UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

APPLE INC.,
Petitioner

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner

_____

Case: IPR2024-00332
U.S. Patent No. 10,929,512

_____

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I. INTRODUCTION 1

II. BACKGROUND 3

A. THE '512 PATENT 3

B. THE ART 6

1. Kesanupalli (Ex. 1006) and Challener (Ex. 1007) 6

2. Cheng (Ex. 1008) 11

C. TRUSTED PLATFORM MODULES 11

D. PERSON OF SKILL IN THE ART 13

E. CLAIM CONSTRUCTION 13

III. ARGUMENT 13

A. A POSITA (LIKE RAMESH KESANUPALLI) WOULD NOT HAVE COMBINED KESANUPALLI AND CHALLENER TO ARRIVE AT THE CLAIMED TWO PROCESSOR SYSTEM. 14

1. The Board must consider what a POSITA actually did. 14

2. The Kesanupalli reference was interested in curbing social engineering attacks and would not have benefited from a TPM such as the one taught by Challener. 16

3. Using a TPM had drawbacks that a POSITA would have been aware of. 29

B. THE PETITION FAILS TO SHOW THE COMBINED CHENG WITH CHALLENER/KESANUPALLI DISCLOSES "SECOND PROCESSOR CONFIGURED TO" (CLAIM 1.7) "PERFORM A SECURE BACKUP OF THE RECORD TO A STORAGE SERVICE" (CLAIM 1.7A). 31

1. Petitioner has failed to show a "second processor configured to" (claim 1.7) "perform a secure backup of the record to a storage service" (claim 1.7A). 32

2. A POSITA would not have reasonably expected the Cheng backup to work with the Kesanupalli/Challener TPM architecture. 35

C. EVEN IF COMBINED, THE PETITION FAILS TO SHOW THAT THE DEFENDANT CLAIMS 2 AND 12 ARE UNPATENTABLE IN LIGHT OF KESANUPALLI, CHALLENER, AND CHENG. 38

1. Kesanupalli, Challener, and Cheng do not teach or suggest "[t]he system recited in claim 1, wherein the storage service comprises a cloud storage service" (claim 2) and (claim 12). 38

D. INDEPENDENT CLAIMS 11 AND 21 ARE NOT INVALIDATED BY KESANUPALLI, CHALLENER, AND CHENG. 39

IV. CONCLUSION 39

TABLE OF AUTHORITIES

Page(s)

CASES

Allied Erecting & Dismantling Co. v. Genesis Attachments, LLC,
825 F.3d 1373 (Fed. Cir. 2016) 14

Apple Inc. v. Samsung Elecs. Co.,
839 F.3d 1034 (Fed. Cir. 2016) 15

Axonics, Inc. v. Medtronic, Inc.,
73 F.4th 950 (Fed. Cir. 2023) 14, 15

In re Jones,
958 F.2d 347 (Fed.Cir. 1992) 16

In re Urbanski,
809 F.3d 1237 (Fed. Cir. 2016) 14

Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.,
821 F.3d 1359 (Fed. Cir. 2016) 29

Juniper Networks, Inc. v. Correct Transmission, LLC,
No. 2023-1046, 2024 WL 3517862 (Fed. Cir. July 24, 2024) 37

KEYnetik, Inc. v. Samsung Electronics Co., Ltd.,
841 Fed.Appx. 219 (Fed. Cir. 2021).....35

KSR Int'l Co. v. Teleflex Inc.,
550 U.S. 398 (2007).....15

Pfizer, Inc. v. Apotex, Inc.,
480 F.3d 1348 (Fed. Cir. 2007) 14

St. Jude Med., Inc. v. Access Closure, Inc.,
729 F.3d 1369 (Fed. Cir. 2013) 29

Virtek Vision Int'l ULC v. Assembly Guidance Sys., Inc.,
97 F.4th 882 (Fed. Cir. 2024) 28

PREVIOULSY SUBMITTED EXHIBITS

Exhibit	Description
2001	*Carbyne Biometrics, LLC v. Apple Inc.*, 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	*Carbyne Biometrics, LLC v. Apple Inc.*, 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	*Carbyne Biometrics, LLC v. Apple Inc.*, 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	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 64 (Defendant's Opposed Motion to Stay Pending Transfer) (W.D. Tex. November 28, 2023)
2005	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 37 (Defendant's Opposed Motion to Transfer (redacted)) (W.D. Tex. July 26, 2023)
2006	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 66 (Carbyne's Response to Motion to Stay Pending Transfer) (W.D. Tex. December 5, 2023)
2007	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 50(Carbyne's Response to Motion to Transfer Venue) (W.D. Tex. October 27, 2023)
2008	*Carbyne Biometrics, LLC v. Apple Inc.*, 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	*Carbyne Biometrics, LLC v. Apple Inc.*, 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	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 42 (Apple's Opening Claim Construction Brief) (W.D. Tex. October 4, 2023)
2011	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 49 (Carbyne's Response to Apple's Proposed Claim Construction) (W.D. Tex. October 25, 2023)
2012	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Dkt 54 (Apple's Reply Claim Construction Brief) (W.D. Tex. November 8, 2023)
2013	*Carbyne Biometrics, LLC v. Apple Inc.*, 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	*Carbyne Biometrics, LLC v. Apple Inc.*, 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	*Carbyne Biometrics, LLC v. Apple Inc.*, 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	*Carbyne Biometrics, LLC v. Apple Inc.*, 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	*Carbyne Biometrics, LLC v. Apple Inc.*, 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	*In Re Apple*, Case No. 2024-111, Dkt 2 (Apple's Petition for Writ of Mandamus) (Fed. Cir. February 1, 2024)
2019	*In Re Apple,* Case No. 2024-111, Dkt. 13 (Carbyne's Response to Writ of Mandamus) (Fed. Cir. February 20, 2024)
2020	*In Re Apple Inc.*, Case No. 2024-111, Dkt 15 (Apple's Reply In

	Support of Petition for Writ of Mandamus) (Fed. Cir. February 27, 2024)
2021	*In Re Apple Inc.*, 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	*Cloud of change, LLC v. Lightspeed POS Inc.,* Case NO. 6:21-cv-0102 Order Denying Lightspeed POS Inc's Opposed Motion to Stay Pending Resolution of *Inter Partes* Review (W.D. Tex. Dated May 15, 2023)
2024	*Sonrai Memory Limited v. LG Electronics, Inc.* 2022 WL 2307475 (W.D. Tex. June 27, 2022)
2025	*Carbyne Biometrics, LLC v. Apple Inc.*, Case No. 1:23-cv-00324, Apple's Amended Preliminary Invalidity Contentions (W.D. Tex. October 6, 2023) (excerpts)
2026	U.S. Patent No. 11,514,138
2027	U.S. Patent No. 11,841,929
2028	U.S. Patent No. 11,475,105
2029	U.S. Patent No. 11,556,617
2030	U.S. Patent Application 2011/0138450 ("Kesanupalli '450")
2031	U.S. Patent No. 7,780,080 ("Owen")
2032	*Intentionally Omitted*
2033	*Intentionally Omitted*
2034	*Intentionally Omitted*
2035	Email Correspondence From Counsel Of Petitioner To Counsel of Patent Owner re *Sotera* Stipulations and *Carbyne Biometrics, LLC*

	v. Apple Inc., 1:23-cv-0032 (W.D. Tex.)
2036	Email Correspondence From Counsel Of Petitioner To The Board re *Sotera* Stipulations for IPRs IPR2024-00329, -00330, -00331, -00332, -00333, -00334 and-00507.

NEW EXHIBITS WITH THIS REPSONSE

Exhibit	Description
2037	Declaration of Dr. Michael Goodrich
2038	CV of Dr. Michael Goodrich
2039	FIDO Presentation of Ramesh Kesanupalli
2040	PUBLIC Excerpts of the deposition transcript of Mr. Michael Barrett
2041	David Challener & Will Arthur, A Practical Guide to TPM 2.0 (Apress 2015)
2042	David C. Challener & J. D. Osborn, Trusted Platform Module Evolution (2015)
2043	Rachna Dhamija, J.D. Tygar & Marti Hearst, Why Phishing Works, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06) 581 (2006), https://doi.org/10.1145/1124772.1124861.
2044	S Sinclair, SW Smith, The TIPPI point: Toward trustworthy interfaces, IEEE Security & Privacy 3 (4), 68-71, 2005
2045	Ramesh Kesanupalli, LinkedIn Profile, https://www.linkedin.com/in/ramesh-kesanupalli-22b73/ (accessed Oct. 5, 2024)

Exhibit	Description
2046	Dave Challener, LinkedIn Profile, https://www.linkedin.com/in/dave-challener-bbab7b/ (accessed Oct. 5, 2024)
2047	Nok Nok, About, https://noknok.com/about/ (accessed Oct. 5, 2024)
2048	Ramesh Kesanupalli, Team, Nok Nok, https://noknok.com/about/team/ramesh-kesanupalli/ (accessed Oct. 5, 2024)
2049	Federal Trade Commission, How to Recognize and Avoid Phishing Scams, https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (accessed Oct. 5, 2024)
2050	Microsoft, Introduction to Windows Biometric Framework, https://download.microsoft.com/download/9/c/5/9c5b2167-8017-4bae-9fde-d599bac8184a/wbfintro.docx (accessed Oct. 5, 2024)
2051	ISO/IEC 11889-1:2009, Information Technology — Trusted Platform Module — Part 1: Architecture (2009).
2052	Deposition transcript of Dr. McDaniel
2053	Excerpts from Deposition transcript of Dr. Nielson

I. INTRODUCTION

The Board instituted this IPR without the benefit of a complete and accurate factual record. The Board's institution decision rests on an incomplete understanding of the problems addressed by the references and of the relevant technology. The Petition, in seeking to rewrite history, incorrectly posits what a POSITA would have done when faced with the challenges encountered by bad actors employing social engineering attacks and ignores what a POSITA *actually* did. The Board should decline to find the patents unpatentable for a number of reasons.

First, as the record plainly demonstrates, Kesanupalli's decision to forego the use of a TPM was a deliberate choice informed by the specific context and technological considerations of the problems facing users. The Kesanupalli reference is directed to curbing social engineering attacks that trick a user into providing their credentials to an imposter. The factual record, when fully and properly considered, reveals precisely what a POSITA would have done—and indeed did do—when faced with issues related to social engineering attacks and that was to not incorporate a TPM as disclosed by Challener, which would not have done anything to address these attacks. Rather, as Kesanupalli discusses the proper thing to do is promote better password practices and/or use other methods (such as binding credentials to URLs) to ensure that a user was sending their credentials to a

legitimate recipient and not an imposter. What a POSITA did cannot be ignored or explained away nearly 15 years later because the '512 Patent teaches something else.

Second, even if a POSITA would have combined Kesanupalli with the TPM disclosed by Challener, the combination is still lacking with respect to the challenged claims. The Kesanupalli/Challener system does not disclose the claimed second processor that is configured to perform a secure backup. Acknowledging this, the Petition points to Cheng's disclosure of a tiered backup method. But even with this addition, the Petition fails to show that the *second processor* (the TPM/fingerprint sensor processor) of the Kesanupalli/Cheng combination *performs* a secure backup *to* a storage service as required by the claims. This is because the TPM/fingerprint processor can only communicate via a restricted interface with the general processor (first processor) and nothing else.

At bottom, the Petition attempts to rewrite history based on a hindsight analysis that uses the claims of the '512 Patent as a map. The Petition ignores what a POSITA would actually have done (and indeed did do) and instead invents reasons to combine references that are devoid of real world context. And even with those contrived motivations to combine, the claimed grounds fail to disclose the claimed limitations.

II. BACKGROUND

A. The ’512 Patent

The ’512 Patent concerns systems and methods for authentication translation. As the Patent explains, previous authentication techniques made “[p]roviding credentials to a service, whether via a mobile or other device . . . a tedious experience for a user.” Ex. 1001 (’512 Patent) at 1:35-37. Because the experience was so tedious, users would “often engage in practices such as password re-use, and/or the selection of poor-quality passwords, which render their credentials less secure against attacks.” *Id*. at 1:38-40. Thus, “improvements in authentication techniques [were] desirable.” *Id*. at 1:40-42.

The ’512 Patent addresses these shortcomings by disclosing novel authentication systems and methods where “users need not type such usernames and passwords into their devices whenever required by a service. Instead, users can authenticate themselves to an ‘authentication translator’ via an appropriate technique, and the authentication translator will provide the appropriate credentials to the implicated service on the user’s behalf.” *Id*. at 2:63-3:1. By doing this, the system promotes better user security practices by making it easier for a user to use complex passwords.

As the ’512 patent discloses, the process begins “when a request to access a resource is received, as is an authentication input.” *Id.* at 6:20-21. For example,

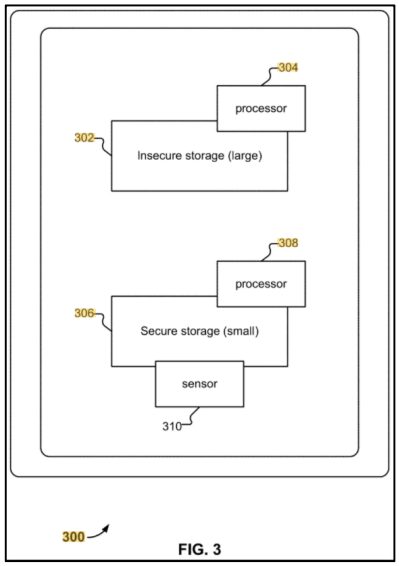
suppose "[the user] wishes to sign into social networking website." *Id*. at 6:22-23. "[The user] directs [their] web browser . . . to the social networking website." *Id*. at 6:23-25. The "Authentication translator module **132** recognizes, from the context of [the user's] actions (e.g., that [the user] is attempting to access site **120** with [their] browser) that [the user] would like to access a particular resource." *Id*. at 6:25-28 (emphasis in original). The authentication translator module may then prompt "[the user] (e.g., by a popup message or via a sound) to provide biometric information (e.g., to use the integrated fingerprint reader on [the user's device])." *Id.* at 6:28-31.

Once a biometric has been supplied by the user, the supplied biometric data is compared "to the templates stored on [the user's device]." *Id*. at 6:39-40. "If a suitable match is found . . . the username and password for the website, as stored in a vault, such as vault **220**, are retrieved from the vault" and provided to the resource. *Id*. at 6:40-46 (emphasis in original). In the '512 Patent specification, biometrics include but are not limited to fingerprints, "facial recognition, voiceprints, or retina scan technology." *Id*. at 3:28-29, 3:18-19.

To keep the user's biometrics secure, the '512 Patent discloses a device with "a large and insecure storage **302** attached to a fast processor **304**, and a smaller but secure storage **306** attached to a dedicated processor **308** and a sensor **310** (e.g., a camera or a fingerprint reader)." *Id*. at 3:67-4:4 (emphasis in original); *see also id.* at Fig. 3 (reproduced below). The "[u]sers (and applications) can read from and write

to the insecure storage area." *Id*. at 4:4-5. Data such as authentication information and biometrics can be stored in the secure storage. *Id*. at 3:63-65. "However, users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API." *Id*. at 4:5-8.

Figure 3 of the '512 Patent, which depicts a device with large and insecure storage attached to a fast processor, and a smaller but secure storage attached to a dedicated processor and a sensor in accordance with an embodiment of the inventions, is reproduced below.



Id. at Fig. 3.

Further enhancing the user authentication experience and promoting better security practices across multiple devices, the '512 Patent also discloses uploading a secure backup of the records stored in the secure storage to a cloud storage service. *Id*. at 7:55-8:8. "The cloud storage service **140** is configured to accept backups from

multiple devices associated with a single account, and synchronize the updates so that all devices get automatically refreshed." *Id*. at 7:56-59 (emphasis in original). This allows a user to access and synchronize authentication information across multiple devices, *id*. at 7:59-62, further reducing the tedious experience of using complex passwords.

B. The Art

1. Kesanupalli (Ex. 1006) and Challener (Ex. 1007)

a) Kesanupalli (Ex. 1006)

Kesanupalli is titled "Secure User Authentication Using Biometric Information." Ex. 1006 (Kesanupalli). Kesanupalli states that "[t]ypical user authentication systems and procedures use passwords to authenticate the identity of the user." Ex. 1006 (Kesanupalli) at 1:27-28; Ex. 2037 (Goodrich Decl.) at ¶33. However, "passwords are subject to various attacks" including "phishing attacks [and] social engineering attacks." Ex. 1006 (Kesanupalli) at 1:35-37; Ex. 2037 (Goodrich Decl.) at ¶33. Kesanupalli adds that longer passwords with combinations of letters and numbers provide a higher level of security but users do not always use longer and more complicated passwords because they "are more difficult for users to remember." *Id*. at 1: 1:36-41; Ex. 2037 (Goodrich Decl.) at ¶33.

Thus, according to Kesanupalli, it would be desirable to "provide a user authentication method and system that provides a more secure authentication of the

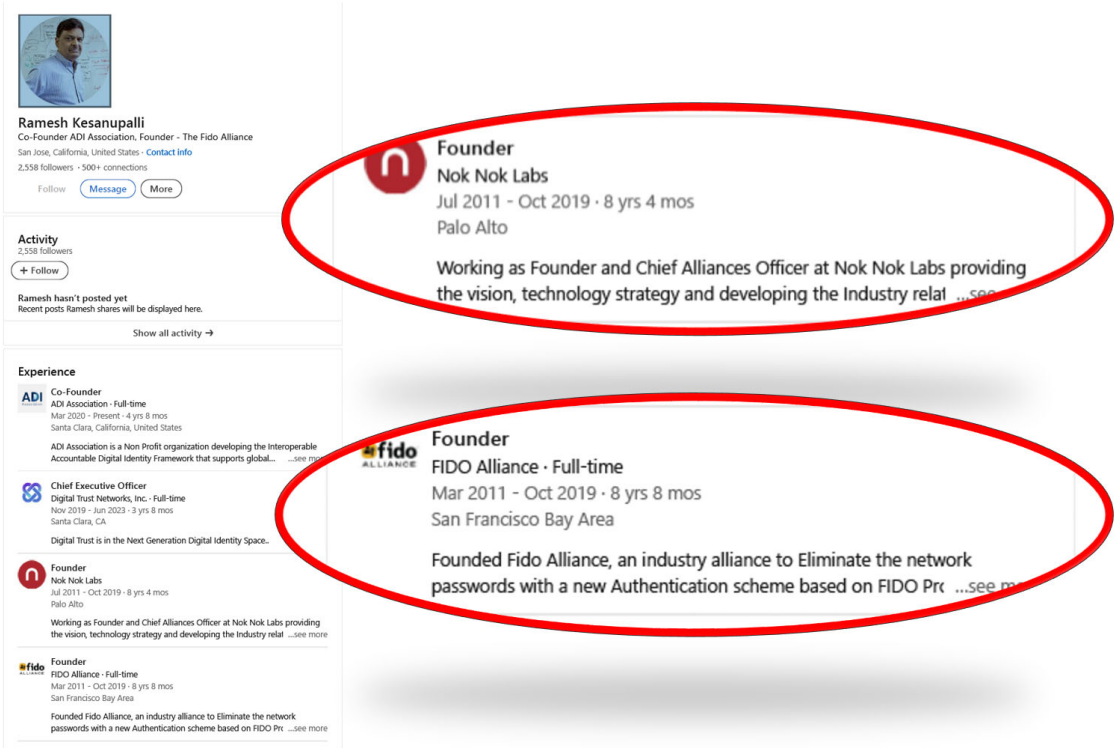
user than commonly used password-based methods and systems." Ex. 1006 (Kesanupalli) at 1:59-62; Ex. Ex. 2037 (Goodrich Decl.) at ¶33. To do this, Kesanupalli discloses a system that uses a fingerprint scan to release credentials to bound websites so that users can use more complicated passwords without having to remember them and so that credentials will not be released to spoofed websites. *See* Pet. 10 ("For example, based on a match between a fingerprint template stored for a particular user and fingerprint information read from a finger presented at a fingerprint reader, Kesanupalli's methods retrieve credentials associated with the user and communicate those credentials to an external system or process."); Ex. 2037 (Goodrich Decl.) at ¶¶33-34.

b) Challener (Ex. 1007)

Challener is titled "Apparatus and Method for Enabling Applications on a Security Processor." Ex. 1007 (Challener). Challener's invention "relates to securely protecting computer data, and more particularly to security processors provided in computer systems to implement security features." *Id*. at 1:7–9; Ex. 2037 (Goodrich Decl.) at ¶35. To do this, inventor David Challener, describes a system with "a Trusted Platform Module (TPM) from the Trusted Computing Group (TCG)." Institution Decision at 23-25; Ex. 2037 (Goodrich Decl.) at ¶35.

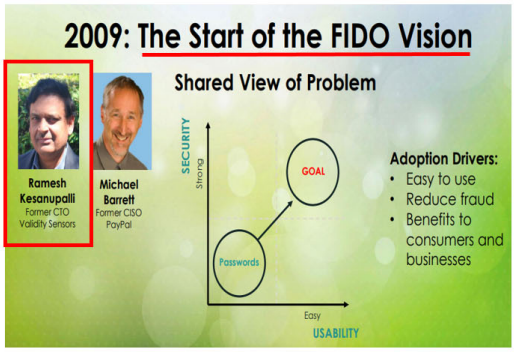
c) Ramesh Kesanupalli and David Challener

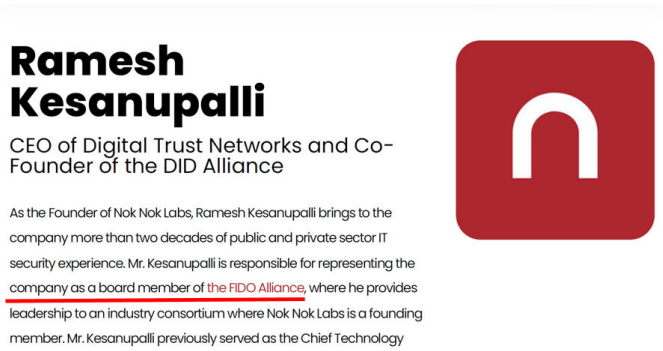
The authors of the Kesanupalli and Challener references are thought leaders in the secure computing/authentication and the decisions they made in their patented systems cannot be simply ignored. Ex. 2037 (Goodrich Decl.) at ¶¶36-39. First, Ramesh Kesanupalli is an entrepreneur and technologist best known for his pioneering work in the field of identity management and authentication. Ex. 2037 (Goodrich Decl.) at ¶37. He is the founder of Nok Nok Labs, a leading provider of next-generation authentication solutions, and a *founder* of the FIDO (Fast IDentity Online) Alliance, an industry consortium dedicated to creating open standards for authentication. Ex. 2039; Ex. 2037 (Goodrich Decl.) at ¶37.



See, e.g., Ex. 2045 (Ramesh Kesanualli LinkedIn).

Beyond his work on FIDO, Mr. Kesanupalli was well aware of TPMs. Ex. 2037 (Goodrich Decl.) at ¶37. During the deposition of Mr. Michael Barrett in the underlying district court case, Mr. Barrett discussed the founding of the FIDO Alliance by himself and Mr. Kesanupalli, which is corroborated by documents published by FIDO and Dr. Kesanupalli.



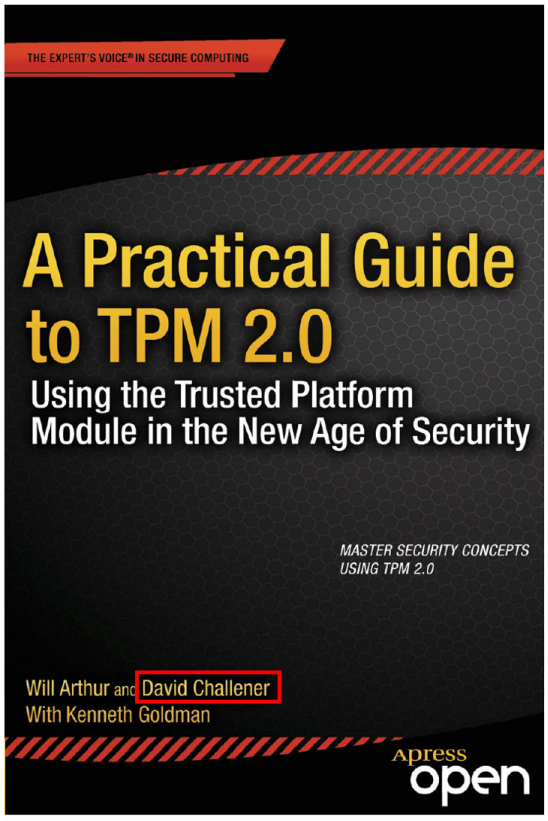


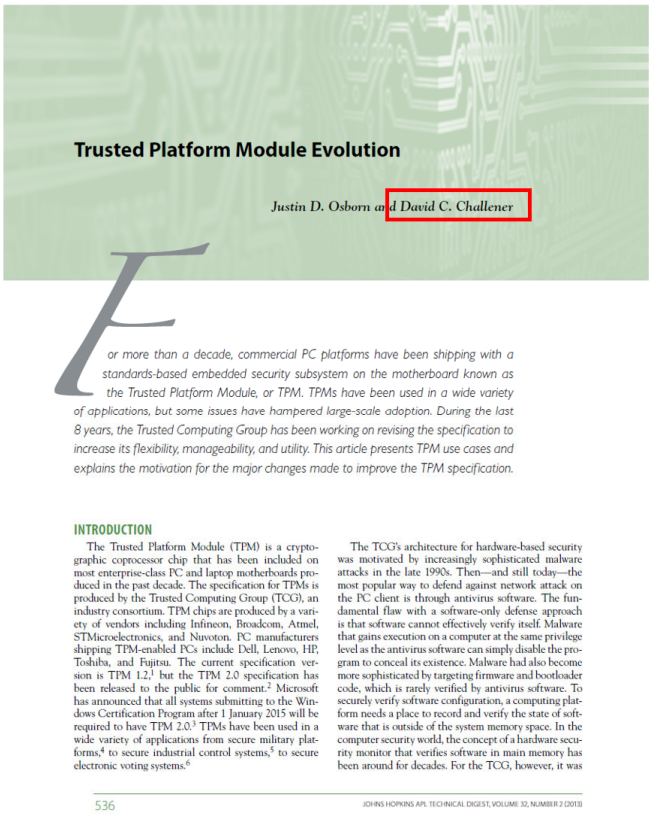
Ex. 2039 (left); Ex. 2048 (right). Mr. Barrett stated that prior to founding FIDO, Mr. Kesanupalli "was part of the Trusted Computing Group, which developed the original TPM standard":

> Q. So secure elements were known before the introduction of mobile phones, right?
>
> A. Oh, yeah, yeah, yeah. Yeah, I mean TPMS—in fact, one of the other FIDO founders, a guy called ***Ramesh Kesanuappli,*** was part of the Trusted Computing Group which developed the original TPM standard.

Ex. 2040 (Redacted Transcript of Michael Barrett) at 91-92 (emphasis added); Ex. 2037 (Goodrich Decl.) at ¶37.

The named inventor on Challener (Dr. Challener) was "active in the TCG, serving on the Board of Directors, chairing the TSS Workgroup, and participating in the Technical Committee, Virtualization Workgroup, and Storage Workgroup. He currently co-chairs the TPM Working Group." Ex. 2042 at 543; Ex. 2037 (Goodrich Decl.) at ¶38. Dr. Challener has authored multiple textbooks and journal articles on TPMs.





See Exs. 2041 (left) and 2042 (right).

2. Cheng (Ex. 1008)

Cheng discloses a method for backing up and restoring a user's device while preserving the secrecy of the data. Ex. 1008 (Cheng) at [Abstract]; Ex. 2037 (Goodrich Decl.) at ¶39. It uses a two-tier encryption structure where data in the lower tier can only be decrypted after the upper tier data has been decrypted and validated. *See, e.g.*, Ex. 1008 (Cheng) at [0007]-[0009]; Ex. 2037 (Goodrich Decl.) at ¶39; Pet. 15-18.

C. Trusted Platform Modules

Trusted Platform Modules (TPMs) are a "standards-based embedded security subsystem on the motherboard." Ex. 2042 at 539; Pet. 13 ("In particular, Challener describes system implementations in accord with a well-known Trusted Platform Module (TPM) specification promulgated by a standards organization, the Trusted Computing Group (TCG)."); Ex. 2037 (Goodrich Decl.) at ¶40. The TPM 1.0 and 1.2 standards were introduced in the early 2000s. Ex. 1003 (McDaniel Decl.) at ¶48; Ex. 2041 at 1-3 (detailing the early TPM specifications); Ex. 2037 (Goodrich Decl.) at ¶¶40-41.

Even though they were well known (Pet. 19), TPMs were not substantially used in the 2000's. Ex. 2037 (Goodrich Decl.) at ¶¶41-43. In his book, Dr. Challener (the named inventor of the Challener reference) explains that even though as of ***2015*** TPMs were "nearly ubiquitous . . . they've [were] mostly invisible to uses due to a

lack of compelling applications to use them." Ex. 2041 at 1; Ex. 2037 (Goodrich Decl.) at ¶¶41-43. This is because, as Dr. Challener wrote in another article, "although the TPM 1.1b and 1.2 specifications created the foundation for the use cases described, a number of roadblocks occurred that hampered adoption by industry. These included ambiguities in the specification, rigidness in the policy regarding how keys are used, tight coupling to specific cryptographic algorithms, and issues related to control of the TPM by platform software." Ex. 2042 at 539; Ex. 2037 (Goodrich Decl.) at ¶¶41-43.

These issues led to the operating system providers, such as Windows, not requiring TPMs until January *2015* and device manufacturers including them in their devices but not enabling them by default. Ex. 2042 at 536 ("Microsoft has announced that all systems submitting to the Windows Certification Program after 1 January 2015 will be required to have TPM 2.0."); Ex. 2042 at 542 ("Without question, the biggest hindrance to widespread adoption of TPM 1.2 is that PC vendors ship machines with the TPM turned off by default."); Ex. 2037 (Goodrich Decl.) at ¶¶41-43. And because they were not required and not on by default, most TPMs were never used. Ex. 2042 at 539 ("Because most users never touch their firmware settings, this means that most TPMs have never been turned on."); Ex. 2037 (Goodrich Decl.) at ¶¶41-43.

D. Person of Skill in the Art

Patent Owner has applied Petitioner's POSITA for the sake of this Response. Pet. 6. This Response does not depend on this skill level. *See* Section III, *infra*; Ex. 2037 (Goodrich Decl.) at ¶¶25-27. Patent Owner's expert meets the definition of a POSITA and met the definition at the priority date. Ex. 2037 (Goodrich Decl.) at ¶¶25-27.

E. Claim Construction

Petitioner takes a position on the plain and ordinary meaning of "restricted interface." *See* Pet. 7-8. This Response does not depend on this definition so Patent Owner does not address this position. *See* Section III, *infra*; Ex. 2037 (Goodrich Decl.) at ¶28.

III. ARGUMENT

As shown below, the Petition fails to show: (1) that a POSITA would have combined Challener's TPM with Kesanupalli's fingerprint sensor given that Kesanupalli was concerned with social engineer attacks that would not be prevented by a TPM; (2) that even if a POSITA combined Cheng's backup method with the Kesanupalli/Challener system, there is no disclosure of a second processor *performing* a secure backup of a record *to* a storage service; and (3) that the unique elements of the dependent claims are taught. *See* Ex. 2037 (Goodrich Decl.) at ¶44. The Board should find that the '512 Patent is not unpatentable in light of the

challenged grounds.

A. A POSITA (like Ramesh Kesanupalli) would not have combined Kesanupalli and Challener to arrive at the claimed two processor system.

1. The Board must consider what a POSITA actually did.

When an obviousness challenge asserts a combination of identified prior art, the motivation-to-combine portion of the inquiry is "whether 'a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention.'" *Allied Erecting & Dismantling Co. v. Genesis Attachments, LLC*, 825 F.3d 1373, 1381 (Fed. Cir. 2016) (internal citations omitted); *see also Pfizer, Inc. v. Apotex, Inc.*, 480 F.3d 1348, 1361 (Fed. Cir. 2007). "The inquiry is not whether a relevant artisan would combine a first reference's feature with a second reference's feature to meet requirements of the first reference that are not requirements of the claims at issue." *Axonics, Inc. v. Medtronic, Inc.*, 73 F.4th 950, 957 (Fed. Cir. 2023).

Taking "[a] contrary view would run counter to established principles, including that the claim defines the invention whose obviousness is being assessed and that a skilled artisan may be motivated to combine particular features of different references, *e.g.*, to secure some benefits at the expense of others, even when bodily incorporation would be impossible or inadvisable." *Id.* (citing *In re Yamamoto*, 740 F.2d 1569, 1573 (Fed. Cir. 1984); *In re Urbanski*, 809 F.3d 1237, 1243–44 (Fed.

Cir. 2016). As the Federal Circuit has stated, "[t]he real question is 'why a person of ordinary skill in the art would have combined elements from specific references in the way the claimed invention does.'" *Axonics*, 73 F.4th at 957.

Here, the Board does not need to look far or make many assumptions about what a person of skill in the art would have done and why they would have done it. The Board is presented with a unique opportunity to review a reference from a contemporary POSITA—Ramesh Kesanupalli. Mr. Kesanupalli was one of the leaders in computer security and a member of the TCG. *See* Section II.B.1, *supra*; Ex. 2037 (Goodrich Decl.) at ¶37. Mr. Kesanupalli was certainly aware of TPMs and made a conscious decision to not use them in his patented system. *See* Section II.B.1, *supra*; Ex. 2037 (Goodrich Decl.) at ¶37. As will be discussed below, Mr. Kesanupalli made this decision for a myriad of reasons. This decision must be respected.

Contrary to Federal Circuit precedent, Petitioner ignores "common sense and real world indicators," such as Mr. Kesanupalli's own decisions as a POSITA to use a TPM, and instead relies on improper hindsight bias to arrive at the claimed invention. *Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1058 (Fed. Cir. 2016) ("Common sense and real world indicators indicate that to conclude otherwise would be to give in to hindsight, to allow the exact ex post reasoning against which the Supreme Court cautioned in *Graham* and *KSR*."); *see also KSR Int'l Co. v. Teleflex*

Inc., 550 U.S. 398, 421 (2007) ("Rigid preventative rules that deny factfinders recourse to common sense, however, are neither necessary under our case law nor consistent with it."); Ex. 2037 (Goodrich Decl.) at ¶45 ("Ramesh Kesanupalli was aware of TPMs but nonetheless chose not to use TPMs in the Kesanupalli reference. Ramesh Kesanupalli's design choices illustrate what a POSITA would have done and the reasons why a POSITA would have done so").

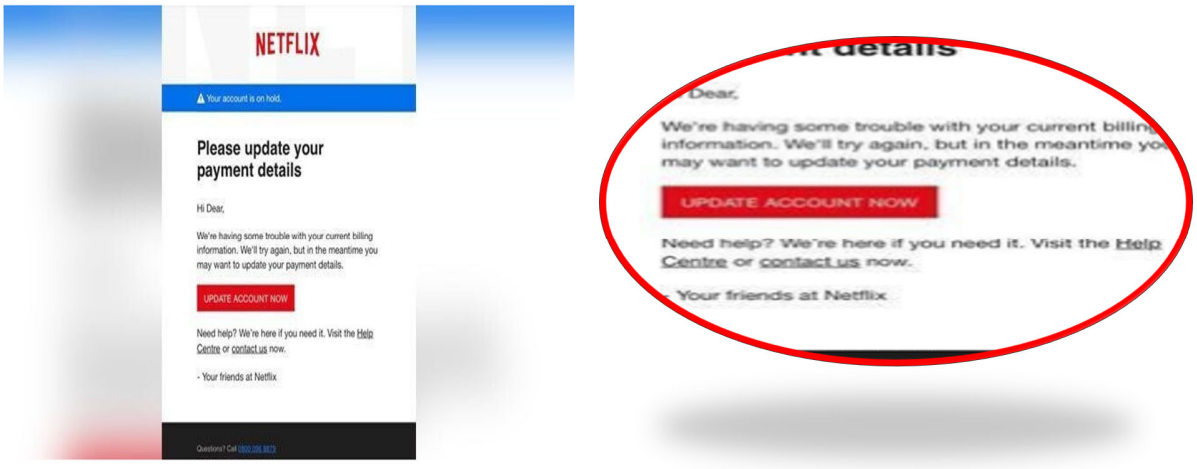
As discussed in the following sections, the unique facts presented in this Response preclude a finding that a POSITA would have been motivated to combine Kesanupalli with Challener. Ex. 2037 (Goodrich Decl.) at ¶¶45-64; *see, e.g.*, *In re Jones*, 958 F.2d 347, 350 (Fed.Cir. 1992) ("Every case, particularly those raising the issue of obviousness under section 103, must necessarily be decided upon its own facts."). The present facts overwhelming support a finding of not unpatenable.

2. The Kesanupalli reference was interested in curbing social engineering attacks and would not have benefited from a TPM such as the one taught by Challener.

To begin, Kesanupalli's concerns are not addressed by a TPM and a POSITA, like Mr. Kesanupalli, would have recognized this. Ex. 2037 (Goodrich Decl.) at ¶¶46-60. Kesanupalli was concerned with addressing social engineering attacks like phishing and spoofed websites. Ex. 1006 (Kesanupalli) at 1:35-37; Ex. 2037 (Goodrich Decl.) at ¶46. As Dr. Goodrich explains, these attacks do not depend on how securely information is stored on the actual device (such as by securing data

with a TPM) and instead depend on tricking the user to release their credentials to imposters or bad actors. Ex. 2037 (Goodrich Decl.) at ¶46 ("These attacks rely on tricking users to release credentials, which can occur by emailing or texting links to legitimate looking fake websites that a user enters personal information to thereby compromise their legitimate account.").

Tricking the user to release their credentials is typically done through email or text messages containing a link to a fake website that looks legitimate to convince the victim to enter their sensitive information. Ex. 2037 (Goodrich Decl.) at ¶¶47-50. For example, someone could trick a user by pretending to by Netflix and telling the user that they must log in and provide updated payment details to get their account off hold. If the user selects the update account now button, they will be redirected to an spoofed version of Netflix where the bad actor will collect the user's credentials.



Ex. 2037 (Goodrich Decl.) at ¶49-50 (citing Ex. 2049 (excerpted above)).

Dr. Goodrich provides a further details on this type of attack:

> The email is from an illegitimate source — a sender other than Netflix in this example (i.e., in fact not "Your friends at Netflix" as the email falsely states), but it nevertheless appears to be from a legitimate source. The email threatens the user by claiming "Your account is on hold." The email then claims there is an issue with billing information that needs to be updated. This message invites a user to fix the claimed issue by clicking the big red rectangle with the text "UPDATE ACCOUNT NOW." This button contains a link to an illegitimate website that impersonates the legitimate Netflix website. ***When a user is tricked into clicking this button***, the user enters sensitive information such as Netflix credentials and personal information (e.g., credit card information, address information, security question answers, etc.). The illegitimate source then has access to all this personal information. In many cases, the tricked user is unaware of the fact that they provided this sensitive information to an illegitimate source, which

> provides an illegitimate source with a longer window to exploit this sensitive information without detection.

Ex. 2037 (Goodrich Decl.) at ¶50 (emphasis added).

Bad password practices, such as the ones that Kesanupalli wants to discourage, are more vulnerable to phishing attacks / social engineering attacks. *See* Ex. 1006 (Kesanupalli) at 1:37-39 ("Typically, longer passwords with combinations of letters and numbers provide a higher level of security."); Ex. 2037 (Goodrich Decl.) at ¶51 ("These and other weak password practices (e.g., shorter passwords without combinations of letters and numbers) are more susceptible to phishing attacks, which the Kesanupalli reference aims to discourage").

To address these attacks, Kesanupalli wanted to promote the use of stronger passwords and it does this by binding credentials to biometrics and websites so that users can easily swipe a finger to autofill a credential on the correct website. Ex. 2037 (Goodrich Decl.) at ¶52 ("This enables a user to swipe a finger, which autofills credentials for a **legitimate** web site."). Instead of trying to remember multiple complex passwords, a user can store their login information in the safe environment (the fingerprint sensor) and easily use it with a single master biometric scan. Ex. 2037 (Goodrich Decl.) at ¶52. This reduces the temptation to use simple, easy-to-remember passwords, which are more vulnerable to phishing and other social

engineer attacks. Ex. 2037 (Goodrich Decl.) at ¶52. Further, the system discloses binding credentials to certain web addresses so that a user cannot be tricked to input their credentials on a fake website. *See* Ex. 1006 (Kesanupalli) at 4:36-5:58, 8:2-53; Ex. 2037 (Goodrich Decl.) at ¶¶53-54.

The integration of a TPM would not have helped avoid social engineering attacks. *See* Ex. 2037 (Goodrich Decl.) at ¶60. As Dr. Goodrich explains, adding a TPM would be "like adding gold plating to a toothpick. There is and was no reason or motivation for a POSITA to combine a TPM . . . with the Kesanupalli system." *Id*. This is because social engineering attacks are not about breaching the user device and accessing the credentials—presumably protected by a TPM; rather, these attacks are about tricking users to provide their credentials to bad actors or using common techniques such as a dictionary attack which exploit human psychology to gain access to a user's accounts. Ex. 2037 (Goodrich Decl.) at ¶60. Like gold plating a toothpick, the addition of the TPM adds nothing to achieving the goals of the original system.

During his deposition, Apple's expert, Dr. McDaniel, stated that the goal of TPM was to "provide[] a zone of security that is isolated from general processors." Ex. 2052 at 20-21. Dr. McDaniel provided many examples of issues that TPMs were meant to address, such as side channel attacks, insider against, and malware. *See* Ex. 2052 at 20-23. Not once did Dr. McDaniel state that a TPM was meant to address

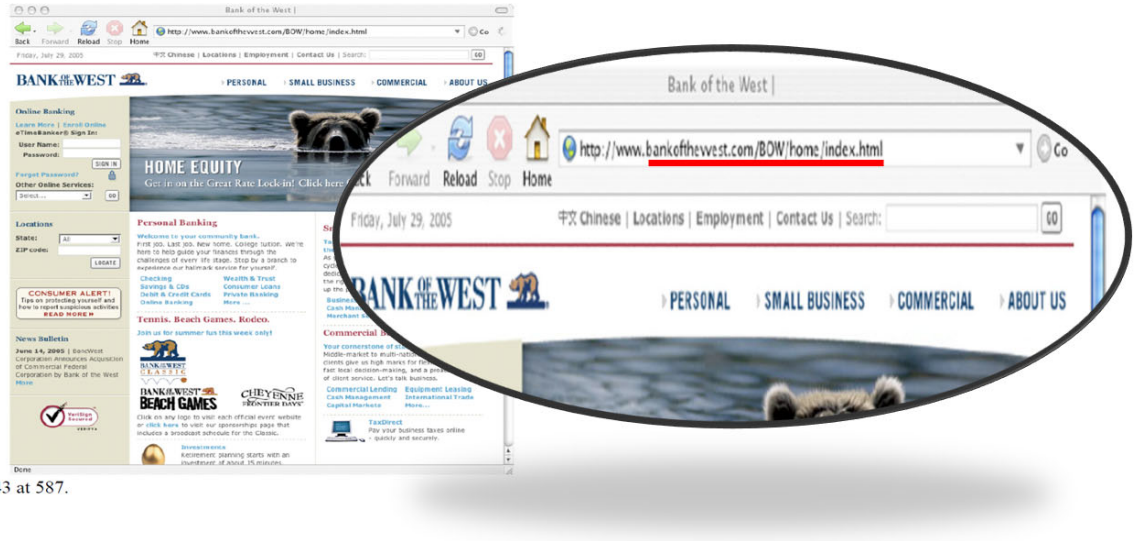
social engineering attacks because, again, those attacks are not about protecting the data on the device. Rather, Dr. McDaniel agrees, social engineering attacks are about tricking a user:

> Q) What are phishing attacks?
>
> A) Phishing attacks are where someone sends you some kind of communication, most often a kind of email that poses as somebody else and uses what we call social engineering to convince somebody to enter their passwords in a, say, a fake website.
>
> Q) So that is about tricking the user?
>
> A) Yeah, I mean, yes, I think that is fair to say.

Ex. 2052 at 31; *see also* Ex. 2053 at 5-6 (Apple's district court expert discussing that social engineering attacks are "typically one where a human psychology is manipulated in some way by an attacker.").

Kesanupalli discloses multiple ways to deter against different social engineering attacks. For example, one type of social engineering attack is an attack that spoofs a real website and tricks user's to input their account information into the spoofed website. *See* Ex. 2037 (Goodrich Decl.) at ¶47. Dr. Goodrich provides an

example of such an attack where "a fake web site address that looks at first to be that of the Bank of the West, but upon closer inspection one can see that the web address makes use of two "v"'s instead of a "w" in a web address URL." Ex. 2037 (Goodrich Decl.) at ¶48.



Ex. 2043 at 587.

Kesanupalli addresses this type of user tricking by binding the user's biometrics to the legitimate website URL. Ex. 2037 (Goodrich Decl.) at ¶52; Ex. 1006 (Kesanupalli) at 4:36-5:58, 8:2-53. Thus, if a user went to Bank of the VVest's (two V's) website, it the system would not release the Bank of the West's credentials because the URL would not match the bound URL.

Dr. Goodrich provides other examples of social engineering attacks such as dictionary attacks. Ex. 2037 (Goodrich Decl.) at ¶54. A dictionary attack exploits human psychology by "attempt[ing] to access an account through the use of a list of

common passwords." Ex. 2037 (Goodrich Decl.) at ¶54. This is one of the specific attacks mentioned by Kesanupalli that could be addressed by better password practices:

> Although passwords are commonly used to authenticate users, passwords are subject to various attacks. Such as phishing attacks, social engineering attacks, dictionary attacks and the like.

Ex. 1006 (Kesanupalli) at 35-41; *see also* Ex. 2052 at 30 ("Q) What is a dictionary attack? A) A dictionary attack is where the adversary has a precomputed set of passwords for sort of well-known or frequently used passwords, and then just simply uses that dictionary to – to identify what a particular password is.").

Kesanupalli explains that one way to curb dictionary attacks is to use "longer passwords with combinations of letters and numbers provide a higher level of security." *Id*. In order to promote better password practices, Kesaunpalli discloses allowing a user to use biometrics to retrieve and autofill passwords and credentials, which allows users to use more complicated passwords that they do not have to remember. Ex. 2037 (Goodrich Decl.) at ¶52 ("This occurs because users can choose passwords that are harder to remember without having to remember the passwords due to the fingerprint scan autofilling the password and the fingerprint (or other

biometric) being bound to the particular legitimate web site address. This results in beneficial effects because basic passwords are vulnerable to phishing attacks compared to more complex passwords, e.g., due to users reusing a simple password at multiple web sites or using passwords that are in password dictionaries."). By having more complicated passwords, the likelihood of a guessing or dictionary attack is decreased.

Social engineering attacks, such as dictionary attacks, do not require the device to be breached. Spoofing a website does not require installing malware on a device—just making the URL look similar to a real URL so that a user provides their credentials without thinking twice. Likewise, guessing and dictionary attacks do not require breaching the user device—just exploiting human psychology of using an easy to remember password. Accordingly, as Dr. Goodrich explains, a TPM would not be beneficial in curbing these types of attacks:

> Adding a TPM to the Kesanupalli reference would not aid in reducing such social engineering attacks because these social engineering attacks trick a user into providing their credentials to illegitimate sources or use prevalent techniques to breach common passwords. If a user is tricked to unlock their credentials, even using biometric data and a TPM, they could then send that data to a

> phishing web site; hence, the TPM provides no additional security to the Kesanupalli reference. . . As with a phishing attack based on a fake web site that is not bound to biometric data, a TPM would not aid in reducing dictionary social engineering attacks because the TPM is for device side security while social engineering attacks occur outside the device.

Ex. 2037 (Goodrich Decl.) at ¶54. Thus there is no reason for a POSITA to combine Challener's TPM with Kesanupalli's social engineering protections.

To the extent Petitioner argues that social engineering is not the concern of Kesanupalli, Petitioner is wrong. Beyond the explicit disclosures about social engineering attacks, the basic architecture of Kesanupalli demonstrates that Kesanupalli is only concerned with social engineering and not breaches to the actual device. Ex. 2037 (Goodrich Decl.) at ¶¶46-60. Consider Kesanupalli's enrollment process, which is depicted in Figure 11 (reproduced below). Ex. 1006 (Kesanupalli) at 2:2-21 ("FIG. 11 depicts another embodiment of a procedure for enrolling a user of a biometric authentication system."); Ex. 2037 (Goodrich Decl.) at ¶56. Here, the user's *biometrics* are being provided to the browser extension. Ex. 2037 (Goodrich Decl.) at ¶57.

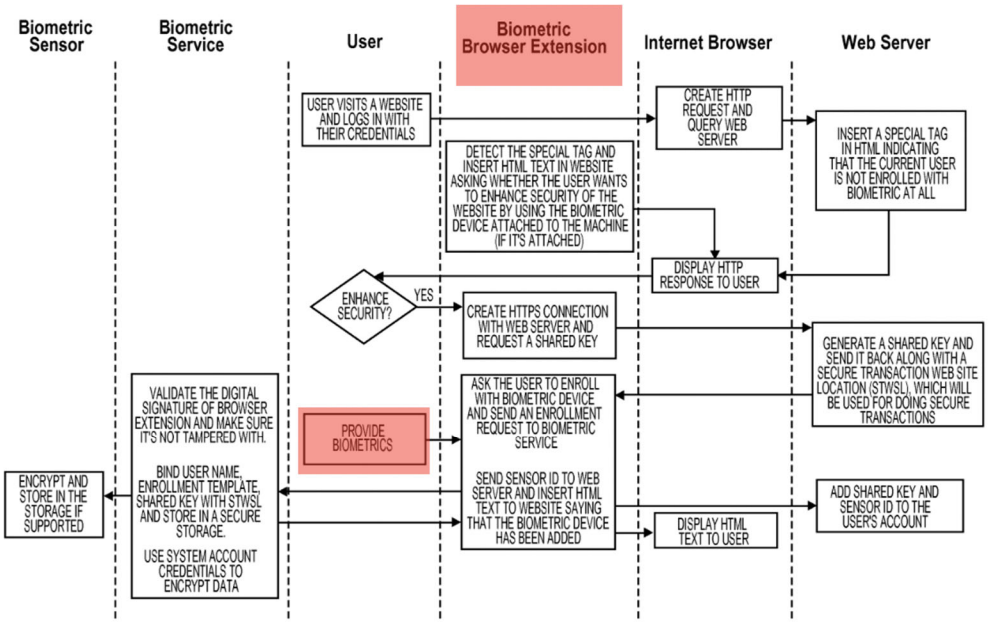


FIG. 11

Ex. 1006 (Kesanupalli) at Fig 11; *see also* Fig. 12 (providing the biometrics to the browser extension); Ex. 2037 (Goodrich Decl.) at ¶¶57-58. A POSITA reviewing Figure 11 would see that Kesanupalli provides biometrics from the user (third column) to the biometric browser extension (fourth column), meaning the biometrics are processed by the general processor, where all browser extensions run. Thus, malware on the device would be able to access the biometrics. But again, Kesanupalli was not concerned with bad actors ***breaching the device*** to get the credentials—Kesanupalli was worried about those bad actors ***tricking users*** for their credentials. Ex. 2037 (Goodrich Decl.) at ¶60.

Further demonstrating Kesanupalli's lack of concern for anything but social engineering attacks, Kesanupalli specifies that one type of credential is a cryptographic key (Ex. 1006 (Kesanupalli) at 3:41-44), which is communicated directly to a recipient website. *See* Ex. 1006 (Kesanupalli) at 4:3-11; Ex. 2037 (Goodrich Decl.) at ¶59. Kesanupalli highlights that this approach is secure because the key is not sent to an impostor site. Ex. 1006 (Kesanupalli) at 4:7-9; Ex. 2037 (Goodrich Decl.) at ¶59. In other words, the system is confirming that the user is sending their credentials to the actual website and not a faked version set up to trick the users to disclose their credentials. *Id*.

Yet as shown in Figure 12, it is the biometric browser extension that sends the credential to the web server. Ex. 2037 (Goodrich Decl.) at ¶58.

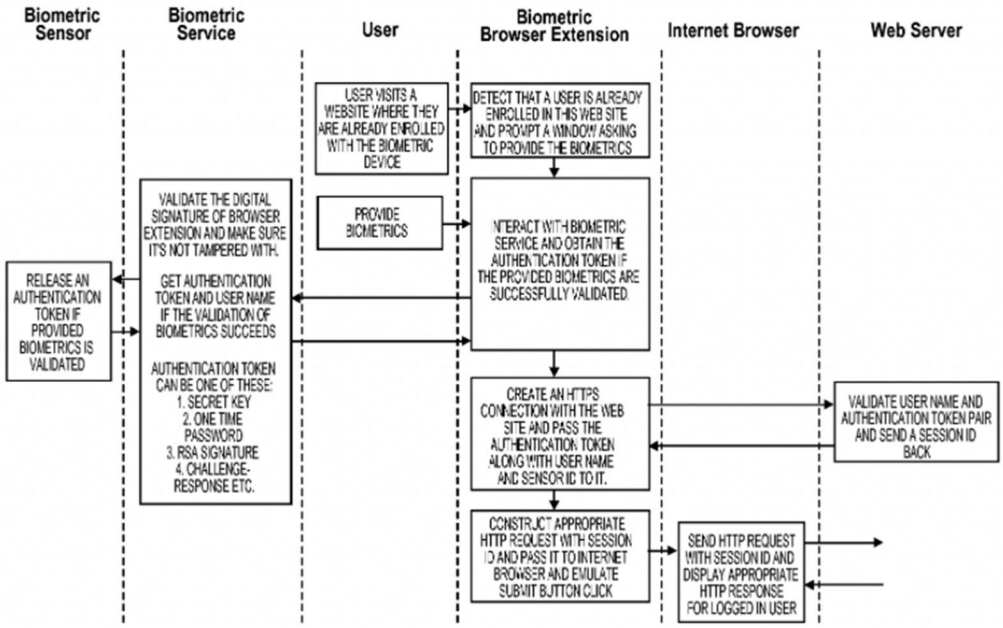


FIG. 12

Ex. 1006 (Kesanupalli) at Fig. 12. Again, this shows that Kesanupalli is comfortable with providing sensitive information, such as biometrics and cryptographic keys, to the browser extension executing on the device's general processor. Ex. 2037 (Goodrich Decl.) at ¶59. If the device was breached by a bad actor, this process would make the credentials available to the bad actor, but again, this wasn't the concern of Kesanupalli. Ex. 2037 (Goodrich Decl.) at ¶59.

Kesanupalli's concern was curbing social engineering attacks and not breaches to the actual device. Adding a TPM just to add a TPM would be like "gold plating a toothpick"—it can be done, but it doesn't address the problem a toothpick was designed to address. Ex. 2037 (Goodrich Decl.) at ¶59; *see Virtek Vision Int'l*

ULC v. Assembly Guidance Sys., Inc., 97 F.4th 882, 887 (Fed. Cir. 2024) ("The mere fact that these possible arrangements existed in the prior art does not provide a reason that a skilled artisan would have [done it]"); *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367 (Fed. Cir. 2016).

Petitioner, through its lawyers and an expert more than 14 years after the filing of the references, cannot overcome the fact that a POSITA made a conscious decision to *not* use a TPM since it would have no impact on curbing social engineering attacks. Ex. 2037 (Goodrich Decl.) at ¶59. Petitioner's argument thus faces a "logical chasm—a chasm not bridged by the prior art [or] common sense." *St. Jude Med., Inc. v. Access Closure, Inc.*, 729 F.3d 1369, 1381 (Fed. Cir. 2013) ("Even under our "expansive and flexible" obviousness analysis . . . we must guard against 'hindsight bias' and 'ex post reasoning'"). Kesanupalli decided to confront social engineering attacks with his system and a POSITA given the disclosures of the reference would not have been motivated to add a TPM as it would not have added any additional benefit to the user. Ex. 2037 (Goodrich Decl.) at ¶60.

3. Using a TPM had drawbacks that a POSITA would have been aware of.

Beyond Kesanupalli's concerns with social engineering, which would not have been prevented by the addition of a TPM, the decision to exclude Trusted Platform Modules (TPMs) from Kesanupalli would also have been influenced by

several practical considerations related to their adoption and deployment. Ex. 2037 (Goodrich Decl.) at ¶61.

First, utilizing a TPM would have introduced compatibility issues with existing systems and software that did not support TPMs. Ex. 2037 (Goodrich Decl.) at ¶62; *see* Section III.A.2, *supra*. Many security solutions that did not rely on TPMs were available and widely adopted. Ex. 2037 (Goodrich Decl.) at ¶62. Kesanupalli for example, preferred embodiment used the Windows Biometric Framework (WBF), WBF Interface, and the WinUSB driver. *See* Ex. 1006 (Kesanupalli) at 5:59-6:10; Figs. 1 and 2; Ex. 2037 (Goodrich Decl.) at ¶63. The Windows Biometric Framework did not require or even mention a TPM. *See generally* Ex. 2050; Ex. 2037 (Goodrich Decl.) at ¶63. This is likely because TPMs were not required by Windows in 2012 and TPMs were disabled by default. Ex. 2037 (Goodrich Decl.) at ¶63; *see* Section II.C, *supra*.

Second, since the TPM's were not turned on by default, utilizing TPMs would have required end users to make firmware changes to even enable the TPM to work. A POSITA (like Mr. Kesanupalli) aiming to address the risk of social engineering (which again would not have benefited from a TPM) would not have wanted to further deter users from using the patented system by requiring them to set up and configure a TPM. Ex. 2037 (Goodrich Decl.) at ¶63.

At bottom, there are a myriad of reasons why Mr. Kesanupalli did not include a TPM in his patented system and why the Board should not rewrite history and add one now. Ex. 2037 (Goodrich Decl.) at ¶¶44-64.

B. The Petition fails to show the combined Cheng with Challener/Kesanupalli discloses "second processor configured to" (claim 1.7) "perform a secure backup of the record to a storage service" (claim 1.7A).

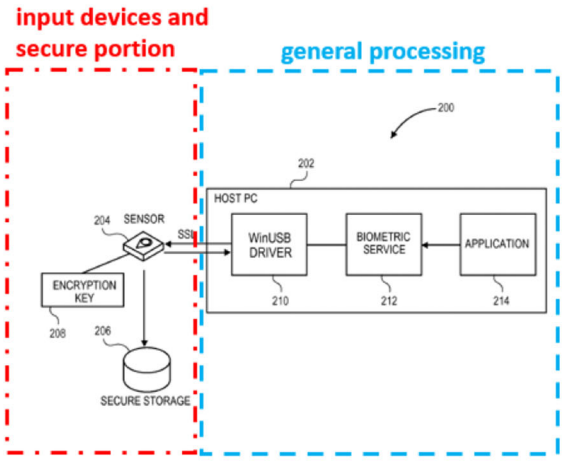
Petitioner has failed to show that (1) the TPM/Sensor of Kesanupalli/Challener combined with Cheng meets this limitation and that (2) a POSITA would have had a reasonable expectation of success combining Cheng with the system architecture of the Kesanupalli/Challener TPM based system. Ex. 2037 (Goodrich Decl.) at ¶65.

Here, the Board is faced with another unique situation. With respect to TPMs there are few POSITAs like Dr. Challener. Ex. 2037 (Goodrich Decl.) at ¶65; *see* Section II.B.1, *supra*. Petitioner states that changing the Challener's TPM to incorporate Cheng's backup method "would have been straightforward for POSITA to implement including widely practiced porting of code to a TPM environment. *Id*; APPL-1019 (describing secure backup protocol elements from TCG standardization and implemented in a TPM), APPL-1017 (showing porting)." Pet. 55. Yet, Petitioner does not show a *single* application of a TPM backing up its records to a storage service and certainly no reference from Dr. Challener who was incredibly

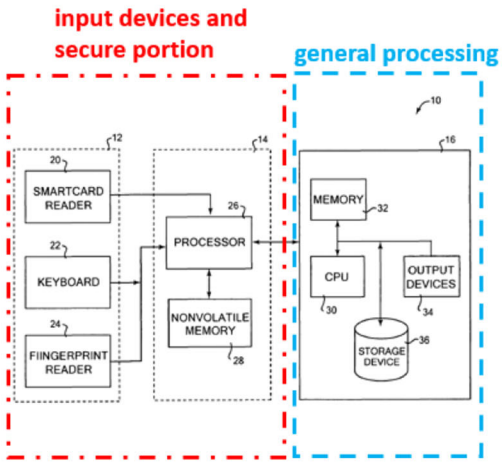
knowledgeable about TPMs. Ex. 2037 (Goodrich Decl.) at ¶65; *see* Section II.B.1, *supra*. This is because not only does the combination fail to do it, but it would have been difficult to make the system work while keeping the TPM data safe. Ex. 2037 (Goodrich Decl.) at ¶65.

1. Petitioner has failed to show a "second processor configured to" (claim 1.7) "perform a secure backup of the record to a storage service" (claim 1.7A).

The combination of Kesanupalli/Challener with Cheng does not disclose a "second processor configured to" (claim 1.7) "perform a secure backup of the record to a storage service" (claim 1.7A). Petitioner's architecture of the Kesanupalli/Challener system is reproduced below:



Kesanupalli, FIG. 2, Annotated



Challenger, FIG. 1, Annotated

Pet. 20. In this system, Petitioner has taken the Challener TPM secure portion and incorporated it into the sensor of Kesanupalli. Pet. 20; Ex. 2037 (Goodrich Decl.) at

¶ 66. Petitioner points to the TPM/Sensor as the "second processor" that the claims explicitly require "*perform[s]* a secure backup of the record *to* a storage service."

However, there is no disclosure that TPM/Sensor of Kesanupalli/Challener is the processor *performing* the secure backup *to* a storage service. As Petitioner states time and time again, and one of the main reasons Petitioner believes that a POSITA would have combined Kesanupalli/Challener is because the TPM of Challener is isolated so as to keep its contents secure. Pet. 21("[A] POSITA would have been motivated to implement Kesanupalli's functionality on Challener's TPM architecture using a specialized security processor (e.g., Challener's security processor 26 including its APIs) to isolate the secure functions of Kesanupalli's sensor 204 and secure storage 206, while hosting on a general processor (Challener's microprocessor 30) the applications and other functions of Kesanupalli's Host PC 202. APPL-1003, ¶79"); Ex. 2037 (Goodrich Decl.) at ¶67. The TPM/Sensor is isolated and it is not connected to any external storage service—the only thing it can do is communicate with the "general" processor, which would then be the processor "performing" any secure backup "*to* a storage service." Ex. 2037 (Goodrich Decl.) at ¶66.

Petitioner's combination with Cheng does not change the change the underlying Kesanupalli/Cheng architecture that limits what can access the secure portion and what would be doing the backup. Ex. 2037 (Goodrich Decl.) at ¶67; *See,*

e.g., Pet. 38 ("Such restrictions limit access and thereby protect the **functions and data in the security portion of a TPM-based security architecture** (e.g., sensor 204 and the secure storage 206) from being misused by an untrusted or malicious program."). The sensor connects *only* to the Host PC 202 via a SSL connection. *See* Ex. 1006 (Kesanupalli) at 6:39-45 ("The biometric sensor 204 creates a secure communication with Host PC202 using SSL v3 protocol or other secure communication technique."); *see also id.* at Figs. 1-2; Ex. 2037 (Goodrich Decl.) at ¶67. Thus, even if Cheng is added, the TPM/Sensor of Kesanupalli/Cheng is not the processor that will be backing up anything "to" a storage service as it is only connected to the Host PC via the SSL connection Ex. 2037 (Goodrich Decl.) at ¶67 ("Combining the Cheng reference with the Kesanupalli and Challener references does not change that the general processor – as opposed to the TPM and sensor combination – would be the processor that actually performs a backup to a storage service.").

To the extent that Petitioner argues that second processor does not need to be the processor doing the backup "to" the storage service to "perform the secure backup", Petitioner is incorrect. Ex. 2037 (Goodrich Decl.) at ¶¶68-69. Compare the language of limitation 1.6B, which requires the second processor to "*facilitate* a login of the user to the external resource," to the present language which requires that the second processor "perform *a secure backup of the record to a storage*

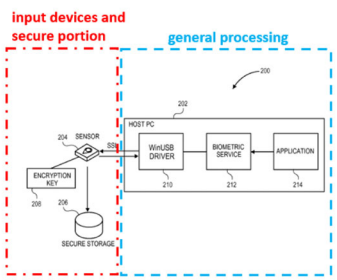
service." Ex. 2037 (Goodrich Decl.) at ¶¶68-69. In the former, the second processor need only *facilitate* an action that the first processor can finish. Ex. 2037 (Goodrich Decl.) at ¶¶68-69. In the later, the second processor needs to *perform* a secure back up of the record up "to" a storage service. The Kesanupalli/Cheng TPM/Sensor does not do that even with the teachings of Cheng. Ex. 2037 (Goodrich Decl.) at ¶¶68-69.

2. A POSITA would not have reasonably expected the Cheng backup to work with the Kesanupalli/Challener TPM architecture.

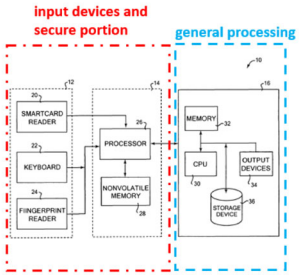
It is Petitioners' burden to "to demonstrate that the skilled artisan would have had a reasonable expectation of success in combining references." *KEYnetik, Inc. v. Samsung Electronics Co., Ltd*., 841 Fed.Appx. 219, 227-228 (Fed. Cir. 2021) (internal quotations omitted). Petitioners have not met their burden with respect to combing Cheng with Kesanupalli/Challener. Ex. 2037 (Goodrich Decl.) at ¶70.

In a single paragraph Petitioners allege that a POSITA would have a had a reasonable expectation of success "in adding backup feature such as taught by Cheng in a biometric authentication system such as taught by Kesanupalli in view of Challener." Pet. 26. Petitioner's *single* reason is that "[a]dding a backup feature would merely have been applying a known technique to a known device (method, or product) ready for improvement to yield predictable results." *Id*. But this conclusory single reason fails to consider how the backup method would be added to the Sensor/TPM architecture. Ex. 2037 (Goodrich Decl.) at ¶¶70-71.

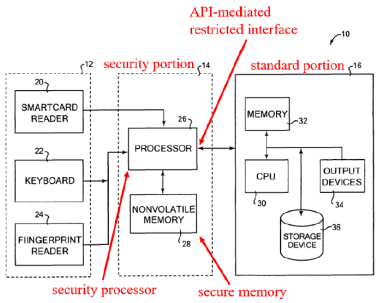
As discussed above, access to the TPM is restricted so as to keep its content safe from unauthorized access. *See, e.g.*, Pet. 36 ("TPM-based implementation, are widely recognized examples of a security architecture that provides a restricted interface in the form of an access limiting API to restrict access to the TPM (secure processor, here second processor) by programs running on a general processor (here first processor) in a standard (non-secure) portion of a system."); Ex. 2037 (Goodrich Decl.) at ¶71. The annotated figures from the Petition demonstrate the isolation.



Kesanupalli, FIG. 2, Annotated



Challenger, FIG. 1, Annotated



APPL-1007, FIG. 1, annotated

Pet. 20 and 14.

The TPM/Sensor (input and secure portion above) is not connected to any backup service. Ex. 2037 (Goodrich Decl.) at ¶71; *see* Section II.C, *supra*. Petitioner has not shown, let alone with a reasonable expectation of success, how modifying the TPM/Sensor architecture of Kesanupalli/Challener could be done in a way that would permit the TPM/sensor to maintain its "restricted access" but allow the TPM sensor to communicate with more than the Host PC general processing section, such as a backup service. Ex. 2037 (Goodrich Decl.) at ¶71 ("Petitioner's omission is a

glaring, because it is very difficult to maintain a TPM's high level of security (that is tied to its isolation) while simultaneously communicating its sensitive contents to a backup storage service that is inherently not isolated.").

As it did in its Preliminary Reply, Petitioner may argue in response that this is a bodily incorporation argument. Reply at 4-5. Patent Owner disagrees. Patent Owner's argument is not that these systems cannot be physically combined; rather, that Petitioner's *single* reason is that "[a]dding a backup feature would merely have been applying a known technique to a known device (method, or product) ready for improvement to yield predictable results" does not prove that a POSITA would have had an expectation of success making this combination work. *See Juniper Networks, Inc. v. Correct Transmission, LLC,* No. 2023-1046, 2024 WL 3517862, at *6 (Fed. Cir. July 24, 2024) ("Nonetheless, it was Juniper's burden to offer proof that the combination could be made with a reasonable expectation of success. In this case, Dr. Akl's testimony rebuts Juniper's theory that a POSA would have a reasonable expectation of success because the required combination was simple. Juniper's evidence that making the combination would be "very simple" was found not credible. . . It was Juniper's burden to establish a reasonable expectation of success, and Juniper presented no theory other than that the combination was simple.") (citations omitted). Simply saying it could have been done because it's a known technique does not meet Petitioner's burden. This is especially true when the point

of a TPM is to restrict access to its contents and Petitioner is attempting to open up access to that TPM.

C. Even if combined, the Petition fails to show that the defendant claims 2 and 12 are unpatentable in light of Kesanupalli, Challener, and Cheng.

1. Kesanupalli, Challener, and Cheng do not teach or suggest "[t]he system recited in claim 1, wherein the storage service comprises a cloud storage service" (claim 2) and (claim 12).[1]

Petitioner points to Cheng's disclosure of an "internet-based storage service." Pet. 60 (citing APPL-1008, [0029]). Petitioner adds that a "POSITA would recognize that an internet-based storage service is a cloud storage service. APPL-1003, ¶182; APPL-1021 showing geographically dispersed services." *Id*. This argument highlights the issues of adding Cheng to Kesanupalli/Challener. Ex. 2037 (Goodrich Decl.) at ¶¶72-73; *see* Section III.A-B, *supra*.

Claim 2 requires the "second processor perform a secure back up to" (claim 1) "a cloud storage service" (claim 2); Ex. 2037 (Goodrich Decl.) at ¶¶72-73. As discussed in claim 1, the Kesanupalli/Challener TPM/Sensor is not connected to anything but the host PC via an SSL connection. Ex. 2037 (Goodrich Decl.) at ¶73;

[1] Claim 12 is a similar dependent claim to claim 2 but limited to the method of claim 11.

see Section III.A-B, *supra*. The TPM/Sensor is not configurable to "*perform* a backup *to*" a "cloud storage service" such as an internet-based storage. Ex. 2037 (Goodrich Decl.) at ¶73; *see* Section III.B.1, *supra*. Only the general processing area of the Kesanupalli system on the host pc would be able to an internet-based storage service. Ex. 2037 (Goodrich Decl.) at ¶73. The Kesanupalli/Challener TPM/Sensor "second processor" thus does not and cannot meet this limitation. Ex. 2037 (Goodrich Decl.) at ¶73.

D. Independent Claims 11 and 21 are not invalidated by Kesanupalli, Challener, and Cheng.

Claims 11 and 21 are similar to claim 1 outside of their respective preambles. Pet. 71; Ex. 2037 (Goodrich Decl.) at ¶74. And the Petition states that "[d]ependent claims 12–16 and 20 are substantively identical to claims already addressed" (Pet. 69). These claims are not invalidated for the same reasons as discussed above. Ex. 2037 (Goodrich Decl.) at ¶74; *see* Section III.A-C, *supra*.

IV. CONCLUSION

For any or all of the above-described reasons, Patent Owner respectfully requests that the Board find all claims of the '512 Patent valid.

Dated: October 8, 2024

Respectfully submitted,

/s/Richard A. Kamprath
Richard A. Kamprath
Reg. No. 65,320
rkamprath@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 RESPONSE** specified in 37 C.F.R. §42.24 have 7,722 words, in compliance with the 14,000 word limit set forth in 37 C.F.R. §42.24(b)(1). This word count was prepared using Microsoft Word 2010.

Dated: October 8, 2024

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 RESPONSE PURSUANT TO 37 C.F.R. § 42.10(b)** has been served on Petitioner via email on the following counsel of record for Petitioner:

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

Kelly Gehrke Lyle
Kelly.lyle@haynesboone.com

Hong Shi
Hong.shi.ipr@haynesboone.com

Dated: October 8, 2024

Respectfully submitted,

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