**, PO fails to rebut that 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. APPL-1056, ¶40.

Similarly, PO fails to rebut the Petition's explanation that 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. APPL-1056, ¶41.

Accordingly, PO's arguments are meritless and should be rejected. APPL-1056, ¶42.

2. Stone combined with Hoyos renders obvious “*wherein the virtual likeness comprises an avatar selected by the account holder*” in claims 8 and 17.

PO argues that “Petitioner provides no justification why it would be obvious to use an avatar for an electronic payment system—besides hindsight bias.” POR, 42.

However, PO disregards Petition's explanation that an “avatar selected by the account holder is **a well-known alternative of a picture for a user icon**” is within a POSITA's knowledge. Pet. 56-57; *KSR Intern. Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1732 (POSITA “has good reason to pursue the known options within his or her technical grasp” where there are “there are a finite number of identified, predictable solutions” for solving the design need). PO further disregards Petition's explanation of benefits of using an avatar, supported by multiple references. *Id.* Thus, PO's arguments should be rejected. APPL-1056, ¶¶43-44.

IV. Ground 2: Stone Combined with FFIEC Guidance (Guidance) Renders the Challenged Claims Obvious.

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

PO does not dispute that the Guidance is analogous art to the '656 Patent, nor does PO dispute that a POSITA "could have accessed" the Guidance. POR, 46. 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, 46. PO's arguments are contrary to the record illustrating a POSITA's interest in the Guidance, contrary to its own expert's practices, contrary to the law, and should be rejected. APPL-1056, ¶¶45-51.

First, PO's arguments are contrary to the record illustrating that the Guidance is within a POSITA's interest of the subject matter (biometric authentication). Pet., 6-7; APPL-1003, ¶¶47-50 (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 (Dr. Jones testifying regarding the significance of the Guidance in the biometrics industry and personal knowledge of the Guidance); APPL-1056, ¶¶45-51 (Dr. Jones explaining that a POSITA would have interest in the Guidance). 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. APPL-1056, ¶50.

Second, 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. APPL-1056, ¶51.

PO’s reliance on *Samsung* is misplaced, because *Samsung* does not address the issue of a POSITA’s interest in regulations, but is directed at the legal standard for whether a POSITA “could have accessed” a reference, which is not in dispute here. *Samsung Elecs. Co., Ltd. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1375 (Fed. Cir. 2019).

B. Stone combined with Guidance renders obvious the challenged claims.

PO relied upon its arguments in Ground 1 and argued that Stone-Guidance does not render the Challenged Claims obvious. POR, 43-44, 48. PO’s arguments fail for the same reasons that they fail for Ground 1 as explained above. APPL-1056, ¶52.

V. Grounds 3 and 4: Combination of Stone, Hoyos, Varghese, and Borovsky (Ground 3) and Combination of Stone, Guidance, and Borovsky (Ground 4) Render obvious Claims 2-3 and 11-12.

PO does not dispute that Borovsky teaches the limitations of claims 2-3 and 11-12. POR, 48-51. Instead, PO states that there is no motivation in Stone for “using social networks to populate any information for the disclosed interface,” and that “[n]othing in Stone suggests introducing another third-party server to Stone’s existing client-server.” POR, 49, 50. PO’s arguments fail, because they are contrary to the record, contrary to the law, and disregard Petition’s reasons to combine. APPL-1056, ¶53.

“There is a motivation to combine when a known technique ‘has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way,’ using the ‘prior art elements according to their established functions.’” *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1380–81 (Fed. Cir. 2023). Here, the Petition identifies Borovsky’s known techniques used to improve a user interface by updating contact display on a user device with a photo from social networks. Borovsky’s techniques would improve the user interface and user experience in Stone’s system, in the same way when used according to Borovsky’s teachings. Pet. 77-79; APPL-1056, ¶54. Accordingly, PO’s arguments are meritless and should be rejected.

Respectfully submitted,

Dated: January 16, 2025
HAYNES AND BOONE PLLC
2801 N. Harwood Street, Suite 2300
Dallas, TX 75201

/David W. O'Brien/
David W. O'Brien
Lead Counsel for Petitioner
Registration No. 40,107

VI. Certificate of Word Count

Pursuant to 37 C.F.R. § 42.24, the undersigned attorney for the Petitioner declares that the argument section of this Reply (Sections I-V) has a total of 5,160 words, according to the word count tool in Microsoft Word™.

/David W. O'Brien/

David W. O'Brien
Lead Counsel for Petitioner
Registration No. 40,107

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. § 42.6(e), service was made on Patent Owner as detailed below.

Date of service: January 16, 2025

Manner of service: Electronic Mail: Rkamprath@mckoolsmith.com;
gfishback@mckoolsmith.com;
Carbyne_Apple@mckoolsmith.com

Documents served: **Petitioner's Reply to POR;
EXHIBITS APPL-1049 – APPL-1056.**

Persons served: Richard A. Kamprath
MCKOOL SMITH, P.C.
300 Crescent Court, Suite 1500
Dallas, Texas 75201

George Fishback
MCKOOL SMITH, P.C.
303 Colorado Street, Suite 2100
Austin, Texas 78701

/David W. O'Brien/
David W. O'Brien
Lead Counsel for Petitioner
Registration No. 40,107