UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Samsung Electronics Co., Ltd.,

Petitioner,

v.

Ward Participations B.V.,

Patent Owner.

PGR2022-00007
Patent 10,992,480

PATENT OWNER WARD PARTICIPATIONS B.V.'S PRELIMINARY RESPONSE TO PETITION FOR POST GRANT REVIEW OF U.S. PATENT NO. 10,992,480

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

PAGE

Cases

Statutes

Patent Owner's Exhibit List

Exhibit No.	Description
2001	Declaration of Bart Preneel, Ph.D.
2002	Remarks of December 23, 2020, Amendment and Response for U.S. Patent Application No. 16/597,773
2003	December 22, 2020, USPTO Examiner Interview Summary
2004	September 18, 2020, Final Office Action for U.S. Patent Application No. 16/597,773
2005	December 17, 2020, USPTO Examiner Interview Summary
2006	*Curriculum Vitae* of Bart Preneel, Ph.D.
2007	Europass *Curriculum Vitae* of Bart Preneel, Ph.D.
2008	Publication List of Bart Preneel, Ph.D.

I. INTRODUCTION TO THE PROCEEDING

Pursuant to 35 U.S.C. §323 and 37 C.F.R §42.207, Patent Owner Ward Participations B.V. ("Patent Owner") respectfully submits the following Patent Owner's Preliminary Response ("Preliminary Response") to the petition for post-grant review ("Petition") of claims 1-19 of U.S. Patent No. 10,992,480 to Ward *et al.* (the '480 Patent", Exhibit 1001), Case No. PGR2022-00007. On November 22, 2021, the Board mailed a Notice of Filing Date Accorded to Petition. As this Preliminary Response is being submitted January 31, 2022, Patent Owner's Preliminary Response is timely pursuant to 37 C.F.R. §§1.7, 42.1, 42.207.

II. LISITING OF FACTS

The Petition did not include a Statement of Material Facts to be Admitted or Denied.

III. THE '480 PATENT IS NOT ELIGIBLE FOR PGR

The '480 Patent is not eligible for PGR because the invention claimed has § 112 support in a Dutch Application PCT/NL03/00436, filed June 13, 2003. '480 Patent, Cover. The Petitioner bears the burden to show that a patent is eligible for PGR. *See Mylan Pharms. Inc. v. Yeda Res. & Dev. Co.*, Case PGR2016,00010, Paper No. 9, Denial of Institution at 10 (PTAB Aug. 15, 2016) . In order for a patent to be eligible for PGR, Petitioner must show that at least one claim has a priority date after March 16, 2013. *Fox Factory, Inc. v. SRAM, LLC*, PGR-2016-

00043, Paper No. 9, Denial of Institution at 7 (PTAB April 3, 2017). Here, Petitioner has failed to meet that burden.

To show that the claims have a priority date after March 16, 2013, despite the earlier filing, Petitioner must identify, "specifically, the features, claims and ancestral applications allegedly lacking § 112 . . . support for the claims based on the identified features." *See e.g., Polaris Wireless, Inc. v. TruePosition, Inc.*, IPR2013-00323, Paper No. 9, Institution Decision at 29 (PTAB Nov. 15 2013);; *Amazon.com, Inc. v. Personalized Media Communications, LLC*, IPR2014-01533, Paper No. 7, Institution Decision at 11-16 (PTAB Mar. 26, 2015) (finding priority date from an earlier application where "Petitioner has failed to establish that the priority date" was later).

The '480 Patent claims priority to a filing that dates to June 13, 2003. This filing date significantly predates March 16, 2013. Moreover, the U.S. Patent application for the '480 Patent was examined under pre-AIA first to invent provisions. *See e.g.*, Ex. 2004, p. 2.

A patent gains the benefit of an earlier filed application under 35 U.S.C. § 120 when each application in the chain leading back to the earlier application complies with the written description requirement of 35 U.S.C. § 112(a). *Zenon Envtl. Inc., v. U.S. Filter Corp.*, 506 F.3d 1370, 1378 (Fed. Cir. 2007). Here, as will be discussed in further detail in Section V, the '480 Patent and the earlier filed

applications in the patent chain comply with the written description requirement of § 112(a). Therefore, Petitioner is required to address every disclosure in the chain and explain how a person of ordinary skill in the art ("POSITA") would interpret the disclosure prior to March 16, 2013. Petitioner has not done this.

Instead, Petitioner broadly asserts that the '480 Patent does not have written-description support in an application filed before March 16, 2013. This assertion is made despite Petitioner's acknowledgement that the feature which is allegedly unsupported is in fact supported by the disclosure. *See* Petition at 14 (stating [t]he '480 Patent teaches that the authentication software may have its own private encryption key.").

Accordingly, Petitioner has failed to meet its burden to show that the '480 Patent is eligible for PGR and the Petition should not be granted.

IV. PETITIONER MISREPRESENTS A EUROPEAN PROCEEDING THAT HAS ABOSLUTELY NO BEARING ON THE PATENTABILITY OF THE '480 PATENT

Petitioner begins its argument regarding the written description requirements under 35 U.S.C. § 112(a) by conflating European patent law (with its own set of differing standards) with United States patent law and cherry-picking European provisional rulings for its benefit. However, even if Petitioner's characterization of the European proceedings were correct (they are not), none of the European

proceedings are relevant to the written description patentability requirements of a United States Patent.

Petitioner first argument against whether the '480 Patent claims satisfy the written description requirement of 35 U.S.C. § 112(a) is that claims in corresponding European patents were held invalid for a lack of similar support. Petition at 11. This is curious because the determinations by European courts with respect to European patent law of European patents is not a consideration for the patentability of U.S. Patents under United States Patent law. More importantly, it is also a blatant misrepresentation of the proceeding in Europe.

The proceedings before the district court of The Hague ("DCTH") in the Netherlands concerned infringement of European Patents EP 1 634 140 ("EP140") and EP 3 229 099 ("EP099") by Samsung Electronics Benelux B.V., Samsung Electronics Europe Logistics B.V., and Samsung Electronics Overseas B.V. Ex. 1015, p. 1–3.

Petitioner alleges that the DCTH invalidated the European patents. This allegation is not supported by the decision of the DCTH. The DCTH implicitly and explicitly did **not** decide on the validity of the European patents of the listed countries outside the Netherlands. Ex. 1015, p. 44, ¶5.50. In contrast, the DCTH (1) reserved all further judgement and suspended both proceedings and (2) decided

that either party may bring the case or cases on the continuation role, as appropriate. The DCTH stated:

> 5.50. As the assessment of the alleged patent infringement **on foreign parts of EP 099 and EP 140 is subject to the opinion of the competent courts of the countries listed in 2.3** ***with regard to the validity of these parts***, the District Court will reserve all further judgment in both cases *and suspend both proceedings*. Most diligent party may bring one or both cases in the continuation role as soon as one or more final decisions of competent foreign courts on Samsung's and others' invalidity objections against EP 099 and/or EP 140 are known or it is certain that DTS will not be able to enforce the patents in the countries where they have been granted.

Ex. 1015, p. 44, ¶5.50. The countries listed in 2.3 are "Netherlands, Belgium, Switzerland, Germany, Denmark, Spain, Finland, France, United Kingdom, Ireland, Italy, and Sweden." Ex. 1015, p. 4, ¶2.3.

In contrast to Petitioner's allegation that the European patents were invalidated for lacking written disclosure support, the proceedings of EP099 and EP140 were merely suspended ***as it pertains to the Netherlands***. The DCTH made no determination on the validity of EP099 and EP140 with respect to any of the other European countries.

Petitioner continues on and states "in related European proceedings, the European Patent Office issued additional opinions that similarly held 'that the

subject-matter of the patent [EP 140 and EP 099] appears to extend beyond the content of the earlier application as filed'." Petition at 13. This assertion is also not supported by the communication from the EPO.

The Opposition Division ("OD") of the European Patent Office in Munich, Germany issued two separate summons on May 25 and May 27, 2020, respectively for EP 140 and EP 099. EX 1016, 1017. This was in preparation of the oral proceedings called by Samsung Electronics Benelux B.V. in light of their submitted oppositions to EP 099 and EP 140. Ex. 1016, p. 3, sheet 1; Ex. 1017, p. 2, sheet 1. The summons contained "***provisional, non-binding opinion[s]"*** of the OD based on the positions adopted by the parties, not by any independent analysis done by the OD. Ex. 1016, p.6, sheet 4; Ex. 1017, p. 5, sheet 4. In terms of the "subject-matter" issue, the provisional findings of the summons were **not** aligned with each other.

For example, the EP 099 summons stated:

> The provisional opinion of the Opposition Division is therefore that the subject matter of the patent appears to extend beyond the content of the earlier application as filed. **Depending on the results of the discussion concerning the points mentioned above**, it will have to be assessed whether the subject-matter of the patent extends beyond the content of the application as filed **or not**.

Ex. 1017, p. 16, sheet 15, ¶15.

> The Opposition Division refers to point 6.7 above. Here also the objections made by the Opponent appear to be of similar nature as those concerning the extension of subject-matter compared to the earlier application. **The discussion concerning this argumentation will therefore depend on the results of the one concerning extension of subject-matter**.

Ex. 1017, p.18, sheet 17, ¶21.1.3. The EP 140 summons stated:

> As a conclusion, although most of the features of the claims appear to have some basis in D2, it is not always immediately apparent whether the presently claimed combinations (including mixing of different embodiments) can be derived directly and unambiguously from the originally filed application. The **provisional opinion** of the Opposition Division is therefore that the subject-matter of the patent appears to extend beyond the content of the application as filed.

Ex. 1016, p. 16, sheet 14, ¶18, emphasis added.

Thus, Petitioner's attempt to categorize the entirety of the European patent validity into one line from one of two provisional opinions is misguided. Patent Owner respectfully submits that the above-noted opinions of the OD were provisional and non-binding, a qualification that Petitioner omitted from the remarks in the Petition. Moreover, the decision by the OD came at the end of June 2021, after the oral proceedings on June 23 and June 24, 2021, well **after** the '480 Patent was granted. Ex. 1018, p. 1; Ex. 1001, Cover.

This is important because Petitioner alleges that the U.S. Examiner was not informed of the European proceedings. Petition at 11, 13. However, the U.S. Patent Examiner need not be informed of Dutch litigation on European patents and provisional opinions of a pending (at the time of prosecution) proceeding in Munich because these are not material to the patentability of a U.S. application under 37 C.F.R. § 1.56(b) with entirely different patentability standards than Europe. Moreover, at the time the '480 Patent issued on April 27, 2021, there was no provisional decisions by the OD and therefore nothing that needed to be brough to the USPTO Examiner's attention.

Accordingly, Petitioner's reliance on provisional, non-binding decisions regarding European patents has no relevance to the patentability of the '480 Patent. Additionally, Petitioner's allegations are unsupported and substantiated because the European decisions were provisional and limited to the Netherlands. Finally, Petitioner's insistence that the European decision be reported to the United States Patent Examiner are unfounded in any relevant legal authority and are also irrelevant because the '480 Patent had already issued by the time the OD decision came out.

V. THE CHALLENGED CLAIMS ARE PATENTABLE AND SATISFY THE REQUIREMENTS OF 35 U.S.C. § 112

Institution of PGR may only be authorized where "the information presented in the petition filed under section 321, if such information is not rebutted, would demonstrate that it is **more likely than not** that at least 1 of the claims challenge in the petition is unpatentable." 35 U.S.C. § 342(a), emphasis added.

The Petition should be denied as to each of the challenged claims for at least the following reasons: (i) Claims 1-19 of the '480 Patent are patentable under 35 U.S.C. § 112; (ii) neither Ellison nor Muir teach or suggest a decryption key for decrypting the private key (used by the first transaction party to digitally sign a transaction) being incorporated in the electronic device; (iii) neither Ellison nor Muir teach or suggest authentication software is stored in said secure memory inaccessible to said operating system; (iv) neither Ellison nor Muir teach or suggest authentication software is run in a secure processing environment inaccessible to said operating system; and (v) Al-Saqan and Searle do not overcome the above deficiencies relating to the combination of Ellison and Muir.

Petitioner calls for the Board to consider 1 alleged ground of unpatentability based on the written description requirement of 35 U.S.C. §112(a) and 3 alleged grounds of unpatentability based on 4 different references applied in various ways.

Petitioner's arguments in Ground A1 rely on Petitioner's dissatisfaction with the "manner" in which the '480 Patent describes claim features despite full support for the '480 Patent claim features in the specification. Petition at 14.

Moreover, with respect to Grounds B1-B3, a resolution favorable to the Patent Owner does not require the complexity suggested by the Petition. In fact, the Petition must be denied if the Patent Owner prevails any of reasons (ii), (iii), or (iv) above, because all grounds B1-B3 for unpatentability set forth by Petitioner require the combination of Ellison and Muir. For the reasons set forth *infra*, the Petition fails in each of these respects and, therefore, must be denied.

Petitioner's reliance on a proposed combination of Ellison and Muir is supported by improperly interchanging words contrary to both their meaning and the respective disclosures in an attempt to mask a failure of both Ellison and Muir to disclose elements of Patent Owner's claims. This reason alone is sufficient grounds for the failure of Ellison and Muir to teach the obviousness of Patent Owner's features. Accordingly, Ground B1 of the Petition must fail.

If the Board denies Ground B1 of the Petition for the reasons set forth above, then there is no need for it to address Patent Owner's arguments herein concerning Al-Salqan and Searle (*i.e.*, above-noted reason (v)). However, as discussed *infra*, Ground B2-B3 should be independently denied, because Al-Salqan and Searle fail to overcome the deficiencies of the combination of Ellison and Muir, as set forth above.

In view of all the foregoing, the Petition should be denied.

VI. GROUND A1 FAILS BECAUSE THE CLAIMS OF THE '480 PATENT SATISFY THE WRITTEN DESCRIPTION REQUIREMENT UNDER 35 U.S.C. §112

Each and every claim in the '480 Patent is fully supported in the specification. Petitioner does not allege that the claims as a whole are not supported. Rather, Petitioner asserts that the claims do not meet the written description requirement solely because the private key limitation, which was added as a result of a **suggestion by the Examiner** (Ex. 2005, p.2), is not disclosed in the manner Petitioner desires. Petition at 14. However, literal disclosure is not required.

Courts have long recognized that the "[T]he hallmark of written description is disclosure." *Ariad Pharma. Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010). "The standard for satisfying the written description requirement is whether the disclosure 'allows one skilled in the art to visualize or recognize the identity of the subject matter purportedly described.'" *Alcon Research Ltd. v. Barr Labs., Inc.*, 745 F.3d 1180, 1190 (Fed. Cir. 2014) (*quoting Enzo Bichem, Inc. v. Gen-Probe Inc.*, 323 F.3d 956, 968 (Fed. Cir. 2002)). The disclosure is sufficient if it "reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date," based on an "objective inquiry into the four corners of the specification." *Ariad Pharma*, 598 F.3d at 1351.

Here, Petitioner admits that the specification includes description of a private key, including that "[t]he '480 Patent teaches that the authentication software may have its own private encryption key." Petition at 14. Petitioner further acknowledges the '480 Patent's reference to the private key being able to sign a digital signature or be "any other application identifying character string." Petition at 15 (*quoting '480 Patent*, 13:31–44). Moreover, Petitioner acknowledges an embodiment disclosed in the '480 Patent including a private key. Petition at 15 (*quoting '480 Patent*, 13:31–33). As the PTAB has stated, the embodiments in the specification need not literally match those of the claims. *See Fox Factory*, PGR-2016-00043, Paper No. 9 at 7 ("However, 'that a claim may be broader than the specific embodiment disclosed in a specification is in itself of no moment'") *quoting In re Rasmussen*, 650 F.2d 1212, 1215 (CCPA 1981).).

For reasons discussed below, each of and every claim of the '480 Patent is supported, and Petitioner has failed to satisfy its burden of showing that it is more likely than not that any of the claims of the '480 Patent are unpatentable under § 112(a) for lack of written description.

1. The '480 Patent Describes a Private Key as Recited in the Claims

Petitioner puts fourth four limitations related to the private key of the '480 Patent claims that are allegedly unsupported. Petition at 15–16. Patent Owner respectfully submits that each limitation is fully supported by the written

description of the '480 Patent and that one of ordinary skill in the art would readily recognize the claim limitations based on the disclosure of the '480 Patent. Ex. 2001, ¶4.

(1) "providing a private key in a memory of said electronic device, said memory being a secure part of a Basic In Out System or any other secure location in said electronic device"

The '480 Patent discloses, "[t]he authentication software preferably has its own unique serial number, software ID and/or private encryption key." Ex. 1001 5:39–40. A POSITA would recognize that since the authentication software has a private encryption key, the private key forms an integral part of the authentication software component and/or is embedded therein. Ex. 2001, ¶62. This is especially evident because the '480 Patent does not provide that the authentication software would have (undefined) access to its own private key by requesting such access from any other software component. Ex. 2001, ¶63. Additionally, the '480 Patent does not provide description the authentication software's private key would be subsequently retrieved after a request and handed over to the authentication software from any source or memory when need to perform unique digital signing. Thus, a POSITA would recognize that the private key is with the authentication software. Ex. 2001, ¶62.

As a result of recognizing that the private key can be an integral part of the authentication software because the '480 Patent clearly states this, a POSITA

would recognize that disclosure relating to the authentication software also includes the private key embedded therein. Ex. 2001, ¶64; Ex. 1001 5:39–40.

The '480 Patent contains numerous examples of the authentication software being stored in a memory of the electronic device, the memory being a secure part of a Basic In Out System (BIOS). For example, the specification includes the following paragraphs:

> The device is now set-up. **Authentication software** and an encoded authentication table are **installed in the BIOS**.

Ex. 1001, 6:56–57, emphasis added;

> The BIOS manufacturer **embeds** the bit string, **like the authentication software, in the BIOS** according to cell 8.

Ex. 1001, 6:2–4, emphasis added;

> The connection with the TTP . . . may also be initiated **by the authentication software, which is embedded in a secure part of the BIOS**…"

Ex. 1001 6:17–19, emphasis added;

> Next, according to cell 28B, the device needs to reboot **to store the authentication software** and the bit string **in a secure part of the BIOS which is not accessible for the operating system**.

Ex. 1001, 7:45–48, emphasis added. Additionally with respect to "any other secure location in said electronic device," this feature is also disclosed in the '480 Patent:

> This secure part of the BIOS may also be any other secure location in the device. For instance, it may be a separate part of a hard drive of a computer, which part may not be accessible to the operating system, but only to the BIOS and/or authentication software.

Ex. 1001, 6 :48–53. Furthermore, FIG.3 of the '480 Patent clearly discloses authentication software 54 installed and stored in secure area 62. Ex. 1001, FIG. 3. Since the authentication software 54 includes the private key contained or embedded therein, the private key would be provided in secure memory location 54 of the Secure Area 62. Ex. 2001, ¶65.

Therefore, a POSITA would clearly recognize based on (1) the extensive disclosure in the '480 Patent of the authentication software stored in a memory of the electronic device, wherein the memory is part of a BIOS or any other secure location and (2) the disclosure that a private key is an integral part of the authentication software, the claim limitation of "providing a private key in a memory of said electronic device, said memory being a secure part of a Basic In Out System or any other secure location in said electronic device," is fully supported in the '480 Patent specification. Ex. 2001, ¶66.

With respect to claims 17 and 18, Petitioner errantly equates "a memory" (*e.g.*, a regular flash memory) of claims 17 and 18 with "a memory being a secure part of a Basic In Out System or any other secure location," as recited in independent claims 1 and 16. Petition at 18-19. Nonetheless, the feature recited in

claims 17 and 18 are disclosed in the '480 Patent. For example, the '480 Patent states:

> Thus, the device is provided with the authentication software and the authentication data, the authentication data being secured by encryption from becoming known to a user. The device is installed for performing the transaction method and the legitimate use verification method according to the present invention.

Ex. 1001, 11:17–22;

> The generated authentication data may be stored in a user accessible memory**, such as a hard drive of a computer device, or on a removable memory such as a floppy disk or a flash memory**. As mentioned above, the authentication data need to be protected from any user, especially from a malicious user. Thereto, **the authentication data are encrypted by the authentication software**, preferably running in a secure processing environment, **before the authentication data are stored in said user accessible memory**.

Ex. 1001, 10:59–67, emphasis added.

> If the authentication data are stored **in a removable memory, for example a flash memory**, the **encryption key** may be **associated with a serial number of the removable memory**. Preferably, the encryption key is (also) associated with a user identifying number, e.g. a personal identifying number (PIN) or a number or a template associated with a fingerprint of the user, or the like.

Ex. 1001, 11:9–15, emphasis added.

Therefore, even though Petitioner fails to recognize the differences between the embodiments of claims 17 and 18 which recite "a memory" and the embodiments of the other independent claims, the recited claim features are support in the written description of the '480 Patent.

(2) "which private key is inaccessible to a user of said electronic device"

As discussed above, the authentication software has the private key. Ex. 1001, 5:39–40. Encryption of the authentication software and thus its private key is supported, for example, at step 20 in FIG. 1 of the '480 Patent. Additionally, "[t]he authentication software may be encrypted, or not." Ex. 1001, 11:44–45. A POSTITA would recognize that if the authentication software with the private key is encrypted, it would be inaccessible to a user of the device. Ex. 2001, ¶67. Additionally, the '480 Patent provides the following support for this feature:

> Further, the authentication software stores and activates a digital-signing algorithm to generate a session- or transaction-specific digital signature. **The authentication software preferably runs in a separate operating environment** in the BIOS or in a console and is ***independent from and inaccessible to the operating system*** (OS) on the device.

Ex. 1001, 4:66 – 5:3, emphasis added;

> The secure area 62 comprises applications and storage locations, which are not reported to the operating system 48. **That means that the operating system 48 does not know that the applications and**

> **data in the storage locations are present** and maybe even running in a separate environment.

Ex. 1001, 8:63 – 9:1, emphasis added;

> Therefore, **the authentication software 54 may be installed** in an application environment **in the secure area 62**.

Ex. 1001, 9:16–18, emphasis added;

> **To prevent that the authentication data becomes accessible to a user**, the authentication data should only be decrypted in a secure processing environment such as a 'Ring Zero' processing environment, which is embedded in a processing unit of commonly used personal computers. Such a secure processing environment may only be accessible to selected software applications, **preferably not to user-operated software applications**. Further, **a decryption algorithm and/or a decryption key should not be obtainable to any user**.

Ex. 1001, 9:42–51, emphasis added.

Any POSITA would clearly understand that if the operating system 48 cannot gain specified access, such access is also denied to the user. Ex. 2001, ¶68. Therefore, the feature of "which private key is inaccessible to a user of said electronic device," is fully supported in the '480 Patent specification. Ex. 2001, ¶69.

(3) "wherein the private key is encrypted when the private key is stored in said memory"

As discussed above, the authentication software has the private key. Ex. 1001, 5:39–40. In the '480 Patent, FIG. 1, steps 14-16-18-20 and corresponding in FIG 2 steps 34-36-38-40 of the '480 Patent disclose the principles of the decryption, re-encryption and re-encrypted storage of an authentication table as example of authentication data in new and existing devices are set out. Ex. 1001, FIG. 1, 2. A POSITA would understand that this principle can be readily applied to any authentication data that are used to perform unique digital signing according to the '480 Patent, including the private key of the authentication software. Ex. 2001, ¶70.

Additionally, the '480 Patent discloses this feature as follows:

> Next, according to cell 16, the authentication table is encoded by the authentication software to prevent that the authentication table may be uncovered (*e.g.* by a person). Uncovering of the authentication table would weaken the protection conferred by the method and should therefore be virtually impossible. The encoding is performed using a number, which is specific for the BIOS. When the authentication table is needed later, it may then be decoded by the authentication software using that BIOS-specific number. The BIOS-specific number may be a unique serial number or any ordinary encryption key incorporated in or generated by the BIOS, for example. The BIOS-specific number is sent to the authentication software according to cell 18 after a request from the authentication software according to cell 16. The installation in a new device is completed according to cell 20. The encoded

> authentication table is stored in a secure part of the BIOS, where it may only be retrieved by the BIOS and not by the operating system. This secure part of the BIOS may also be any other secure location in the device. For instance, it may be a separate part of a hard drive of a computer, which part may not be accessible to the operating system, but only to the BIOS and/or authentication software. Storing the authentication table in a secure location further decreases the possibility of retrieval of the authentication table.

Ex. 1001, 6:30–55;

> According to cell 34, the decrypt key is used to decrypt the authentication software and to decrypt the bit string and generate the corresponding authentication table. Next, according to cell 36, the authentication software verifies the authentication table and requests BIOS-specific data from the BIOS to encrypt the authentication table again.
>
> According to cell 38 the BIOS sends BIOS-specific data, for example any common encryption key, to the authentication software in reply. The method is completed according to cell 40, wherein the authentication table is encrypted and stored in a secure part of the BIOS. Any data remaining in the operating system from the transfer of the authentication data and authentication software is deleted by the BIOS.

Ex. 1001, 7:55–67;

> To prevent that the authentication data becomes accessible to a user, the authentication data should only be decrypted in a secure processing environment such as a 'Ring Zero' processing environment,

> which is embedded in a processing unit of commonly used personal computers. Such a secure processing environment may only be accessible to selected software applications, preferably not to user-operated software applications.

Ex. 1001, 9:42–49. With respect to claims 16-18 of the '480 Patent, there is support as follows:

> Thus, the device is provided with the authentication software and the authentication data, the authentication data being secured by encryption from becoming known to a user. The device is installed for performing the transaction method and the legitimate use verification method according to the present invention.

Ex. 1001, 11:17–22. Thus, a POSITA would recognize that the feature of "wherein the private key is encrypted when the private key is stored in said memory," is fully supported in the '480 Patent specification. Ex. 2001, ¶71.

(4) "wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software"

Regarding Petitioner's first assertion on page 21 of the Petition that there is no disclosure of decryption of a private key, Patent Owner has already established above that the '480 Patent describes the authentication data containing the private key is to be encrypted when stored and decrypted in a secure processing environment. *See supra* Section VI.1.3. In particular the '480 Patent provides:

> To prevent that the authentication data becomes accessible to a user, **the authentication data should only be decrypted in a secure processing environment such as a 'Ring Zero' processing environment**, which is embedded in a processing unit of commonly used personal computers. **Such a secure processing environment may only be accessible to selected software applications, preferably not to user-operated software applications**.

Ex. 1001, 9:42–49.

A POSITA would readily acknowledge that Ring 0 processing, also known as kernel mode processing, is a particular execution mode of the processor that is inaccessible by the operating system and, therefore, the user-operated software. Ex. 2001, ¶72. Thus, the '480 Patent discloses encryption and decryption in a secure environment inaccessible to user-operated software applications.

Petitioner's second assertion regarding the third embodiment are unfounded. Petition at 22–24. The third embodiment is claimed in independent claims 17 and 18, *i.e.* by "a memory." The "a memory" of claims 17 and 18 is not the same as the ***secure*** memory as with the other independent claims 1 and 16. In fact, "a memory" of independent claims 17 and 18 are supported in the '480 Patent as follows:

> The generated authentication data may be stored in a user accessible memory, **such as a hard drive of a computer device, or on a removable memory such as a floppy disk or a flash memory**. As

> mentioned above, the authentication data need to be protected from any user, especially from a malicious user. Thereto, **the authentication data are encrypted by the authentication software**, preferably running in a secure processing environment, **before the authentication data are stored in said user accessible memory**.

Ex. 1001, 10:59–67, emphasis added.

Finally, Petitioner's conclusion that: "the result of multiple reviews by multiple courts/offices has confirmed that the '480 Patent specification (which is similar to the specification in EP 099 and EP 140) has no description of an embodiment where a key is stored in a secure memory in encrypted format and decrypted in a secure environment" is blatantly untrue (as discussed above in Section IV). Petition at 24. Moreover, the provisional determinations of European proceedings regarding a European patent are completely irrelevant to whether the specification of United States '480 Patent provides written description support for the US claims.

Despite Petitioner's attempts to move the focus on irrelevant European proceedings, a POSITA would recognize that the written description in the '480 Patent supports the authentication software including a private key and describes the secure processing environment (not accessible to user-operated software programs) in which the authentication software decrypts authentication data (which the private key is). Ex. 2001, ¶73. This sufficiently describes the claim feature of

"wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software."

2. The '480 Patent Describes Claim 2

The '480 specification provides support that the bit string is (originally) authentication data. *See* Ex. 1001, 4:60–66. Thus, in the '480 Patent, the bit string can be a private key. A second party, *e.g.*, the network administrator provides and stores the bit string. Specifically:

> It is noted that in **another embodiment** of the present invention, the bit string **may be generated and stored by another actor than the TTP**. For example, **in case of network access identification**, **the network administrator** and/or a network server **may generate and store** the bit string such that when a user attempts to access the private network, the network administrator or server may regenerate the digital signature of said user. Thus, the user may unambiguously be identified by the network administrator or server before the user is granted access to the network.

Ex. 1001, 4:36–45, emphasis added. Additionally, the private key may be stored with data identifying the first transaction party:

> Upon connection, the requesting device sends a digital signature that was generated using fixed data components and variable data components. **The fixed data components may comprise a password or a personal identification number (PIN)**. The fixed data components are known to the corporate network and do not need be

> sent over the unsecured network connection; only the variable data components used are sent over the unsecured connection. Thus, the corporate network may regenerate the digital signature of the connecting device after receipt of the used variable data components. This method has the advantage that no password or PIN is sent over an unsecured connection **and that the digital signature identifies both the device (authentication table) and the user (PIN or password)**.

Ex.1001, 15:25–39, emphasis added.

Thus, a POSITA would recognize that because the bit string is provided by the second party, network administrator, and stored with data identifying the first transaction party, the '480 Patent describes the claim feature of claim 2. Ex. 2001, ¶74.

3. The '480 Patent Describes Claims 4 and 5

In the '480 Patent specification an authentication table (*i.e.* a bit string) is an example of authentications data. *See* Ex. 1001, 10:34–36. Additionally, as discussed above, and would be known to a POSITA, a private key can be authentication data. Ex. 2001, ¶76. Therefore, it follows that a private key is also a bit string.

Regarding claim 4, the authentication data and accompanying private key is encrypted by the second party using **an** encryption key before the private key is provided to the first transaction party. For example:

> It is noted that in **another embodiment** of the present invention, the bit string **may be generated and stored by another actor than the TTP**. For example, **in case of network access identification**, the **network administrator** and/or a network server **may generate** and store the bit string.

Ex. 1001, 4:36–40, emphasis added. Clearly, in this embodiment the network administrator is the **second party**. Additionally:

> The BIOS may be coupled to the TTP to receive a decryption code and **enable the authentication software** to decrypt an authentication table, which will then be encoded again and stored in a secure part of the device.

Ex. 1001, 4:52–56, emphasis added. Thus, a POSITA would recognize that the TTP may also be the second transaction party and the authentication data are encrypted by the TTP/second transaction party. Ex. 2001, ¶75. Therefore, claim 4 is described in the '480 Patent.

Regarding claim 5, which further recites retrieval of a decryption key (associated with the encryption key) by the authentication software and decryption of the private key at its first use. Ex. 1001, 18:41–44.

The above-noted passages of the '480 Patent support the embodiment where the TPP may also be the second transaction party. Further:

> **At the first start-up of the computer** according to cell 10 the BIOS **or the authentication software** uses a connection to a network, such as the Internet, to establish a connection with the TTP. **The**

> **connection is being made** to collect the data string, which is needed to decrypt the bit string and generate an authentication table. The BIOS or the authentication software may be identified by the TTP using the fixed data, which is a unique number as mentioned above. **The connection with the TTP does not need to be initiated by the BIOS**, but may also be initiated by the authentication software, which is embedded in a secure part of the BIOS, or by a third party application.

Ex. 1001, 6:9–20, emphasis added. Thus, a POSITA would recognize that first start-up of the computer, which may initiate the authentication software to decrypt the bit string sufficient describes retrieval of a decryption key associated with the encryption key and decrypts the private key at its first use. Ex. 2001, ¶77.

4. The '480 Patent Describes Claims 16, 18, and 19

Again, with respect to claims 16, 18, and 19, Petitioner errantly equates "a memory" (*e.g.*, a regular flash memory) of claims 18 and 19 with "a memory being a secure part of a Basic In Out System or any other secure location," as recited in independent claim 16. Petition at 27-28. Nonetheless, the feature recited in claims 18 and 19 are disclosed in the '480 Patent. For example, the '480 Patent states:

> Thus, the device is provided with the authentication software and the authentication data, the authentication data being secured by encryption from becoming known to a user. The device is installed for performing the transaction method and the legitimate use verification method according to the present invention.

Ex. 1001, 11:17–22;

> The generated authentication data may be stored in a user accessible memory, **such as a hard drive of a computer device, or on a removable memory such as a floppy disk or a flash memory**. As mentioned above, the authentication data need to be protected from any user, especially from a malicious user. Thereto, **the authentication data are encrypted by the authentication software**, preferably running in a secure processing environment, **before the authentication data are stored in said user accessible memory**.

Ex. 1001, 10:59–67, emphasis added.

Additionally, Petitioner asserts that the '480 Patent "does not disclose a processor that is configured for an operating system **and** for activating the authentication software . . . wherein the authentication software is run in a secure processing environment inaccessible to the operating system." Petition at 27. This argument is unfounded because a POSITA would recognize that a processer must be configured for an operating system in order for the device to run at all. Ex. 2001, ¶78. Furthermore, processors support kernel mode processing, *e.g.,* Ring 0 processing which is where the '480 authentication software is executed. Ex. 2001, ¶79. A POSITA would recognize this architecture and find the features of claim 16 disclosed in the '480 Patent. Ex. 2001, ¶80.

VII. GROUND B1 FAILS BECAUSE THE CLAIMS OF THE '480 PATENT ARE PATENTABLE OVER ELLISON AND MUIR

The combination of Ellison and Muir cannot form a proper ground for claims 1, 3, 6, 11, and 14-19 of the '480 Patent being unpatentable, because neither Ellison nor Muir teach or suggest: (i) a decryption key for decrypting the private key (used by the first transaction party to digitally sign a transaction) being incorporated in the electronic device; (ii) authentication software stored in said secure memory inaccessible to said operating system; or (iii) authentication software run in a secure processing environment inaccessible to said operating system.

1. Ellison

Ellison is directed toward an operating architecture 50 with ring-0 10, ring-1 20, ring-2 30, ring-3 40, and a processor nub loader 52, the operating architecture 50 having two modes of operation: normal execution mode and isolated execution mode. Ex. 1006, 2:64–67; 3:4–7; and FIG. 1A. In the isolated execution mode, there is secure platform 200 that includes an OS nub 16, a processor nub 18, a key generator 240, a hashing function 220, and a usage protector 250 all operating within an isolated execution environment. Ex. 1006, 8:25–30. Ellison's isolated execution architecture allegedly prevents attacks and vulnerabilities in electronic and software systems. Ex. 1006, 2:40–61.

The isolated execution environment relates to and is dependent on ring 0 architecture of the processor. *See* Ex. 1006, FIG. 1A. Ellison discloses that critical

modules are ***loaded*** into the execution space by processor nub 52. *See* Ex. 1006, 6:27–67 which states:

> The digest memory 154, typically implemented in RAM, stores the digest (e.g., hash) values **of the loaded processor nub 18, the operating system nub 16, and any other critical modules (e.g., ring-0 modules) *loaded into* the isolated execution space**.

Emphasis added. This module loading implies that the modules are stored in non-volatile memory, from which they are loaded into the execution space.

Ellison includes a memory controller hub (MCH) 130, a system memory 140, an input/output controller hub (ICH) 150, a non-volatile memory 160, and a mass storage device 170. Ex. 1006, 4:41–44.

2. Muir

Muir is directed toward a computing system 110 that includes an application 120, a device operating system 125, a smart card interface 150, and a virtual smart card 151. Ex. 1008, p. 7, ¶4. Virtual smart card 151 includes Virtual Smart Card Driver 155 and memory 140 which includes a restricted memory space 170. Ex. 1008, p. 7, ¶4. Smart card driver 155 is outside of memory 140. *See* Ex. 1008, FIG. 3. Virtual Smart Card Driver 155 is software code, which upon execution, emulates a physical smart card and can intercept commands from the device operating system 125 to process the commands. Ex. 1008, p. 8, ¶4. Virtual Smart Card Driver 155 uses the restricted memory 170 to store private keys 167 and may

further use restricted memory space 170 to store encrypted and decrypted data. Ex. 1008, p. 9, ¶3.

A. Neither Ellison nor Muir Teach or Suggest a Decryption Key for Decrypting the Private Key (used by the first transaction party to digitally sign a transaction) Being Incorporated in the Electronic Device

Petitioner's bare assertion that Ellison discloses a decryption key for decrypting the private key being incorporated in an electronic device is not supported by the references. Additionally, Petitioner's attempt to interchange "incorporating" with "storing" fails to remedy that neither Ellison nor Muir teach Patent Owner's feature of a decryption key for decrypting the private (used by the first transaction party to digitally sign a transaction) key being incorporated in an electronic device.

First, Ellison mentions a symmetric key stored in the cryptographic key storage of the ICH hub. *See* Ex. 1006, 6:64 –7:3. However, Ellison fails to demonstrate that this key is used in decrypting any key used to secure a transaction (by the first transaction party). It is completely unclear how this key is being used.

Additionally, Petitioner states "[t]he OSNK 203 is incorporated in the electronic device of the first transaction party." Petition at 63. However, the disclosure of Ellison fails to support this and the language of Ellison that Petitioner cites states:

> The key generator 240 generates a key operating system nub key (OSNK) 203 which is provided only to the OS Nub 16. The OS nub 16 may supply the OSNK 203 to trusted agents, such as the usage protector 250. The key generator 240 receives the OS Nub identifier 201 and the BK0 202 to generate the OSNK 203. There are a number of ways for the key generator 240 to generate the OSNK 203. The key generator 240 generates the OSNK 203 by combining the BK0 202 and the OS Nub ID 201 using a cryptographic hash function. In one embodiment, the OS nub ID 201 identifies the OS nub 16 being installed into the secure platform 200.

Ex. 1006, 9:1–14.

The OSNK 203 is used to decrypt the register values or to sign the software to be run in the secure processing environment—not to sign a transaction between a first and second transaction party. Ex. 2001, ¶87. Even if key generator 240 is part of the isolated environment, where is the software stored when it is not in main memory? And, what prevents someone from running it outside this environment and looking at the result, namely OSNK 203? Put differently, what prevents an attacker from looking at OS NUB ID and PROCESSOR NUB (stored in Non-Volatile Memory) and regenerating OSNK 203 in the same way?

It is unclear where the OSNK key 203 is stored or whether is it generated every time it is needed. Ex. 2001, ¶88. The protected (encrypted) private key is

stored in a secure location but that is not necessary; the key to decrypt it has to be stored in a secure location.

Moreover, the OSNK 203 is generated by the key generator 240 *after* the device has been put in circulation. Ex. 2001, ¶89. It may be subsequently stored somewhere in the isolated environment, but that does not mean that the decryption key is incorporated as part of the electronic device.

Muir cannot cure this deficiency in Ellison because Muir discloses that the decryption key is **re-generated** for use, either at login or whenever a cryptographic function is requested. Specifically, Muir states:

> Key generation unit 416 operates **to generate a symmetric key** using a user password /ID from user interface 412. User interface 412 receives a user password/ID. In one embodiment, the user is asked to provide a user password /ID **at login**. In another embodiment, the user provides a password/ID **whenever a cryptographic function is requested**.

Ex. 1008, p. 14, ¶2, emphasis added.

Since neither Ellison nor Muir disclose a decryption key for decrypting the private key (used by the first transaction party to digitally sign a transaction) being incorporated into the electronic device, Petitioner simply states the OSNK 203 allegedly discloses this feature even though that is contrary to the disclosure of

Ellison which clearly shows OSNK 203 is *generated* rather than already incorporated into the electronic device as recited in Patent Owner's claims.

B. Neither Ellison nor Muir Teach or Suggest Authentication Software is Stored in Said Secure Memory Inaccessible to Said Operating System

Neither Ellison nor Muir disclose **storing** authentication software in a secure memory and Petitioner ignores this feature completely. Instead, Petitioner states that Ellison's usage protector 250 is "located in a secure platform 200 and operates within the isolated execution environment." Petition at 71.

The first problem with Petitioner's assertion is that the goal of usage protector 250 is to protect the software and registry states in the secure environment, that is to protect the secure environment itself and not to protect electronic transactions by a user (first transaction party). Ex. 2001, ¶91. Hence, it is not the same as the authentication software of the '480 Patent. The second problem is the "location" of usage protector 250 that Petitioner refers to is where the usage protector 250 is loaded ***into*** in order to ***execute***. Patent Owner respectfully submits that the execution environment is not the same as where something is ***stored***. Ex. 2001, ¶92.

Petitioner appears to recognize this distinction (and shortcoming) in the argument because Petitioner states "[a]nd even if the usage protector 250 is loaded from another memory into the isolated execution environment, code for executing

the usage protector 250 while in the isolated environment would have been stored in a secure memory so as to prevent unauthorize access of sensitive data." Petition at 71–72. Despite this assertion by Petitioner and Dr. Black, there is no support whatsoever in either Ellison or Muir to suggest **storage** of authentication software **in a secured area**. Without any support from the references, the suggestion that Patent Owner's claim feature of authentication software **stored in secure memory** would be obvious is unsubstantiated and solely based on improper hindsight.

For example, Petitioner relies on Ellison's usage protector 250 to allegedly disclose authentication software. Petition at 71. There is not a single instance in Ellison disclosing where the usage protector 250 is stored. Ex. 2001, ¶93. However, Ellison does make clear that usage protector 250 is **not** stored in the isolated area 70 (which Petitioner relies on as teaching a secure platform) because critical modules (such as usage protector 250) are *loaded into* the execution space by processor nub loader 52. *See* Ex. 1006, FIG. 1A and 6:27–67. These loaded modules are stored in mass storage device 170 which can be CD ROM 172, floppy diskettes 174, and hard drive 176. Ex. 1006, 7:33–39. Thus, the mass storage 170 where the usage protector 250 could be stored (like other critical code in Ellison) is **not** secured memory.

Unable to point out in Ellison where usage protector 250 is stored, Petitioner fails to even make a plausible explanation of why the storage of usage protector

250 would be treated differently than the storage of other critical code which is all stored in mass storage device 170. Furthermore, Muir offers no remedy for the deficiencies of Ellison.

Muir's Virtual Smart Card Driver 155 performs cryptographic calculations. Ex. 1008, p. 10, ¶1. However, Virtual Smart Card Driver 155 is stored outside of memory 140 where the restricted space 170 is located. *See* Ex. 1008, FIG. 3. The Virtual Smart Card Driver 155 is fully accessible because it is stored in one of fixed disk 225, RAM 205 or ROM 204, or "other memory devices within computer system 110." Ex. 1008, p. 11, ¶1. None of these storage locations are secure memory. Ex. 2001, ¶95. Thus, the only element of Muir which could reasonably be considered to pertain to Patent Owner's authentication software is also stored outside of restricted memory. Accordingly, Muir cannot remedy the deficiencies in Ellison because it is also silent as to storing authentication software in secure memory.

Since Petitioner cannot point to any disclosure in either Ellison or Muir of authentication software **stored in a secure memory**, Petitioner relies on where Ellison's usage protector 250 is "located" when it is executed. Petition at 71. However, the location of execution fails to disclose storage in a secure memory and secure execution does not preclude accessing the usage protector 250 in its ***unsecured storage location***. So, Petitioner is simply left with a conclusory

assertion by Dr. Black that it would be obvious to store the usage protector 250 securely. Ex. 1003, ¶109. However, this conclusion can only be gleaned from improper hindsight and knowledge of Patent Owner's disclosure because both references are silent as to this feature.

C. Neither Ellison nor Muir Teach or Suggest Authentication Software is Run in a Secure Processing Environment Inaccessible to Said Operating System

Neither Ellison nor Muir teach or suggest authentication software running in a secure processing environment inaccessible to the operating system because Ellison's failure to disclose the storage location of usage protector 250 implies the primary OS 12 would have access to usage protector 250 for running in the normal execution environment. Additionally, Ellison's drivers all run in normal execution mode and any combination of Ellison and Muir would require Muir's Virtual Smart Card Driver 155, which also runs openly accessible to the operating system, in order for the proposed combination of Ellison and Muir to run authentication software.

Petitioner relies on Ellison's usage protector 250 to allegedly disclose a secure processing environment. Petition at 73. However, Ellison does not disclose where usage protector 250 is stored nor does Ellison disclose that usage protector 250 is encrypted at any time. Therefore, Ellison's primary OS 12 would always have access to the usage protector 250 and could subsequently run the usage

protector 250 in the normal execution environment. This is because, like Ellison's code (e.g., processor nub 18) and applets (e.g., applets 46_l to 46_k) the usage protector is likely stored in mass storage device 170 which is fully accessible to the primary OS 12. *See* Ex. 1006, 7:33–36. Since the primary OS 12 could retrieve and access usage protector 250 from mass storage device 170 and run it in normal execution mode, Ellison fails to disclose authentication software that is run in a secure processing environment inaccessible to the operating system.

Additionally, a POSITA would not look to Muir to cure the above-noted deficiencies of Ellison regarding authentication software running in a secure processing environment inaccessible to the operating system. First, Ellison cannot be combined with Muir's pointer 171 to restricted memory space 170 ***without also incorporating*** Muir's Virtual Smart Card Driver 155. Ex. 2001, ¶101. This is because without Muir's driver 155, the restricted memory space 170 cannot be accessed with any element of Ellison's system.

Muir's driver 155 operates in a normal execution mode (the only type of execution disclosed by Muir) and outside of memory 140 where restricted memory space 170 is. CITATION *See* Ex. 1008, FIG. 3. Additionally, all of Ellison's drivers 13, 14 as well as the primary OS 12 operate in ***normal execution mode***. *See* Ex. 1006, 3:9–15 and FIG. 1A and 1B. What this means is that even if Ellison's system was combined with Muir, the driver 155 would be used in normal

execution mode because that is the only place Ellison operates drivers and because Muir's driver 155 is specifically used ***outside*** of restricted memory space. This would leave the proposed addition of restricted memory space 170 in Ellison ***completely accessible*** to the operating system in the normal operating environment.

A POSITA would recognize that combining Muir with Ellison would nullify the purpose of Ellison because any request to create a digital signature would come through the primary OS 12 operating with the driver 155 without even touching the isolated execution environment of Ellison. Ex. 2001, ¶102. This would destroy the functionality of Ellison's isolated execution environment.

Put differently, a POSITA would not combine Muir's Virtual Smart Card Driver 155 with full access to Muir's memory space 170 into Ellison's normal execution environment where Ellison's drivers operate. Such a proposed combination is not a secure processing environment nor is it inaccessible to the operating system.

In view of the foregoing, Patent Owner respectfully submits that the Board should deny institution of a post grant review proceeding on the basis of Ground A1.

VIII. GROUNDS B2–B3 FAIL, BECAUSE NEITHER OF AL-SALQAN OR SEARLE OVERCOME THE DEFICIENCIES OF ELLISON AND MUIR

In Grounds B2 – B3, Petitioner challenges claims 7, 8, 9, 10, 12, and 13 using the combination of Ellison and Muir with Al-Salqan (Ground B2) and Searle (Ground B3). Petitioner's position in Grounds B2 – B3 turns on the fundamentally false assertion that the proposed combination of Ellison and Muir can teach or suggest all of Patent Owner's independent claim features.

However, Petitioner does not argue that Al-Salqan or Searle cure the deficiencies noted above with respect to Ellison and Muir regarding claims 1, 3, 6, 11, and 14-19. Instead, Al-Salqan is cited for teaching multiple layers of encryption using private information (*see, e.g.*, Petition, 93-95) and Searle is cited for teaching encryption based on hardware device serial number (*see, e.g.*, Petition, 100-101).

Thus, Grounds B2 – B3 must fail for the reasons noted above with regard to the combination of Ellison and Muir. Therefore, Grounds B2 – B3 are fatally deficient and institution of a post grant review proceeding on these Grounds should be denied.

IX. CONCLUSION

For the foregoing reasons, Petitioner's request for institution of post grant review of the '480 Patent should be denied.

Respectfully submitted,

Date: January 31, 2022

/William P. Ramey, III/

William P. Ramey, III
Ramey & Schwaller, LLP
Registration No. 44,295
Lead Counsel for Patent Owner
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
(713) 426-3923 (telephone)
(832) 900-4941 (fax)
wramey@rameyfirm.com
uspto@rameyfirm.com

Counsel for Patent Owner
Ward Participations B.V.,

X. CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), this is to certify that on this 31st day of January 2022, I caused a true and correct copy of the foregoing PATENT OWNER WARD PARTICIPATIONS B.V.'S PRELIMINARY RESPONSE TO PETITION FOR POST GRANT REVIEW OF U.S. PATENT NO. 10,992,480 and EXHIBITS by e-mail on the following counsel of record (as agreed in the Service Information section of the Petition):

W. Karl Renner (Lead Counsel)
Registration No. 41,265
FISH & RICHARDSON P.C.
3200 RBC Plaza
60 South Sixth Street
Minneapolis, MN 55402
Tel: (202) 783-5070
Fax: (877) 769-7945
Service E-mail: PGR39843-0109IP1@fr.com

Jeremey J. Monaldo (Back-up Counsel)
Registration No. 58,680
Usman A. Khan (Back-up Counsel)
Registration No. 70,439
FISH & RICHARDSON P.C.
3200 RBC Plaza
60 South Sixth Street
Minneapolis, MN 55402
Tel: (202) 783-5070
Fax: (877) 769-7945 Service email:
PTABInbound@fr.com
Axf-ptab@fr.com
monaldo@fr.com
khan@fr.com

Date: January 31, 2022

/William P. Ramey, III/

William P. Ramey, III
Ramey & Schwaller, LLP
Registration No. 44,295
Lead Counsel for Patent Owner
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
(713) 426-3923 (telephone)
(832) 900-4941 (fax)

wramey@rameyfirm.com
uspto@rameyfirm.com

Counsel for Patent Owner
Ward Participations B.V.,

XI. CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION

Pursuant to 37 C.F.R. § 42.24(d), this is to certify that this PATENT OWNER WARD PARTICIPATIONS B.V.'S PRELIMINARY RESPONSE TO PETITION FOR POST GRANT REVIEW OF U.S. PATENT NO. 10,992,480 contains 9,159 words according to the word-processing system used to prepare it exclusive of the parts exempted by 37 C.F.R § 42.24(b) and complies with the type-volume limitation of 37 C.F.R. § 42.24(b).

Date: January 31, 2022

/William P. Ramey, III/

William P. Ramey, III
Ramey & Schwaller, LLP
Registration No. 44,295
Lead Counsel for Patent Owner
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
(713) 426-3923 (telephone)
(832) 900-4941 (fax)
wramey@rameyfirm.com
uspto@rameyfirm.com
Counsel for Patent Owner Ward Participations B.V.,