

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

ERICSSON AB,
Patent Owner.

Case No. IPR2025-00003

Patent No. 9,313,178

**PETITIONER'S OPPOSITION TO PATENT OWNER'S REVISED
MOTION TO AMEND**

TABLE OF CONTENTS

I.	THE RMTA VIOLATES 35 U.S.C. § 316(D) AND 37 C.F.R. § 42.121	1
A.	The Revised Amendments Still Improperly Enlarge Claim Scope.....	2
B.	Revised Amendments [21.6] and [33.7] Introduce New Matter	5
II.	THE REVISED MOTION TO AMEND CLAIMS REMAIN UNPATENTABLE UNDER SECTION 103	7
A.	Ground 6A: Peterka-Traw	7
1.	Overview of Peterka	8
2.	Overview of Traw	8
3.	Reasons to combine Peterka and Traw	9
4.	Substitute Claim 21	12
5.	Substitute Claim 22	20
6.	Substitute Claim 23	21
7.	Substitute Claims 24-26 and 29	22
8.	Substitute Claim 30	23
9.	Substitute Claims 33-35, and 37	23
B.	Additional Traw Combinations (Grounds 6B-6E).....	24

TABLE OF AUTHORITIES

CASES

<i>K/S HIMPP v. Bragi GmbH</i> , IPR2023-01204, Paper 40 (PTAB Mar. 7, 2025).....	2
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	14, 20, 21
<i>Lectrosonics, Inc. v. Zaxcom, Inc.</i> , IPR2018-01129, -01130, Paper 15 (PTAB Feb. 25, 2019) (precedential).....	2
<i>Pannu v. Storz Instruments, Inc.</i> , 258 F.3d 1366 (Fed. Cir. 2001)	4
<i>Silencerco Weapons Rsch. Center v. Huxwrx Safety</i> , IPR2024-01214, Paper 22 (PTAB Aug. 18, 2025)	5
<i>Sisvel Int’l S.A. v. Sierra Wireless, Inc.</i> , 81 F.4th 1231 (Fed. Cir. 2023).....	5
<i>Spectrum Sols. LLC v. DNA Genotek Inc.</i> , IPR2023-01424, Paper 45 (PTAB Feb. 19, 2025)	5

STATUTES

35 U.S.C. § 102(a)	9
35 U.S.C. § 103	1, 7
35 U.S.C. § 316(d)	1, 7

REGULATIONS

37 C.F.R. § 1.175(b)	5
37 C.F.R. § 42.121	1

LISTING OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 9,313,178 (“178 Patent”)
1002	Prosecution History of U.S. Patent No. 9,313,178 (“178 FH”)
1003	Declaration of Anthony J. Wechselberger (“Wechselberger”)
1004	Curriculum Vitae of Anthony J. Wechselberger (“Wechselberger-CV”)
1005	U.S. Patent Publication No. 2002/0172368 (“Peterka”)
1006	Certified Translation of Japanese Published Patent Application No. 2004-166153 (“Suzuki”)
1007	U.S. Patent Publication No. 2010/0235528 (“Bocharov”)
1008	U.S. Patent Publication No. 2008/0270308 (“Peterka308”)
1009	European Patent Publication No. 1,418,756 A2 (“Chen”)
1010	U.S. Patent Publication No. 2005/0138362 (“Kelly”)
1011	U.S. Patent No. 8,677,428 (“Lewis”)
1012	U.S. Patent No. 8,789,196 (“Pestoni”)
1013	International Publication No. WO 2010/107625 A2 (“Sood”)
1014	U.S. Patent No. 8,806,050 (“Chen050”)
1015	T. Stockhammer, “Dynamic adaptive streaming over HTTP: Standards and design principles,” in Proc. ACM MMSys’11, San Jose, CA, USA, Feb. 23–25, 2011, pp. 133–144 (“Stockhammer”)
1016	W. Van Lancker, D. Van Deursen, E. Mannens and R. Van de Walle, “HTTP adaptive streaming with Media Fragment URIs,” 2011 IEEE International Conference on Multimedia and Expo, Barcelona, Spain, 2011, pp. 1-6, doi: 10.1109/ICME.2011.6012149 (“Van Lancker”)
1017	3GPP TS 26.234 version 9.3.0 Release 9 (2010-06), Technical Specification, “Universal Mobile Telecommunications Systems (UMTS); LTE; Transparent end-to-end Packet Streaming Services (PSS); Protocols and codecs,” Reference RTS/TSGS-0426234v930 (June 2010) (“3GPP-AHS”)
1018	R. Pantos (Ed.), HTTP Live Streaming, draft-pantos-http-live-streaming-06 (Mar. 31, 2011) (“Pantos”)
1019	RFC793: Transmission Control Protocol (September 1981) (“RFC793”)
1020	RFC2616: Hypertext Transfer Protocol – HTTP/1.1 (June 1999) (“RFC2616”)

1021	The Secure Sockets Layer Protocol, V. 3.0, <i>available at</i> https://web.archive.org/web/19970614041044/http://home.netscape.com/eng/ssl3/ssl-toc.html and https://web.archive.org/web/19970617034012/http://home.netscape.com/eng/ssl3/3-SPEC.HTM#1 (“SSL-Standard”)
1022	U.S. Patent No. 8,756,673 (“Barrus”)
1023	Yuan et al., “Layered access control for MPEG-4 FGS video,” Proceedings 2003 International Conference on Image Processing (Cat. No. 03CH37429), Barcelona, Spain, doi: 10.1109/ICIP.2003.1247012 (“Yuan”)
1024	U.S. Patent App. Pub. No. 2005/0060316 (“Kamath”)
1025	RESERVED
1026	<i>Apple Inc. v. Ericsson AB</i> , IPR2022-00618, Paper 2 (Feb. 25, 2022)
1027	<i>Apple Inc. v. Ericsson AB</i> , IPR2022-00618, Paper 9 (July 8, 2022)
1028	<i>Apple Inc. v. Ericsson AB</i> , IPR2022-00618, Paper 11 (Sept. 1, 2022)
1029	<i>Apple Inc. v. Ericsson AB</i> , IPR2022-00618, Paper 13 (Nov. 28, 2022)
1030	<i>Apple Inc. v. Ericsson AB</i> , IPR2022-00618, Paper 14 (Nov. 28, 2022)
1031	<i>Apple Inc. v. Ericsson AB</i> , IPR2022-00618, Paper 17 (Dec. 30, 2022)
1032	<i>In the Matter of Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same</i> , Inv. No. 337-TA-1376, Order No. 25 (Mar. 13, 2024)
1033	<i>In the Matter of Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same</i> , Inv. No. 337-TA-1376, Complaint, Exhibit 24 (October 12, 2023)
1034	<i>Telefonaktiebolaget LM Ericsson et al. v. Lenovo</i> , 5:23-cv-00570, Order Granting Motion to Stay (E.D.N.C. Feb. 9, 2024)
1035	USPTO Binding Interim Guidance Addressing PTAB’s Approach to Discretionary Denials, June 21, 2022, <i>available at</i> https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621.pdf .
1036	<i>In the Matter of Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same</i> , Inv. No. 337-TA-1376, Final Initial Determination (Nov. 15, 2024)
1037	<i>In the Matter of Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same</i> , Inv. No. 337-TA-1376, Commission’s Determination Affirming ALJ’s Final Initial Determination (Jan. 16, 2025)

1038	Declaration of Turhan F. Sarwar in Support of Admission <i>Pro Hac Vice</i>
1039	Declaration of Elizabeth A. DiMarco in Support of Admission <i>Pro Hac Vice</i>
1040	Deposition Transcript of John Villasenor Ph.D. (August 21, 2025) (“Villasenor-Dep.”)
1041	Supplemental Declaration of Anthony J. Wechselberger (“Wechselberger-Supp.”)
1042	U.S. Patent No. 7,392,381 (“Traw”)
1043	USPTO Memorandum Re: PTAB Consideration of Prior Findings of Fact and Conclusions of Law (September 16, 2025)
1044	RESERVED
1045	RESERVED
1046	RESERVED
1047	Second Supplemental Declaration of Anthony J. Wechselberger
1048	U.S. Patent App. Pub. No. 2008/0279387 (“Gassoway”)
1049	U.S. Patent App. Pub. No. 2006/0236096 (“Pelton”)

The Board should deny PO's Revised Motion to Amend ("RMTA"). The Board preliminarily concluded in Paper 30 ("PG") that PO's initial motion to amend ("IMTA") "appear[ed] to broaden the scope" of the original claims and that Petitioner showed a reasonable likelihood that the IMTA claims are unpatentable as obvious over the prior art. PG, 5, 10. The RMTA claims fail for the same reasons.

The IMTA claims broadened the scope of the original claims by removing the word "after," thus allowing "the second key for content decryption to be applied *before or after* the notification-based content encryption key [(‘CEK’)] rotation boundary.”¹ PG, 5. PO's revisions *do not cure* this defect. Although the RMTA restores the word "*after*," it simultaneously adds new structural changes that expand the scope of the original claims and cover implementations that the original claims did not. The RMTA thus fails to comply with 35 U.S.C. § 316(d)(3) and should be denied for the same reasons the PG preliminarily rejected the IMTA.

The substitute claims also remain unpatentable under Section 103 based on the same prior art that rendered the IMTA claims unpatentable.

I. THE RMTA VIOLATES 35 U.S.C. § 316(D) AND 37 C.F.R. § 42.121

PO has the burden to demonstrate that the RMTA complies with 35 U.S.C. § 316(d)(3) and 37 C.F.R. § 42.121. *See Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-

¹ Emphasis added throughout unless otherwise specified.

01129, -01130, Paper 15, at 4 (PTAB Feb. 25, 2019) (precedential). PO must demonstrate “the amendment does not seek to enlarge the scope of the claims of the patent and does not introduce new matter.” *K/S HIMPP v. Bragi GmbH*, IPR2023-01204, Paper 40, at 47-48 (PTAB Mar. 7, 2025).

A. The Revised Amendments Still Improperly Enlarge Claim Scope

PO’s RMTA claims enlarge the scope of the original claims in the same way the IMTA claims did. *See* PG, 4-5. Original claim 1 recited one “key rotation boundary” (hereafter, “*Boundary*”) and required two actions relative to that claimed *Boundary*: (1) “issuing requests to a license server *ahead of* a [*Boundary*] to retrieve a second [CEK]” and (2) “applying the second key for content decryption *after* the [*Boundary*] is reached.” EX1001, claim 1.

IMTA claim 21 required (1) issuing requests to a license server *ahead of* a *Boundary* to retrieve a second CEK; and (2) applying the second CEK *before the Boundary*. Critically, IMTA claim 21 removed the originally claimed requirement of (2) applying the second CEK *after the Boundary*. IMTA, 16. The Board preliminarily agreed this change broadened the claim by covering implementations that “would not meet the requirements of the original claim.” PG, 4-5.

RMTA claims 21/33 still extend to implementations that do not meet the original claims’ requirements and, therefore, still impermissibly broaden claim scope. PO tries to conceal this broadening by splitting the “key rotation boundary”

recited in original claim 1 into two boundaries and restoring the word “after.” But claims 21/33 still eliminate the original, required “ahead of/after” sequence: (1) issuing requests *ahead of a Boundary* and (2) applying a second CEK *after that same Boundary*.

As shown below, RMTA claims 21/33 now recite two separate boundaries: a “*notification-based*” boundary and a “*time-based*” boundary.

[21.5]/[33.6] issu[ing/e] requests to a license server *in response to detecting* said *notification-based [CEK] rotation boundary* *ahead of* [a-]said *time-based [CEK] rotation boundary* for said first key to retrieve a second [CEK]...; and

[21.6]/[33.7] apply[ing] the second key for content decryption *after* the *notification-based [CEK] rotation boundary* [for said first key] and *before* said *time-based [CEK] rotation boundary* for said first key is reached.

RMTA, Claims App’x, ii, v (coloring added). Critically, the RMTA claims do not preserve the same sequence of (1) issuing requests *ahead of a Boundary* and (2) applying a second CEK *after that same Boundary*.

For example, the RMTA claims require (1) issuing requests to retrieve a second CEK *at/after (“in response to”) a notification-based boundary*; and (2) applying the second CEK *after* that *same notification-based boundary*. The original claims would not have been satisfied by (1) issuing a request for a second CEK *after* a notification-based *Boundary* and (2) applying the second CEK for decryption *after the same Boundary*, because the original claim’s required “ahead of”/“after”

sequence is not met. However, the RMTA claims ***cover that implementation***. Thus, the RMTA claims cover scope not covered by the original claim.

The RMTA claims separately require (1) issuing requests to retrieve a second CEK ***ahead of a time-based CEK boundary***; and (2) applying the second CEK ***before*** that ***same time-based CEK boundary***. The original claims would not have been satisfied by (1) issuing a request for a second CEK ***before*** a time-based ***Boundary*** and (2) applying the second CEK for decryption ***before the same Boundary***, because the original claim's required "ahead of"/"after" sequence is not met. The Board already agreed that the original claims were not satisfied by issuing a request for a second CEK ***ahead of*** the claimed boundary and then applying the second CEK ***before*** reaching the same Boundary. PG, 5. But the RMTA claims ***do cover that implementation*** and thus cover scope not covered by the original claim.

As demonstrated, there is now no recited boundary (as existed in the original claims) for which the step of "issuing requests" must occur ***ahead of a Boundary*** ***and*** the step of "applying" the second CEK must occur ***after that same Boundary***. The RMTA claims are thus broader than the original claims in at least this respect. *Pannu v. Storz Instruments, Inc.*, 258 F.3d 1366, 1371 (Fed. Cir. 2001) ("[A] claim that does not include a limitation present in the original patent claims is broader in that respect."). As also demonstrated, the RMTA claims cover new scope because the original claims were not broad enough to cover scenarios where issuing a request

for a second CEK and applying the second CEK for decryption occur *on the same side* of the recited *Boundary*, while the RMTA claims *are* that broad.

This broadening is dispositive even if the substitute claim “may be narrower in other respects.” *Sisvel Int’l S.A. v. Sierra Wireless, Inc.*, 81 F.4th 1231, 1241 (Fed. Cir. 2023) (“[I]f a substitute claim is broader *in any respect* it is...broader than the original claim.”) (emphasis original, quotations omitted); 37 C.F.R. § 1.175(b). Thus, PO’s addition of limitations related to PO’s notification-based boundary elsewhere does not resolve the impermissible, dispositive broadening. The Board has routinely rejected similar substitute claims—broadening in one respect but narrower in others—as impermissibly broadening. *See Sisvel Int’l*, 81 F.4th at 1239-40; *Silencerco Weapons Rsch. Center v. Huxwrx Safety*, IPR2024-01214, Paper 22, at 5 (PTAB Aug. 18, 2025); *Spectrum Sols. LLC v. DNA Genotek Inc.*, IPR2023-01424, Paper 45, at 9-14 (PTAB Feb. 19, 2025). This error permeates all proposed substitute claims, and the Board should deny the RMTA in entirety.

B. Revised Amendments [21.6] and [33.7] Introduce New Matter

The Board agreed that PO’s IMTA limitation [21.6] “appear[ed] to introduce new subject matter.” PG, 8-9. PO’s RMTA limitations do not cure this deficiency. Instead, as with PO’s IMTA, PO provides a conclusory table of string cites. *See* PG, 5-6 (“It is not the responsibility of the Board to search through the string citations to find sufficient written description support for each element.”) (quotation, citation

omitted); IMTA, 10-12; RMTA, 6-9.

RMTA limitations [21.6] and [33.7] recite “apply[ing] the second key for content decryption after the notification-based [CEK] rotation boundary [for said first key] and *before* said time-based [CEK] rotation boundary for said first key is reached.” RMTA, Claims App’x, ii, v (underlining in original).

The RMTA (at 7, 9) alleges the following paragraphs of the ’243 Publication (EX2007) support [21.6]/[33.7]: ¶¶5, 36, 39; Fig. 3; cl. 1, 16.

None do. Every original claim required that a second key be applied for decryption *after* the rotation boundary that demarcated when the issuing requests step occurred, while no original claim required that a second key be applied for decryption *before* the demarcating rotation boundary. The Board recognized this. PG, 9. Likewise, the RMTA’s cited paragraphs do not support the [21.6]/[33.7] amendments. Paragraph 5 mimics original claim 1, stating the device “applies the second key... *after the key rotation boundary is reached.*” EX2007, ¶5.

Paragraph 36 describes checking the expiration of a “current content key to see if a new key should be applied.” Paragraph 39 similarly describes checking CEK expiration and the process for requesting a new CEK. While these two paragraphs generally describe (and Figure 3 illustrates) “two cases—normal period-based expiration and an explicit key change notification,” (*id.*, ¶36) there is *no description* of applying a second key for decryption *before* any rotation boundary.

Nor would such a requirement make sense. In the “normal period-based expiration” case, the second key is applied for decryption *after* a rotation boundary. In the “explicit key change notification” case, replacement keys are applied independent of and, agnostic to, key rotation boundaries. Beyond PO’s conclusory table, PO makes no attempt to demonstrate that a POSA would have understood the specification to support the new limitations. [21.6] and [33.7] violate § 316(d)(3).

II. THE REVISED MOTION TO AMEND CLAIMS REMAIN UNPATENTABLE UNDER SECTION 103

A. Ground 6A: Peterka-Traw

The RMTA claims are similar to the IMTA’s proposed substitute claims, addressed at length in Paper 28. *See also* Pet. (Paper 3), §§ IX-XIII.

The RMTA made two primary changes to the IMTA’s substitute claims. *First*, PO added a requirement that the second CEK be applied after a notification-based boundary. The additional detail specifying when the second CEK is applied relative to the notification-based boundary does not materially alter the obviousness analysis. The RMTA claims still recite requesting, retrieving, and applying a second CEK *before* reaching a time-based boundary, a basic concept that was described long before the ’178 Patent’s priority date, including in U.S. Patent No. 7,392,381 (EX1042, “Traw”). As discussed below, Peterka-Traw also meets the RMTA claims’ requirement of these steps all occurring *after* reaching a notification-based boundary. *Second*, PO added a requirement that key identifiers be “assigned” to an

associated CEK. As discussed below, assigning key identifiers to keys was obvious over prior art/combinations that were presented in the Petition, in view of Traw.

The remaining amendments to the amended substitute claims recite non-functional descriptions, intended purposes, or are otherwise disclosed by Peterka. The Board agreed Petitioner showed “a reasonable likelihood that [initial] proposed substitute claims 21-26, 29, 30, 33-35, and 37 are unpatentable as obvious” over Peterka-Traw. PG, 10. The RMTA claims are likewise unpatentable.

1. Overview of Peterka

Peterka (EX1005) relates to securely distributing multimedia content over a network. Peterka, Abstract, FIG. 1, [0038], [0006]-[0012]. Peterka’s “client” devices download streaming media from a content distribution system. *Id.*, [0038]. Media content is divided into segments that are each encrypted with a different key. *Id.*, [0080]-[0082], [0091]-[0101], [0122]-[0125], FIGs. 7A-7B. These encrypted media segments are streamed to clients. Peterka, [0043], [0119].

Peterka’s client obtains and applies the key required to decrypt each media segment—e.g., a content key (“CK”). *Id.*, [0011], [0091]-[0093], [0127], FIG. 7A; EX1003, ¶50. Peterka describes obtaining such keys through a pull model in which a client tracks its keys and their expiration times and actively requests new/replacement keys as needed. Peterka, [0105]-[0106], EX1003, ¶¶51-52.

2. Overview of Traw

Traw was filed April 13, 2004, issued on June 24, 2008, and is 35 U.S.C. §

102(a)(1)-(2) prior art. Traw is directed to a content protection system that both rotates keys “on a periodic basis” **and** “generate[s] revocation data corresponding to revoked keys in response to...a security compromise.” Traw, Abstract; *see id.*, 1:65-2:6 (key “revocation is also used to prevent access to content if the devices’ keys have been compromised”), 4:37-39. Traw’s system thus “protect[s] content (such as audiovisual entertainment content) against unauthorized access, copying or distribution.” *Id.*, 2:15-19. Traw’s system is “especially” suited for devices that “include software for assisting in implementing content protection” where “software may be updated via a communication mechanism” like the internet. *Id.*, 2:19-51.

Traw describes two types of key revocation in which current content keys are replaced: (1) periodic/planned key revocation (Traw, 5:33-35, 6:10-12); and (2) non-periodic/unplanned key revocation based on compromised keys, security attacks, or emergency situations (*id.*, 3:65-66, 4:37-39, 5:5-7, 5:37-39, FIG. 2). Messages are transmitted “to users and/or devices announcing” the key revocation. *Id.*, 5:63-65.

3. Reasons to combine Peterka and Traw

POSAs would have had numerous reasons to modify Peterka in view of Traw’s key revocation techniques and would have reasonably expected success in doing so. EX1041, ¶262; *see also id.*, ¶¶243-256.

First, Peterka and Traw are in the same field of art. EX1041, ¶¶263-264. Both describe systems that distribute secure content encrypted with content keys and

changing/rotating those keys. *Compare* Traw, Abstract, 1:65-2:2, 2:56-60, 3:13-19, 4:11-14, *with* Peterka, [0116]-[0121], FIG. 14. Both teach providing content keys to clients for decryption. *Compare* Traw, 3:63-66, 4:11-14, 5:5-19, FIGS. 1-3, *with* Peterka, [0080], [0105]-[0106], [0130], FIGs. 7B, 8. And both teach an identification mechanism for managing keys (e.g., “sequence number or time stamp” in Peterka and “key IDs” in Traw). *Compare* Traw, 3:32-46, *with* Peterka, [0082], [0110].

Second, Peterka and Traw share common objectives to prevent unauthorized access to content. *Compare* Peterka, [0135]-[0146] (describing “rules and conditions for providing content in a multicasting environment” to authorized clients), *with* Traw, 2:15-19 (describing protecting content from “unauthorized access”). Peterka recognizes the risk of security attacks and provides security mechanisms to protect against them—e.g., periodically rotating keys “at regular intervals,” “a time stamp” in key-distribution ECMs “to protect against replay attacks.” Peterka, [0105], [0110], [0121]; EX1041, ¶¶265-266. Traw likewise recognizes the benefits of periodic key renewals. *E.g.*, Traw, 3:63-66 (“[R]evocation of keys may be performed proactively on a periodic basis, rather than only reactively in response to an attack.”).

Third, POSAs understood well that notwithstanding Peterka’s described security mechanisms including key rotation, the security of systems like Peterka’s could be improved to address breaches. *See* EX1040 (Villasenor Dep.), 135:20-136:5, 139:7-140:24; *see also id.*, 136:6-25. For example, Traw recognizes the

benefits of “non-scheduled revocation” in systems like Peterka’s including for keys that “have been compromised” (*id.*, 6:39-49) and to protect against “a more general set of threats” or attacks (*id.*, 6:49-57). Peterka leaves to POSAs’ discretion how to rectify a security attack. *See* Peterka, [0110]; EX1041, ¶¶266-267. POSAs understood from Traw that compromised keys should be revoked, including in systems like Peterka with key rotation. Traw, 6:39-56; EX1041, ¶267. POSAs also understood that Traw’s security-driven key revocation teachings complement and support Peterka’s goal of limiting media access to authorized users—a goal Traw itself shares. EX1041, ¶267.

POSAs thus would have been motivated to improve Peterka’s system (*see* EX1040, 135:20-136:5, 139:7-140:24; *see also id.*, 136:6-25) in view of Traw by: (1) providing a notification to clients that a certain key is compromised and requires early expiration (Traw, 5:63-65, 4:62-65) using Peterka’s content packet “signaling methods” for key changes (Pet., 11; Peterka, [0116]-[0120]); (2) having the client obtain a replacement key using Peterka’s “pull” method (Pet., 11-12; Peterka, [0105]-[0106]) when notified that the current key has been revoked before the originally-scheduled expiration of the compromised key (Traw, 6:18-21); and (3) having the client apply the replacement key for decryption when the replacement key is received, before the originally-scheduled expiration of the compromised key in order to minimize service interruptions (Peterka, [0105]). EX1041, ¶268.

This modified system—“Peterka-Traw”—would have maintained Peterka’s overall system while beneficially improving security by including a mechanism to handle successful security attacks—namely, revoking and requiring replacement of a compromised key before it is set to expire (as taught by Traw). EX1041, ¶268.

POSAs would have reasonably expected success with Peterka-Traw, because Traw teaches a straightforward way to address security breaches easily adaptable to Peterka. EX1041, ¶269; Peterka, [0105]-[0106], [0116]-[0121], [0135]-[0138].

4. Substitute Claim 21

RMTA claim 21 amends original claim 1. RMTA, Claims App’x, i-ii. Unchanged claim limitations are obvious for the reasons set forth in Ground 1 (Pet, 19-37) and amended limitations are obvious over Peterka-Traw. EX1047, ¶343.

RMTA’s [21.P] is identical to the IMTA’s [21.P]. *Compare* RMTA, Claims App’x, i, *with* IMTA, 15. Peterka-Traw satisfies [21.P] for the same reasons Peterka did. Pet., 19. To the extent “for [OTT] media delivery” is limiting, Peterka-Traw satisfies it based on Peterka’s teaching to rotate keys in OTT streaming. *See* Pet., 3, 57; Peterka, [0015], [0038], FIG. 1; EX1003, ¶178; EX1047, ¶344.

[21.1] and [21.3] are unchanged and satisfied by Peterka-Traw for the reasons Peterka satisfies [1A] and [1C]. Pet., 19-22, 28-31; EX1047, ¶¶345, 358.

[21.2] adds a new requirement that the CEK identifiers are “each assigned to an associated [CEK]” and adds that the CEK identifiers are “uniquely identifying”

each associated [CEK] from every other [CEK] for the entire duration of a media playback.” [21.2] also adds that the media playback “correspond[s] to the media playback request response.” Peterka-Traw satisfies each of these additions.

Peterka-Traw includes Peterka’s sequence number or timestamp delivered to a client along with a CEK in an ECM/EMM, each of which POSAs understood constitutes a unique CEK identifier that identifies the specific key in the ECM/EMM. Pet., 25-26; Peterka, [0121]; EX1003, ¶¶91-92; EX1041, ¶¶274-277. This understanding of CEK identifier is consistent with the ’178 Patent, which likewise describes key identifiers “selected based on” other data such as “a segment number of the prepared content.” EX1001, 3:34-35, 4:8-10, 6:1-4, 6:17-19.

By virtue of being part of the key’s ECM/EMM, Peterka’s sequence number or timestamp is “assigned to an associated [CEK]” to the same extent disclosed in the ’178 Patent, which leaves to POSAs the details of how “identifiers” are “assigned.” EX1047, ¶¶347-349. Alternatively, directly “assign[ing]” an identifier “to an associated [CEK]” would have been obvious. EX1047, ¶¶350-356. Peterka’s FIG. 7B **shows** delivery of content keys with unique designations assigned to specific CEKs—CK₀, CK₁, CK₂—which would have motivated POSAs to implement Peterka’s client to receive and use an assigned key identifier to identify the content key parsed from an ECM/EMM. *Id.*; Pet. 26; EX1003, ¶94. Traw teaches assigned “key IDs” for targeted revocations. Traw, 3:32-46. Moreover, assigning

identifiers (e.g., key numbers) to CEKs to distinguish keys was a well-known key management technique. Suzuki, [0013], [0016], [0030]-[0031], [0043]-[0048], [0080]-[0084], FIG. 5; Pestoni, 12:16-35; EX1003, ¶¶93-96. In systems where multiple keys are utilized (e.g., Peterka-Traw), POSAs would have recognized the need to differentiate between keys, especially for scenarios where a *single* compromised key held by multiple clients needed to be targeted for revocation. EX-1047, ¶350 (citing Traw, 3:35, 4:45). Assigning CEK identifiers for such purposes would have constituted implementing known methods (assigned CEK identifiers) to known systems (Peterka-Traw’s key rotation system) to achieve predictable results (a key management scheme that distinguishes between keys). *KSR Int’l v. Teleflex*, 550 U.S. 398, 416 (2007); EX1047, ¶350. POSAs would have reasonably expected success using *assigned* key identifiers because this was a well-known option for key identifiers. EX1047, ¶351. Thus, Peterka-Traw meets PO’s “assigned” requirement or this limitation is obvious in view of the prior art discussed *infra* §II.B.

Also, because Peterka’s “sequence number” or “timestamp” is specifically included “*to protect against replay attacks*” during media playback (Peterka, [0121], POSAs understood that each sequence number/timestamp “uniquely identif[ies] each” ECM/EMM (and “[CEK]” within) “from every other” ECM/EMM and corresponding “[CEK] for the entire duration of a media playback.” EX1047, ¶353.

Alternatively, ensuring uniqueness of key identifiers “for the entire duration

of the media playback” was obvious. EX1047, ¶354. POSAs would have been motivated to ensure a client could uniquely identify keys even in scenarios where the client ultimately acquired all the keys needed for the entire duration of media playback. *E.g.*, EX2011 (Wechselberger Tr.), 39:7-40:13 (the “need to identify” and “know which key to use when” is “fundamental”); Pet., 25-26; EX1003, ¶¶94-96 (citing Suzuki, [0013], [0016], [0030]-[0031], [0043]-[0048], [0080]-[0084], FIG. 5; Pestoni, 12:16-35); EX1047, ¶355. Peterka *itself* illustrates such a scenario in FIG. 7B by showing content key identifiers—CK₀, CK₁, CK₂—that are unique for the entire program’s duration. Peterka, FIG. 7B; *id.*, FIG. 7A, [0092] (FIG. 7A “illustrate[s] an example where only two keys are required to decrypt the remainder of the program”); EX1047, ¶355. POSAs would have reasonably expected success using identifiers sufficiently unique to distinguish between CKs over the entire duration of media playback given Peterka’s teachings (Peterka, [0092], FIGs. 7A-7B) and because it was common to use key IDs sufficiently unique to allow clients track keys required to playback content. EX1047, ¶356; Pestoni, 12:4-35, FIG. 4.

POSAs understood that Peterka’s “media playback” also “correspond[s] to the media playback request response” as claimed, because the CKs Peterka’s client receives when it first requests/negotiates access to media content are used to decrypt and play back the media content the client sought access to. Pet., 19-22 (citing, *e.g.*, Peterka, [0080]-[0082], [0091]-[0092], [0141]-[0143]), 23-25, 28; EX1047, ¶357.

[21.3A] adds the requirement “applying a first key for content decryption, said first key having a first expiration time defining a time-based [CEK] rotation boundary.” Peterka-Traw satisfies this requirement.

Peterka discloses applying a first key (“content key”) for “decrypting the program content.” Peterka, [0106], [0116]; *see also id.*, [0090], [0092], [0108]; EX1047, ¶360. Peterka also describes periodically rotating keys “at regular intervals” (Peterka, [0082], [0110]) and that an ECM/EMM that carries a key to a client includes a field indicating “the time remaining in the lifetime of the key” being delivered in the ECM/EMM. Peterka, [0121]; *see id.*, [0106], [0105], FIG. 8; EX1003, ¶97. POSAs would have understood each key “expiration time” to define a “time-based [CEK] rotation boundary” for applying that key for decryption, after which a new key must be applied for decryption. EX1047, ¶¶361-362. Peterka-Traw’s client thus applies a first key for content decryption having a first expiration time that defines a time-based CEK rotation boundary. EX1047, ¶362.

[21.4] adds the requirement of detecting “a notification, the notification including a notification-based [CEK] rotation boundary” wherein “the notification requires expiration of said first [CEK] earlier than said time-based [CEK] rotation boundary for said first key” and “after said notification-based [CEK] rotation boundary for said first key.” By focusing on the compromised key scenario (RMTA, 2), [21.4] tries to change the meaning of the “detecting” limitation in the same way

that PO says the original “detecting” limitation should be construed. POR, 43-49.

Regardless, Peterka-Traw satisfies this limitation. EX1047, ¶¶364-366. Traw teaches revoking a key that has been compromised due to a security breach *before* that key would ordinarily be rotated (Traw, 3:17-19, 5:29-31, 5:35-39, 6:12-21, 6:39-57) and notifying client devices of such revocations (*id.*, 4:62-65, 5:63-65). EX1047, ¶364. In Peterka-Traw, keys would ordinarily be rotated based on the time-based CEK rotation boundary as described above in [21.3A]. Peterka, [0105], [0110], [0121]; EX1047, ¶365. Further, in Peterka-Traw, notifications of these unscheduled key revocations are transmitted to (and detected by) the client using Peterka’s key change signaling methods. EX1047, ¶366; Peterka, [0116]-[0120]. POSAs would understand the notification as a signal to stop using the CEK; it is thus a notification-based CEK rotation boundary. EX1047, ¶366. Peterka-Traw’s client thus detects a notification-based CEK rotation boundary where the notification requires expiration of the first CEK earlier than the time-based CEK rotation boundary for the first key and after the notification-based CEK rotation boundary for the first key.

PO’s amendments in [21.5] (*supra* p. 3) are again aimed at capturing the “compromised key” scenario discussed above for [21.4]. Peterka-Traw satisfies this clause. EX1047, ¶¶367-377. In Peterka-Traw, the client keeps track of its keys and issues a request for a new key in a manner that avoids “service interruptions.” Peterka, [0105]. As explained in [21.3A], POSAs would have understood that the

current key is set to expire (the key rotates) at the time-based CEK rotation boundary. EX1047, ¶370. POSAs would have been motivated to implement Peterka-Traw such that when the client detects an unscheduled key revocation (Traw, 3:17-19, 4:63-65, 5:35-65, 6:12-21, 6:39-57) using Peterka’s key change signaling methods (Peterka, [0116]-[0120]), the client requests a new key immediately, so that it can be used before the current (compromised) key is set to expire. EX1047, ¶¶371-373. This would minimize the impact of service interruptions. EX1047, ¶373; Peterka, [0105].

PO’s attorney argues that neither Peterka nor Traw teach a client requesting a key in response to receiving notice that a key must be changed. RMTA, 16-17. This assertion makes no sense in the context of Peterka, which teaches that under the pull key distribution model relied upon by Petitioner, “the responsibility of determining when a new key is required” is “passed to the client” and “each client requests a new key and is individually responded to by the key distribution server.” Peterka, [0106], [0110]. Based on Peterka’s teachings, POSAs understood that “in response to” *any* scenario where Peterka’s client determines a new key is required to decrypt content—including scenarios where the client does not have a required key due to notice that a key has been revoked—the client requests a new key. EX1047, ¶374.

PO’s attorney argument also misreads Traw, asserting that Traw only “teaches that a notification instructs the client to change to a key that the client has already been provided.” RMTA, 16. This is wrong. Traw discloses “requir[ing]” content

protection implementations to be “renewable... *in the event* of revocation” (e.g., in response to a revocation due to a compromised key), which Traw says can be “achieved by an on-line download of... a new content protection implementation.” Traw, 2:43-64. Traw’s disclosure of having keys be renewable via a “download” “in the event” of revocation is unsurprising: the basic, unremarkable concept of a client requesting a new key in response to notice that a key has been revoked was well-known in client-server contexts (e.g., EX1048, [0017]-[0018], FIG. 1; EX1049, [0147]-[0155]), and far from inventive in the Peterka-Traw context, given the desirability of minimizing service interruptions. EX1047, ¶¶375-377; Peterka, [0105].

As with the IMTA, [21.6] (*supra* p. 3, §I.A) was revised to *eliminate* the “ahead of”/“after” step sequence relative to “the key rotation boundary” recited in original claim 1. Regardless, Peterka-Traw satisfies this limitation. EX1047, ¶378. POSAs would have been motivated to implement Peterka-Traw to minimize “service interruptions” (Peterka, [0105]), such that when the client receives the second (replacement) key due to Traw’s unscheduled key revocation (Traw, 3:17-19, 4:63-65, 5:35-39, 5:63-65, 6:12-21, 6:39-57), the client promptly applies the second key for decryption, before the current key is set to expire (i.e., before “said time-based [CEK] rotation boundary for said first key”), allowing the client to resume consuming content. EX1047, ¶379; Peterka, [0106], [0116]; EX1003, ¶124.

5. Substitute Claim 22

Substitute claim 22 mirrors original claim 2. RMTA, Claims App’x, ii. Unchanged claim limitations are obvious for the reasons set forth in Ground 1. Pet., 37; EX1047, ¶380. Claim 22 newly requires the second CEK expiration time to be “equal to the remaining lifespan of said first expiration time at the time said first [CEK] was expired.” Peterka-Traw satisfies this limitation. EX1047, ¶381.

POSAs understood there were three options for setting the expiration time of a replacement key: (1) *before* the original key expiration; (2) *at the same time* as the original key expiration; or (3) *after* the original key expiration. EX1047, ¶382. All three options would have been obvious to try. *Id.*; *KSR*, 550 U.S. at 421.

POSAs had multiple reasons to try setting the second CEK’s expiration time to be equal to the time remaining lifespan for the prior CEK. *First*, the remaining lifespan of the first (compromised) CEK was already known to both the client and the server, and setting the CEK expiration time for the second CEK as equal to the remaining lifespan for the first CEK would minimize the need to adjust any existing time variables associated with the upcoming key rotation. EX1047, ¶384. *Second*, adjusting the second CEK’s expiration time such that it was not the same time as the first CEK would have required changing already-staged key rotation boundaries tied to future media segments, including interstitial segments like ads, previews, etc. that were common in multicast content distribution. *Id.*, ¶385 (citing Peterka, [0122],

FIG. 7B; Peterka308, [0024], [0029], [0032]; Chen, [0034]-[0044], FIGs. 2A-2C). Using the remaining lifespan of the original (first) key would avoid the need to adjust these already-staged rotation boundaries. *See* EX1047, ¶384.

Further, given Traw’s disclosure that its revocation can target a single key (Traw, 3:35, 4:45), POSAs would have reasonably expected success revoking a single key and replacing it, leaving all other variables alone. EX1047, ¶386.

6. Substitute Claim 23

Substitute claim 23 mirrors original claim 3 and requires the second CEK expiration time to be “equal to the first expiration time plus the remaining lifespan of said first expiration time at the time said first [CEK] was expired.” RMTA, Claims App’x, ii. Unchanged limitations are obvious as set forth in Ground 1. Pet., 38-41.

Claim 23’s amendment falls within option #3 described above for substitute claim 22: expiration for the second (replacement) CEK *after* the expiration of the first (compromised) key. EX1047, ¶388. As noted above, setting the second CEK’s expiration time for *after* the first (compromised) CEK’s expiration was one of three obvious-to-try options. *Id.*, ¶389; *KSR*, 550 U.S. at 421. POSAs would have understood that setting the second CEK to both be applied *before* the first (compromised) key expires² and then expire *after* the first CEK would have expired³

² As discussed *supra* §II.A.4, this was obvious and would have satisfied [21.6].

³ As discussed *supra*, this was obvious to try.

would mean that the CEK originally staged to be applied to the next media segment was no longer usable for the upcoming segment. EX1047, ¶390.

To address this, POSAs would have been motivated to set the second CEK's expiration time to be equal to the remaining lifespan for the pre-existing expiration set for the first CEK plus the fixed expiration time (period duration) originally assigned for the first CEK. *Id.* This would provide Peterka-Traw's servers an additional key rotation period to better handle potential latency issues that would predictably arise from numerous clients attempting to replace the compromised key *and* the now-defunct key that was originally staged. *Id.*; Peterka, [0080] (noting the issue of "a large load on the caching server on the segment boundaries"). This implementation also would avoid disrupting the encryption/decryption of future media segments by desirably allowing POSAs to avoid adjusting already-staged key rotation boundaries. Peterka, [0122], FIG. 7B; EX1047, ¶390 (citing Peterka308, [0024], [0029], [0032]; Chen, [0034]-[0044], FIGs. 2A-2C).

POSAs also would have reasonably expected success with such an implementation because it involves using less than two key rotation periods to give the servers the chance to resume regular key distribution processes. EX1047, ¶391.

7. Substitute Claims 24-26 and 29

Claims 24-26 and 29 are unchanged. Peterka-Traw meets claim 24-26 and 29 for the same reasons Peterka satisfies claims 4-6 and 10. Pet., 41-47; EX1047, ¶392.

8. Substitute Claim 30

Substitute claim 30 amends dependent claim 12 and mirrors its structure but adds the following limitations: “retrieved content is divided into content segments, and said second [CEK] is applied to decrypt the same content segment for which the first [CEK] was used” and “notification-based expiration of the first [CEK] is for security reasons.” RMTA, Claims App’x, iv. Claim 30’s unchanged limitations are obvious for the same reasons set forth in Ground 1. Pet., 48. Peterka-Traw renders obvious the amended limitation. EX1047, ¶¶393-394.

Peterka discloses content divided into segments encrypted (and decrypted) with a different key. Pet., 10, 36-37; Peterka, [0080]-[0082], [0091]-[0101], [0106], [0116], [0121]-[0125], FIGs. 7A-7B. Peterka’s modified system in Peterka-Traw includes a mechanism for responding to security attacks: revoking and requiring replacement of a compromised key before its set expiration. The second CEK is used to decrypt content originally slated to be decrypted by the first (compromised) CEK, and the early expiration of the first (compromised) CEK is for security reasons. Traw, 1:65-2:2, 2:15-19, 3:65-66, 4:37-39, 5:5-39, FIG. 2; EX1047, ¶¶395-396.

9. Substitute Claims 33-35, and 37

Substitute claim 33 amends original claim 16 the same way substitute claim 21 amends claim 1. RMTA, Claims App’x, i-ii, iv-v. Peterka-Traw’s computerized device satisfies substitute claims 33-35 and 37 for the same reasons described above for proposed substitute claims 21-23 and 30. EX1047, ¶397.

B. Additional Traw Combinations (Grounds 6B-6E)

POSAs would also have combined Traw with the original grounds set forth in the Petition (Grounds 2-5), for the same reasons discussed *supra* §II.A.3. EX1047, ¶398. Grounds 6B-6E meet substitute claims 21-26, 29-30, 33-35, and 37 for the same reasons discussed *supra* §§II.A.4-II.A.9, ***and also*** meet substitute claims 27-28, 32, and 36 for the reasons discussed in Grounds 2-5:

Ground and Reference(s)		Substitute Claims
6B	Peterka, Suzuki, Traw	21-26, 29-30, 33-35, 37
6C	Peterka, Bocharov, Traw	21-26, 29-30, <u>32</u> -35, 37
6D	Peterka, Suzuki, Bocharov, Traw	21-26, 29-30, <u>32</u> -35, 37
6E	Peterka, Bocharov, Peterka308, Chen, Traw	<u>27-28</u> , <u>36</u>

If PO argues that Peterka-Traw does not disclose PO’s new [21.2] requirement that the CEK identifiers are “each assigned to an associated [CEK],” at least Grounds 6B and 6D, which rely upon Suzuki’s “key number” teachings to modify the base combination, meet this clause. Grounds 6B and 6D implement Peterka’s system to include Suzuki’s “key number for identifying the key” (Suzuki, [0030]) to help the client keep track of keys, e.g., when determining which key to apply to decrypt a particular segment of content. Pet., 51-55 (citing Suzuki, [0030], [0043]-[0048], [0080], FIG. 2; EX1003, ¶¶161-172), 66-68 (citing EX1003, ¶¶201-207). POSAs recognized the importance of using identifiers for keys (like Suzuki’s key numbers) in multiple-key systems to help differentiate amongst keys and further recognized

that unique identifiers (like Suzuki's key numbers) helped ensure the system does not confuse keys. Pet., 52-53; EX1003, ¶164. This would have been especially important in Peterka-Traw for single-key revocation scenarios. EX1047, ¶¶399-400.

Suzuki's key numbers (for identifying keys) (Suzuki, [0030]) in Ground 6B and 6D meet [21.2]'s "assigned" requirement. POSAs understood that each key number in those implementations was "assigned" to a key because the "key number" is information that is specifically associated with the key to facilitate "identifying the key." EX1047, ¶401; Suzuki, [0013].

Moreover, implementing Suzuki's "key number for identifying the key" (Suzuki, [0030]) to be sufficiently "unique" to distinguish amongst keys "for the entire duration of a media playback," as claimed would have been obvious. *See supra* p. 14. POSAs would have been motivated to ensure (and reasonably expected success that) a client could uniquely identify keys even in scenarios where the client ultimately acquired all the keys needed for the entire duration of media playback because the "need to identify" and "know which key to use when" is "fundamental" to "anybody who has worked with crypto-based content information distribution systems" (EX2011, 39:7-40:13), because Peterka *itself* illustrates such a scenario (Peterka, [0092], FIGs. 7A-7B), and because it was common to use key IDs sufficiently unique to allow clients to keep track of keys required to playback a piece of content (*e.g.*, Pestoni, 12:4-35, FIG. 4). EX1047, ¶402.

Respectfully submitted,

Date: December 4, 2025

/Turhan Sarwar/

Turhan F. Sarwar, admitted *pro hac vice*
WOLF, GREENFIELD & SACKS, P.C.

CERTIFICATE OF SERVICE UNDER 37 C.F.R. § 42.6 (e)(4)

I certify that on December 4, 2025, a copy of the foregoing document, including any exhibits filed therewith, is being served via electronic mail, as previously consented to by Patent Owner, upon the following:

Peter C. Knops
Kayvan B. Noroozi

peter@noroozipc.com
kayvan@noroozipc.com

Date: December 4, 2025

/Dara Del Rosario/
Dara Del Rosario
Paralegal
WOLF, GREENFIELD & SACKS, P.C.