UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC and
LENOVO (UNITED STATES) INC.,
Petitioners,

v.

ERICSSON AB,
Patent Owner.

Case IPR2025-00004
Patent No. 11,122,313

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	Introduction	1
II.	Background of the '313 Patent and the challenged claims	2
III.	Person of ordinary skill in the art	6
IV.	Claim construction	6
V.	The Petition's Ground 1 does not satisfy its burden as to "content encryption key identifiers"	7
VI.	The Petition's Ground 2 likewise fails as to "content encryption key identifiers"	14
VII.	Conclusion	20

EXHIBIT LIST

Exhibit No.	Description
2001	Declaration of Kayvan B. Noroozi in Support of Motion for Admission *Pro Hac Vice*

I. Introduction

The challenged claims of the '313 Patent recite a "live media playback response comprising . . . content encryption ***key*** identifiers." But to meet that limitation, the Petition initially relies on Peterka's ***message*** identifiers, which identify the ***message*** carrying each key, and not the key itself. Pet. 24-25. That theory cannot prevail: message identifiers are not "key identifiers."

The Petition recognizes as much, so it presents two obviousness contentions. In its first attempt, the Petition simply asserts that adding key identifiers to Peterka would have been obvious because key identifiers were allegedly used in ***other*** references, and can differentiate between keys. Pet. 25. That approach fails under Federal Circuit law, particularly because Peterka already uses unique *message* identifiers, and the Petition fails to show why or how Peterka would have benefited from further adding *key* identifiers. *Nuvasive Inc.*, 842 F.3d 1376, 1383-84 (Fed. Cir. 2016); *Duke Univ. v. BioMarin Pharm. Inc.*, 685 App'x 967, 978-79 (Fed. Cir. 2017); *In re Schweickert*, 676 F. App'x 988, 993-96 (Fed. Cir. 2017); *In re Anova Hearing Labs, Inc.*, 809 F. App'x 840, 843 (Fed. Cir. 2020). The Petition's mere conclusory statements in that respect simply cannot suffice. *KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) ("Rejections on obviousness grounds cannot be sustained by mere conclusory statements.").

The Petition's second attempt at obviousness—a proposed combination with Suzuki—fares no better. As a threshold matter, the Petition fails to show that Suzuki teaches ***unique*** key identifiers, as the claims require in view of the specification. Ex. 1001, 3:38-40. To the contrary, Suzuki only teaches identifiers for a current key and a new key—identifiers that are not unique to any particular key and that could be applied to *any* key. The combination thus fails at the outset because it cannot meet the challenged claims. Moreover, the combination again lacks any adequate showing of a *motivation*. Although the Petition articulates several alleged motivations, each fails because it rests on problems Peterka is not shown to have ("confirmation delay," "when to use a key," "facilitating key acquisition and use") and solutions that Suzuki's key identifiers do not provide ("unique" key values; "eliminating confirmation delay").

Accordingly, the Petition lacks a reasonable likelihood of success, and institution should be denied.

II. Background of the '313 Patent and the challenged claims

United States Patent 11,122,313 ("the '313 Patent"), titled "Method and System for Secure Over-The-Top Live Video Delivery," is directed to, among other things, "over-the-top (OTT) media delivery and more specifically key rotation for live streaming media." Ex. 1001, 1:22-24.

The '313 Patent teaches that "[a]s content delivery models move away from streaming distribution over private networks to Web-based delivery of files over the public Internet, referred to as over-the-top (OTT) delivery, traditional content protection paradigms must be modified to support new delivery protocols, e.g., HTTP Live Streaming. For live streaming content with long or indefinite durations, use of a single encryption key for the entire duration increases the probability that the key may be compromised." Ex. 1001, 1:25-33. The '313 Patent teaches that "[t]here are many protocols and methods for generating segmented content . . . . each segment is independently playable, and therefore needs to be independently encrypted and decryptable. Segments are typically of a fixed duration and, in the case of video content, begin with a key-frame and contain no inter-segment references. Segmentation is performed on each of the different encoding generated by the transcoder, by parsing the resultant encoding and determining segment boundaries." Ex. 1001, 2:54-67. "Segments are encrypted on segment boundaries using the current content encryption key and current initialization vector (IV). . . . The generation of new strongly random values for use as content encryption keys and the rotation of content encryption keys provides protection from content encryption keys being compromised in long lived streams." *Id.* at 3:4-14.

"The transitioning between use of different keys is [ ] referred to herein as key 'rotation.'" *Id.* at 3:34-36. "A history of individual content encryption keys and the order in which they were generated is maintained." *Id.* at 3:36-38. Notably, "[e]ach content encryption key in the history is assigned a unique identifier which is referred to herein as the content encryption key identifier." *Id.* at 3:38-40. As the '313 Patent further explains, the Work Flow Manager 102 ("WFM") "generates an initial content encryption key and assigns it a content encryption key identifier." *Id.* at 6:1-2.

The '313 Patent further teaches that a content encryption key may be changed, or "rotated," in two possible scenarios: "normal period-based expiration, and an explicit key change notification received in step 308 that applies to the current segment being decrypted." *Id.* at 11:22-26. In the case of a non-period-based key rotation due to an explicit key change notification, the notification from the packager to the client "describes the expiration of the previous content encryption key ***and*** the content encryption key ***identifier*** of the new content encryption key to be applied." *Id.* at 10:61-66, 11:3-8, 11:12-17 (emphasis added). "If a content encryption key change request is detected, the client notes the need to expire the current content encryption key and the content encryption key identifier of the new key to be used." *Id.* at 11:17-20.

Exemplary claim 1 correspondingly recites:

Element	Claim 1
[1.Pre]	A method for handling secure distribution of live video content comprising:
[1A]	sending a request for live media playback; receiving a live media playback request response,
[1B]	the live media playback response comprising content encryption keys and content encryption key identifiers;
[1C1]	receiving encrypted live media content and manifest files from a content delivery server,
[1C2]	wherein the encrypted live media content comprises one or more content encryption key rotation boundaries wherein each content encryption key rotation boundary is associated with a change to a different content encryption key to decrypt the received encrypted live media content;
[1D]	applying a first content encryption key to the encrypted live media content before a first content encryption key rotation boundary; and
[1E]	prior to reaching the first key rotation boundary, obtaining a second content encryption key, the second content encryption key to be used after the first content encryption key rotation boundary is reached; and
[1F]	applying the second content encryption key for content decryption after the key rotation boundary is reached.

The Petition challenges claims 1-7, 9, 11-17, and 19. The Petition's Grounds are summarized below.

Ground	References	Basis	Challenged Claims
1	Peterka	§ 103	1-4, 6-7, 11-14, 16-17

2	Peterka, Suzuki	§ 103	1-4, 6-7, 11-14, 16-17
3	Peterka, Bocharov	§ 103	1-4, 6-7, 9, 11-14, 16-17, 19
4	Peterka, Suzuki, Bocharov	§ 103	1-4, 6-7, 9, 11-14, 16-17, 19
5	Peterka, Bocharov, Peterka308, Chen	§ 103	5, 15

III. Person of ordinary skill in the art

For purposes of this Preliminary Response, Patent Owner does not dispute the Petition's proposed level of skill for a person of skill in the art ("POSA"), because the level of skill in the art is not necessary for addressing any disputes between the parties.

IV. Claim construction

The Board does not construe claim terms that are not in dispute. *Shenzhen Liown Electronics Co. v. Disney Enterprises, Inc.*, IPR2015-01656, Paper 7 at 10 (Feb. 8, 2016) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). The Petition does not raise a dispute as to any claim construction issues. Pet. 9-10. Patent Owner does not believe the Board need resolve any claim construction issues at this stage. Nonetheless, to the extent the Board believes Patent Owner's arguments herein raise claim construction issues,

Patent Owner provides the evidentiary bases and arguments in support of its positions below.

V. The Petition's Ground 1 does not satisfy its burden as to "content encryption key identifiers"[1]

Limitation 1B and the corresponding language of independent claim 11 recite "the live media playback request response comprising content encryption keys ***and*** content encryption ***key identifiers***."[2]

The '313 Patent teaches that "[e]ach content encryption key in the history is assigned a unique identifier which is referred to herein as the content encryption key identifier." *Id.* at 3:38-40. As the above passage states, the "key identifier" recited in the claims and taught in the specification of the '313 Patent is ***assigned to the key itself***. The '313 Patent again recites this in a later passage, stating that the Work Flow Manager 102 ("WFM") "generates an initial content encryption key and ***assigns it*** a content encryption key identifier." *Id.* at 6:1-2 (emphasis added). The '313 Patent is thus clear that the "content encryption key identifier" must be assigned to the content encryption key itself.

[1] Beyond Grounds 1 and 2, no other Grounds contain additional theories as to "content encryption key identifiers."
[2] This Preliminary Response's arguments regarding claim 1 are exemplary and are directed to all challenged claims including independent claim 11 and its dependents, which recite the same relevant claim language.

To meet limitation 1B and the corresponding limitation of claim 11, the Petition's Ground 1 initially relies on Peterka alone. Pet. 24. The Petition contends that Peterka teaches "a sequence number or time stamp" that is assigned to a ***message*** carrying a content encryption key, and contends that this constitutes the "***key*** identifier" of the challenged claims. *Id.*

The Petition's own statements and Peterka's teachings, however, prove otherwise. As the Petition explains, in Peterka each and every key "is distributed to a client in an Entitlement Control Message ('ECM') or an Entitlement Management Message ('EMM')." Pet. 11. The Petition further acknowledges that the "sequence number/timestamp" that Petitioner relies upon "is unique ***to each ECM/EMM***" in Peterka. Pet. 24. In other words, the Petition itself admits that the "unique identifier" it relies upon from Peterka is assigned to the ***message*** carrying a content encryption key, and ***not*** to the ***key itself***.

Peterka further confirms the same fact. Peterka states: "In multicasting program content such as audio and visual material, entitlement management messages and entitlement control messages can be sent from a server to a client computer. One embodiment of the invention provides a format for ***such messages***. Under this format, a sequence number or a time stamp to protect against replay attacks is provided." Ex. 1005 121 (emphasis added).

The challenged claims, however, recite a unique "***key*** identifier" that is assigned to the key itself, not a "***message*** identifier" that is assigned to the message containing a key. The Petition's reliance on Peterka's ***message*** identifier thus cannot meet its burden of unpatentability as to limitation 1B.

Recognizing its deficiency, the Petition alternatively argues that the POSA would have been motivated "to implement Peterka's client to receive and use a key identifier to identify the content key in an ECM/EMM." Pet. 25. In support, the Petition contends that because ***other*** art allegedly taught the use of key identifiers, the POSA would have felt "the need to differentiate between keys" in Peterka. *Id.* The Petition further contends that Peterka itself "shows delivery of content keys with unique designations—CK_0, CK_1, and CK_2," which would have also allegedly motivated the POSA. Pet. 25.

The Petition's motivations, however, rests on incorrect factually premises, and thus fail.

First, a POSA would see no need for key identifiers in Peterka because Peterka already uniquely identifies each message carrying an individual key. As the Petition itself states, Peterka assigns a ***unique*** identifier to each ECM and EMM. Pet. 24. And as the Petition further states, each and every key in Peterka is distributed through an ECM or EMM. Pet. 11. Moreover, the Petition further states

that each ECM or EMM contains only "***one*** key." Pet. 21 (emphasis added). Thus, even assuming that "POSITAs would have recognized the need to differentiate between keys" in Peterka, Pet. 25—which the Petition fails to show—it does not follow that POSITAs "would have been motivated to do so with key identifiers." Pet. 25. Since Peterka already assigns a unique identifier to the ***message*** carrying each individual key, there would be no need, motivation, or benefit from further assigning a unique identifier to the key contained in each such message.

The Petition's citations to the expert declaration and other art beyond Peterka fail to show otherwise. Under similar circumstances, the Federal Circuit has repeatedly held that a POSA would not have a motivation to modify a reference to solve a problem that ***the reference itself*** did not have, even if ***other art*** may have taught the benefits of the modification ***under other circumstances***. *In re Nuvasive Inc.*, 842 F.3d 1376, 1383-84 (Fed. Cir. 2016); *Duke Univ. v. BioMarin Pharm. Inc.*, 685 App'x 967, 978-79 (Fed. Cir. 2017); *In re Schweickert*, 676 F. App'x 988, 993-96 (Fed. Cir. 2017); *In re Anova Hearing Labs, Inc.*, 809 F. App'x 840, 843 (Fed. Cir. 2020).

Thus, in *Nuvasive*, the Board found a motivation to combine the prior art based on the alleged benefit of "additional information," but the record did not show that "the PHOSITA would have sought this additional information," nor

"why the additional information would benefit a PHOSITA when implanting a posterior lumbar interbody fusion implant," nor "how the PHOSITA would use that information." 842 F.3d at 1384. The Federal Circuit thus concluded that there was no "*reason why* the PHOSITA would have been motivated to modify the SVS-PR or Telamon implants, in light of Baccelli, to obtain this additional information," and reversed on that basis. *Id.* at 1385.

Likewise in *In re Schweickert*, the Federal Circuit reversed the Board's finding of a motivation to combine based on the alleged benefit of "access control." 676 F. App'x at 994. Although the record showed that the semaphore taught in the Cunniff reference indeed provided the benefit of access control by solving the problem of multiple programs simultaneously competing for access to a device's RAM, the Federal Circuit emphasized that the underlying reference to be modified—Birrell—***did not have that problem***. *Id.* at 995 ("the record describes no problem in Birrell that would be resolved by the semaphore in Cunniff"). The Federal Circuit thus reversed because the purported motivation for the combination rested on an improvement or benefit that was not shown to be necessary or useful in the context of the specific reference that was to be modified. *Id.*

Similarly in *Duke v. BioMarin*, the Federal Circuit once again reversed the Board's motivation to combine finding because it rested on the purported benefit of

solving a problem that did not exist ***in the context of the combination***. 685 F. App'x at 978-979.

And in *Anova*, the Federal Circuit set aside the Board's finding of a motivation to combine based the purported desire to create an "open passageway" that would allow "ambient noise to enter the ear canal" where the primary reference "***already include[d] vents***." 809 F. App'x at 843 (emphasis added).

Those precedents refute the Petition's motivation to combine here. As in *Nuvasive*, *Schweickert*, *Duke*, and *Anova*, the Petition's allegation that *other* art taught the use of key identifiers is not an adequate motivation for modifying Peterka to use key identifiers when the Petition has failed to show any need or benefit in Peterka from the use of key identifiers. And Peterka itself refutes any such need because, as the Petition admits, Peterka already provides a unique identifier for each message containing a key, and each message contains only one key. Pet. at 24, 11, 21. Notably, the Petition does not rely on any scenario in which Peterka would distribute a key without a uniquely identified ECM or EMM, nor does it propose to modify Peterka in any way in that respect. There is thus no basis for the Petition's conclusory allegation that the POSA would have felt a need to "differentiate between keys" in Peterka when Peterka already differentiates between the ***messages*** containing each and every key.

Nor is there any basis for Petitioner's expert's contention that adding key identifiers to Peterka would have "facilitate[d] the use of the correct key for the correct segment." Ex. 1003 ¶ 92. Petitioner's expert makes no showing that Peterka *without* modification has any problem or deficiency in using the correct key for the correct segment, nor does he explain how or why the POSA would expect Peterka to be improved in that respect by adding key identifiers. Instead, the expert declaration, like the Petition, simply provides conclusory statements in passing, which cannot suffice. *KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) ("Rejections on obviousness grounds cannot be sustained by mere conclusory statements.").

Thus, like the purported motivation of "additional information" in *Nuvasive*, the Petition here provides no evidence as to *how* "differentiating between keys" would have been expected to benefit or improve Peterka in any way, or why the modification would have "facilitate[d] the use of the correct key for the correct segment" beyond what Peterka already teaches. *Nuvasive*, 842 F.3d at 1384-85. Federal Circuit precedent holds that neither the Petition's conclusory statements nor its mere showing that ***other*** art such as Suzuki and Pestoni allegedly used key identifiers can suffice to establish a motivation here. *Nuvasive*, 842 F.3d at

1384-85; *Schweickert*, 676 F. App'x at 994-995; *Duke*, 685 F. App'x at 978-979; *Anova*, 809 F. App'x at 843.

Second, the Petition's contention that Peterka itself "shows delivery of content keys with unique designations—CK_0, CK_1, and CK_2," is both self-defeating and incorrect. If Peterka did indeed teach the use of unique *key* identifiers, the Petition would have relied on that teaching for its theory, and would have no reason to propose *modifying* Peterka. In reality, Peterka does not provide such a teaching. Instead, Peterka simply uses CK_0, CK_1, and CK_2 to distinguish between the keys shown in its Figure 7B for purposes of clarity in Peterka's specification. Ex. 1005 ¶ 122. Peterka never teaches ***sending*** CK_0, CK_1, and CK_2, or any key identifier, to a client as part of a media playback request response, nor does the Petition identify any evidence of Peterka doing so. Accordingly, the Petition's allegation that Peterka "shows delivery of content keys with unique designations" is incorrect, and cannot provide a motivation for its proposed modification.

VI. The Petition's Ground 2 likewise fails as to "content encryption key identifiers"

The Petition's Ground 2 proposes to modify Peterka in view of Suzuki to incorporate Suzuki's alleged key identifiers. Pet. 46-49. This theory also fails at multiple levels.

First, the Petition fails to show that Suzuki teaches the use of a key number that is ***unique*** to each key, as the challenged claims require. Ex. 1001, 3:38-40. In the passages the Petition cites, Suzuki merely teaches the use of a "key number A," representing the current key in use, and a "key number B," representing the next key to be used. Ex. 1006 ¶¶ 72-77; Pet. 46 (citing and identifying same). Thus, ***any*** key could be named "key number A" or "key number B" simply based on whether that key is the current key or the next key—a nomenclature that is not "unique" to any particular key. By contrast, the '313 Patent teaches and claims ***unique*** key identifiers. Ex. 1001, 3:38-40 (defining "content key identifier" as "a unique identifier"). Moreover, the '313 Patent teaches that its unique key identifiers are used to maintain "[a] history of individual content encryption keys and the order in which they were generated." *Id.* at 3:36-38. Suzuki's mere "current key" and "next key" nomenclature could ***not*** be used to track ***individual*** content encryption keys that are used and the order in which they were generated, as the '313 Patent teaches, and thus cannot constitute the claimed "key identifiers" for that further reason. Indeed, aside from an entirely conclusory statement that "Peterka-Suzuki's 'key numbers' uniquely identify keys," neither the Petition nor the accompanying expert declaration ever purport to show that Suzuki teaches unique key identifiers. *See* Pet. 49 (citing Ex. 1003 ¶ 159); *KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398,

418 (2007) ("Rejections on obviousness grounds cannot be sustained by mere conclusory statements."). The Petition's combination thus fails because it cannot meet the "key identifier" requirement of the claims.

Second, for the same reasons, Suzuki cannot support the Petition's purported motivation of "providing unique values (such as key numbers) to keys." Pet. 48. As shown, Suzuki only teaches identifying keys as the current key or the next key, and does not teach providing unique values to keys. Accordingly, a POSA would not have been motivated by Suzuki to modify Peterka to provide "unique values" to keys, since there is no such teaching in Suzuki.

Third, the Petition's purported motivation of "eliminat[ing] confirmation delay during key changes" likewise fails under Federal Circuit precedent. Pet. 48. The Petition cites to ***Suzuki*** for the alleged benefit of "eliminating confirmation delay during key changes." Pet. 48 (citing Ex. 1006 11). But the Petition does not show that ***Peterka*** had any problem of "confirmation delay during key changes," or that modifying Peterka to add key identifiers would have solved any such non-existent problem. The Petition's failure in that respect is fatal to its "eliminating confirmation delay" motivation. *Nuvasive*, 842 F.3d at 1384 (no motivation where petitioner failed to show "why the additional information would benefit a PHOSITA ***when implanting a posterior lumbar interbody fusion***

implant"); *Schweickert*, 676 F. App'x at 994 (no motivation based on alleged benefit of "access control" when the reference to be modified was not shown to have that problem, even though the secondary reference did have that problem); *Duke v. BioMarin*, 685 F. App'x at 978-979 (rejecting motivation that rested on the purported benefit of solving a problem that was not shown to exist in the primary reference). Moreover, Suzuki does not teach that providing ***key identifiers*** solves the problem of "eliminating confirmation delay (key switch delay)." Ex. 1006 ¶ 11. Rather, it teaches that "encrypting data with a different key at regular intervals during multicast distribution" solves that problem. *Id.* The Petition's "confirmation delay" motivation thus further fails even based on Suzuki's own teachings because Suzuki does not teach that using key identifiers improves confirmation delay.

***Fourth*,** the Petition's motivation of "facilitate[ing] timely key acquisition and use" likewise fails because the Petition does not show *how* adding key identifiers to Peterka would have actually "facilitated timely key acquisition and use." *Nuvasive*, 842 F.3d at 1384 (rejecting motivation based on benefit of "additional information" because petitioner did not show "how the PHOSITA would use that information."). Moreover, Peterka's own teachings refute any such motivation. Peterka discloses that a client may obtain keys through either a "pull" model or a "push" model. Ex. 1005 ¶ 105. Under the pull model, a client only

requests and obtains a new key based on the expiration time of the current key. *Id.* Because the client knows the expiration time of the current key, it knows when to request and use a new key. Ex. 1005 ¶ 106 (Peterka teaching that since the expiration time of the current key is "distributed to the client," "[t]he server need not monitor the status of the client's keys; rather, the responsibility of determining when a new key is required can be passed to the client."). The Petition fails to even allege, much less show, how adding a unique key identifier would "facilitate timely key acquisition and use" for Peterka's client under the pull model. Alternatively, under the "push" model, Peterka expressly discloses that "the sever [] keeps track of active clients and distributes new keys to them before the current keys expire." *Id.* Once again, Peterka teaches that the server knows when to distribute a new key under the push model, and the Petition fails to even allege how adding a unique key identifier would "facilitate" the distribution or use of Peterka's keys in that setting. Moreover, Peterka expressly teaches that "a predetermined bit can be used to indicate if an old or current content key should be used as opposed to a new content key which has recently been distributed to the client. Thus, ***a client can check the predetermined bit in a packet and determine the proper content key to use***." Ex. 1005 ¶ 117 (emphasis added). Although Peterka's "predetermined bit" can only distinguish between a current key and a new key, and is thus not a unique

"key identifier" as recited in the claims for the reasons above, Peterka's "predetermined bit" already allows the client to determine "the proper content key to use." Peterka's own teachings thus further refute the Petition's "facilitating timely key acquisition and use" motivation. *Anova*, 809 F. App'x at 843 (rejecting Board's motivation of an "open passageway" that would allow "ambient noise to enter the ear canal" where the primary reference "***already include[d] vents***.") (emphasis added).

Fifth**,** Peterka also refutes the Petition's overarching motivation that "Peterka leaves to a POSITA how to keep track of keys and their expiration times, and how to determine ***when*** a new key is required." Pet. 46 (emphasis original). Contrary to the Petition's premise, Peterka instructs clients as to the expiration time of a current key, and either pushes a new key to the client to implement or else gives the client the necessary information to request a new key prior to the expiration time of the current key. Ex. 1005 ¶¶ 105-106. In each instance, the client knows "when a new key is required." Pet. 64. Thus, contrary to the Petition's allegations, Peterka does not leave a gap as to how clients should determine when to apply a new key, or how clients should identify key expiration times. Peterka thus has no need for unique key identifiers to "realize Peterka's embodiment where 'each client keeps track of the keys and their expiration times and actively requests

new keys before the current keys expire so as to avoid service interruptions." Pet. 48.

Accordingly, the Petition's proposed combination with Suzuki fails to meet "key identifier" and lacks any viable motivation, and thus presents no reasonable likelihood of success.

VII. Conclusion

For the reasons above, the Board should decline to institute the Petition.

Respectfully submitted,

/s/ *Kayvan B. Noroozi*

Peter C. Knops, Reg. No. 37,659
Kayvan B. Noroozi, *Pro Hac Vice*
NOROOZI PC
11601 Wilshire Blvd., Suite 2170
Los Angeles, CA 90025
Attorneys for the Patent Owner

Date: January 31, 2025

CERTIFICATION OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned **PATENT OWNER'S PRELIMINARY RESPONSE** specified in 37 C.F.R. § 42.24 has 4,327 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 365.

/Kayvan Noroozi/
Kayvan Noroozi

Counsel for Patent Owner

Date: January 31, 2025

CERTIFICATION OF SERVICE

The undersigned hereby certifies that the foregoing **PATENT OWNER'S PRELIMINARY RESPONSE** was served electronically via e-mail on January 31, 2025, on the following counsel of record for Petitioner:

Scott McKeown, Reg. No. 42866
SMcKeown-PTAB@wolfgreenfield.com
Anant K. Saraswat, Reg. No. 76,050
ASaraswat-PTAB@wolfgreenfield.com
Turhan F. Sarwar, pending admission pro hac vice
TSarwar-PTAB@wolfgreenfield.com
Elizabeth A. DiMarco, pending admission pro hac vice
Elizabeth.DiMarco@wolfgreenfield.com

Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue Boston, MA 02210-2206
Telephone: 617-646-8000
Facsimile: 617-646-8646

/Kayvan Noroozi/
Kayvan Noroozi
NOROOZI PC
11601 Wilshire Blvd., Suite 2170
Los Angeles, CA 90025
Tel.: 310-975-7074

Counsel for Patent Owner

Date: January 31, 2025