

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KAHOOT! ASA & KAHOOT EDU, INC.,
Petitioner,

v.

AVIEL D. RUBIN,
Patent Owner.

IPR2023-00693
Patent 9,064,376 B1

Before KEN B. BARRETT, KEVIN W. CHERRY, and
CYNTHIA L. MURPHY, *Administrative Patent Judges*.

MURPHY, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Granting In-Part and Denying In-Part
Patent Owner's Noncontingent Motion to Amend
35 U.S.C. § 318(a)

I. INTRODUCTION

This *inter partes* review proceeding includes the following cast: Kahoot! ASA and Kahoot EDU, Inc. (“Petitioner”), Dr. Aviel Rubin (“Patent Owner”), and U.S. Patent No. 9,064,376 B1 (Ex. 1001, “the ’376 Patent”).¹

The timeline of events begins with Petitioner filing a Petition (Paper 1, “Pet.”) to institute review of claims 1–5, 9–10, 12–17, and 23–25 of the ’376 Patent, and, at least as of today, ends with this Final Written Decision.² Intermediate events in this timeline include Institution (Paper 10), Patent Owner’s Motion to Amend (Paper 19, “MTA”), Patent Owner’s Revised Motion to Amend (Paper 30, “RMTA”), and an Oral Hearing (Paper 36, “Tr.”), with expected papers being interspersed therebetween.³

The RMTA is non-contingent, and, therefore, Patent Owner is making two requests: 1) cancel the claims challenged in the Petition; and 2) add the substitute claims proposed in the motion. We grant in-part the RMTA by canceling the claims challenged in the Petition. We deny in-part the RMTA by not adding the proposed substitute claims.

¹ The parties identify themselves the real parties in interest, and list *Rubin v. Kahoot! ASA et al.*, Civil Action No. 1:23-cv-031-LY (W.D. Tex.) as a related matter. *See* Pet. 96, Paper 4, 2.

² This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a). We have statutory authority to do so under 35 U.S.C. § 6.

³ Patent Owner filed a Preliminary Response to the Petition (Paper 8), Petitioner filed an Opposition to the MTA (Paper 20), we issued Preliminary Guidance on the MTA (Paper 21), Petitioner filed an Opposition to the RMTA (Paper 27), Patent Owner filed a Reply to Petitioner’s RMTA opposition (Paper 30), and Petitioner filed a Sur-reply to Patent Owner’s Reply (Paper 32).

II. THE '376 PATENT

The methods/systems disclosed in the '376 Patent involve “a first [electronic] device” and “a second [electronic] device.” Ex. 1001 2:29–30.

A. *Architecture*

The invention's architecture includes a first device which can be “a computer, a tablet, a smartphone or other electronic device,” and a second device which can be “a computer, tablet, smartphone or another type of electronic device.” Ex. 1001, 2:40–44. “Any combination of electronic devices can be used.” *Id.* at 2:44–45. Thus, for example, if a user named John Doe (*see id.* at Fig. 10) possesses a computer, a tablet, and a smartphone, the invention's architecture could include John's computer as the first device and John's smartphone as the second device.

B. *Two Factor Authentication*

The '376 Patent backgrounds the invention by comparing it to two-factor authentication. *See* Ex. 1001, 1:53–67. The '376 Patent explains that, with two-factor authentication, a user “logs into” a first device, the second device “receives code, for example by text or email,” and “the user is instructed to enter that code into the first device, where the rest of the interaction with the application takes place.” *Id.* at 1:56–61. “In two-factor authentication, the second device is no longer needed once the authentication takes place.” *Id.* at 1:64–65.

John would use both his computer (i.e., his first device) and his smartphone (i.e., his second device) with two-factor authentication. John would log into his computer, John would receive a code on his smartphone, and John would enter the code into his computer. The rest of John's

interaction would take place on his computer (i.e., his first device). Thus, with two-factor authentication, John's smartphone (i.e., his second device) would be "part of the authentication process." *Id.* at 1:58–59. But after John receives the code, he can turn off his smartphone and place it out of sight in a drawer while he interacts with an application on his computer.

C. Disclosed Methods/Systems

The '376 Patent discloses the methods/systems in which John needs to use both his computer (i.e., his first device) and his smartphone (i.e., his second device). *See id.* at 2:29–31. The '376 Patent discusses these methods/systems in the context of gaming preferred embodiments (*see id.* at 2:46–7:30, Figs. 2–6) and in the context of banking preferred embodiments (*see id.* at 7:31–10:22, Figs. 8–10).

In gaming embodiments, John is playing a game of online poker that involves "community cards" that "everyone sees," and "secret 'hole' cards" that only he should see. John uses his computer (i.e., his first device) to receive information corresponding to a virtual poker table with community cards placed faceup thereon. John uses his smartphone (i.e., his second device) to receive information corresponding to his hole cards. John's "sensitive information" (i.e., his hole cards) are "not displayed on the first device." *Id.* at 3:13–14. Thus, if John's computer (i.e., his first device) is attacked with malware, the attacker "cannot gain access to the sensitive information." *Id.* at 3:15–17.

In banking embodiments, John is performing a banking activity, "such as viewing an account balance or performing a funds transfer, or performing a bill payment." *Id.* at 7:53–55. John uses his computer (i.e., his first device)

to send a request related to the banking activity (e.g., a request for an account balance); and John uses his smartphone (i.e., his second device) to receive information about the requested banking activity (e.g., the requested account balance). Thus, “[e]ven if an attacker compromised” John’s computer (i.e., his first device), the attacker would not be able to do anything damaging,” as “part of the activity is performed on” John’s smartphone (i.e., his second device. *Id.* at 9:2–4.

III. ISSUED CLAIMS

The ’376 Patent issued with claims 1–25, with claims 1 and 25 being independent claims. *See* Ex. 1001, 15:18–38, 17:5–28.⁴ These two independent claims are reproduced below with our bolded annotations and slightly altered paragraphing.

[Issued Claim 1]. A **method** for transmitting information to multiple electronic devices, the method comprising:
electronically **storing** a set of information at a server,
identifying a first subset of the information and
identifying a second subset of the information, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application;
determining at the server whether both a first device in possession of and being directly operated by a first user and a second device also in possession of and being directly operated by the first user are accessible over at least one electronic communications network based on the first user being logged into the application at both the first and second devices;

⁴ In the Petition, Petitioner challenges the patentability of issued claims 1–5, 9–10, 12–17, and 23–25 on prior art grounds. *See* Pet., 1–2. As we grant Patent Owner’s request to cancel these claims, we need not consider the persuasiveness of Petitioner’s prior art grounds.

if and only if both the first and second devices are determined to be accessible by the server, then:

transmitting a first subset of the information to the first device from the server; and

transmitting a second subset of the information to the second device from the server,

wherein the second subset of the information includes information not transmitted to the first device.

[Issued Claim 25]. A system for transmitting information to multiple electronic devices, the system comprising:

an electronic data store configured for electronically **storing** a set of information at a server, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application;

a processor device programmed for:

identifying a first subset of the information and **identifying** a second subset of the information;

determining at the server whether both a first device in possession of and being directly operated by a first user and a second device also in possession of and being directly operated by the first user are accessible over at least one electronic communications network based on the first user being logged into the application at both the first and second devices;

if and only if both the first and second devices are determined to be accessible by the server, then:

transmitting a first subset of the information to the first device from the server; and

transmitting a second subset of the information to the second device from the server,

wherein the second subset of the information includes information not transmitted to the first device.

As signaled by our **bolded** annotations, Issued Claims 1 and 25 introduce a method/system in a preamble, and recite storing, identifying, determining, and transmitting steps. The recited steps involve a user (i.e., “a first user”), a first device (i.e., “a first device in possession of and being

directly operated by [the user]”), a second device (i.e., “a second device also in possession of and being directly operated by [the user]”), “a server,” and “first and second subsets of information.” The transmitting steps include “transmitting a second subset of the information to the second device from the server,” wherein “the second subset of the information includes information not transmitted to the first device.”

IV. RMTA CLAIMS

In the MTA, Patent Owner requested the addition of substitute claims 26–41, with claim 26 being an amended version of issued claim 1 and claim 41 being an amended version of issued claim 25. *See* MTA, Appx. A, 3–8. In the RMTA, Patent Owner requested further amendments be made to substitute claims 26 and 41. *See* RMTA, Appx. A, 3–4, 7–8.⁵

Thus, independent claims 26 and 41, as further amended in the RMTA, are now before us. These two independent claims are reproduced below with a clean incorporation of the proposed amendments, our bolded annotations, slightly altered paragraphing.

[RMTA CLAIM 26]. A **method** for protecting information by transmitting information to multiple electronic devices, the method comprising:
electronically **storing** a set of information at a server;
identifying a first subset of the information and
identifying a second subset of the information, wherein the first

⁵ Petitioner challenges the patentability of substitute claims 25–35 and 37–41 on prior art grounds. *See* Paper 27, 4–35, Paper 32, 5–12. As we deny Patent Owner’s request to add these claims to the Patent, we need not consider the persuasiveness of Petitioner’s prior art challenges of these claims.

and second subsets of information are generated by the same application at the server and are specific to that application;

determining at the server whether both a first device in possession of and being directly operated by a first user and a second device also in possession of and being directly operated by the first user are accessible over at least one electronic communications network based on the first user being logged into the application using application specific authentication information that is not specific to a device at both the first and second devices, wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device;

if and only if both the first and second devices are determined to be accessible by the server, then:

transmitting the first subset of the information to the first device from the server; and

transmitting the second subset of the information to the second device from the server,

wherein the second subset of the information includes information not transmitted to the first device **thereby** protecting the second subset of the information not transmitted to the first device from potential malware on the first device.

[RMTA CLAIM 41]. A **system** for protecting information by transmitting information to multiple electronic devices, the system comprising:

an electronic data store configured for electronically **storing** a set of information at a server, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application a set of information at a server;

a processor device programmed for:

identifying a first subset of the information and **identifying** a second subset of the information;

determining at the server whether both a first device in possession of and being directly operated by a first user and a second device also in possession of and being directly operated

by the first user are accessible over at least one electronic communications network based on the first user being logged into the application using application specific authentication information that is not specific to a device at both the first and second devices, wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device[;]

if and only if both the first and second devices are determined to be accessible by the server, then:

transmitting a first subset of the information to the first device from the server; and

transmitting a second subset of the information to the second device from the server,

wherein the second subset of the information includes information not transmitted to the first device **thereby** protecting the second subset of the information not transmitted to the first device from potential malware on the first device.

As signaled by our **bolded** annotations, RMTA Claims 26 and 41, like Issued Claims 1 and 25, introduce a method/system in a preamble, and recite storing, identifying, determining, and transmitting steps. RMTA Claims 26 and 41, like Issued Claims 1 and 25, involve a user, a first device, a second device, a server, and first and second subsets of information. The transmitting steps in RMTA Claims 26 and 41, like the transmitting steps in Issued Claims 1 and 25, include “transmitting a second subset of the information to the second device from the server,” wherein “the second subset of the information includes information not transmitted to the first device.”

The RMTA Claims 26 and 41 (unlike Issued Claims 1 and 25) have a closing thereby clause which reads “thereby protecting the second subset of

the information not transmitted to the first device from potential malware on the first device.”

Patent Owner explains that RMTA Claims 26 and 41 “recite a number of steps” (i.e., the storing, identifying, determining, and transmitting steps) that “when taken together, can isolate information shared with an application [user’s] first and second devices.” RMTA 5. However, if the information sent [to] the second device is not ultimately protected from malware on the first device then the invention is not achieved.” *Id.* Thus, the thereby clause “makes protecting of the second subset of information a requirement of the claims rather than an aspiration result of the practice of the steps.” *Id.*

Patent Owner’s expert further explains that “[a]bsence of the ‘thereby’ clause could technically allow a system to perform the steps of the ’376 patent but not protect the second subset of information sent the second device.” Ex. 2009 ¶ 85. In other words, performing the storing, identifying, determining, and transmitting steps set forth in Issued Claim 1 and Issued Claim 25 would not necessarily provide protection against malware. Although these steps are “are meant, in part, to create isolation between the information sent to the first and second devices,” this isolation could be “undermine[d] by other means.” *Id.* For example, the second subset of information would not be protected if the method/system “allow[s] the first device to access the second device, or allow[s] the broad access to the application server.” *Id.*

During the hearing, it was further explained that “[i]f you send the information to the two devices and the first device has full access to everything on the second device, then there’s no isolation and there’s no

protection.” Tr. 36. Thus, “this limitation is actually extremely material to patentability because without it, you would be sort of technically infringing the patent in the sense that you practice the steps, but your information is not protected.” *Id.*

Notably, this narrowing injects further responsibilities into the recited steps, as they now must do more than just isolate the second subset of information. The storing/identifying/determining/transmitting steps must now do something beyond isolation to protect the second subset of information from potential malware on the first device. They must, for example, not allow the first device to access the second device and/or not allow broad access to the application server.

V. CLAIM CONSTRUCTION

In this proceeding, we use “the same claim construction standard that would be used to construe the claim[s] in a civil action under 35 U.S.C. [§] 282(b).” *See* 37 C.F.R. § 42.100(b) (2020). This claim construction standard includes construing claims in accordance with the ordinary and customary meaning of such claims as would have been understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. *See id.*; *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (*en banc*). Only claim terms in controversy need to be construed, and only to the extent necessary to resolve the controversy at hand. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017); *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

We determine that no explicit construction of any claim term is needed to resolve the dispositive issues in this case.

VI. PERSON OF ORDINARY SKILL IN THE ART (POSITA)

Petitioner portrays a person of ordinary skill in the art as having “a bachelor’s degree in electrical or computer engineering or computer science or a comparable field of study, plus approximately two years of professional experience in the field of computer and security and/or network design and security or other relevant industry experience.” Pet. 5. Patent Owner agrees with the portrayal, except for the phrase “other relevant industry experience.” MTA, 7. For the purposes of this proceeding, we adopt Petitioner’s portrayal of POSITA, minus the “other relevant industry experience” phrase.

VII. ANALYSIS

We deny Patent Owner’s request to add the proposed substitute claims to the ’376 Patent because the RMTA fails to meet meets “statutory and regulatory requirements.” *Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, Paper 15 at 4 (PTAB Feb. 25, 2019) (precedential, “*Lectrosonics*”).

The statutory and regulatory requirement relevant here is that a motion to amend may not “introduce new matter.” 35 U.S.C. § 316(d)(3); 37 C.F.R. § 42.121(a)(2)(ii). Patent Owner “must satisfy the Board” that this no-new-matter requirement is “met.” *Aqua Prods., Inc. v. Matal*, 872 F.3d 1290, 1305–06 (Fed. Cir. 2017) (*en banc*). Patent Owner “bears the burden of persuasion” to show that its revised motion to amend “complies with” this requirement. 37 C.F.R. § 42.121(a)(2)(ii).

To ensure this requirement is met, a motion to amend must set forth “support in the originally filed disclosure of the subject patent for each proposed substitute claim.” *See* 37 C.F.R. §§ 42.121(b)(1), 42.121(b)(2). The ’376 Patent issued from U.S. Patent Application No. 14/444,995 (the “’995 Application”).⁶ *See* Ex. 1001 codes 21, 22.⁷ In the RMTA, Patent Owner lists citations to the ’995 Application as support for each proposed substitute claim.

A. Written Description

The test for sufficiency of a written description is whether the disclosure “clearly allow[s] persons of ordinary skill in the art to recognize that [the inventor] invented what is claimed.” *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc) (quoting *Vas-Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1562–63 (Fed. Cir. 1991)). The disclosure must “reasonably convey[] to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date.” *Ariad*, 598 F.3d at 1351.

“While the written description requirement does not require that the specification recite the claimed invention in any particular way, pointing to

⁶ Our subsequent references to the ‘995 Application and parts thereof (e.g., abstract, paragraphs, drawings) correspond to its condition as filed on July 28, 2014.

⁷ The Patent lists a provisional application, filed on June 6, 2014, as related domestic application data. *See* Ex. 1001 code (60). Patent Owner does not rely on this provisional application in the RMTA. *See* RMTA, 2–7. As such, we do not take the disclosure of the provisional application into consideration.

an ‘amalgam of disclosures’ from which an artisan could have created the claimed invention does not satisfy this requirement.” *Flash-Control, LLC v. Intel Corp.*, No. 2020-2141, 2021 WL 2944592, at *3 (Fed. Cir. July 14, 2021) (non-precedential) (quoting *Novozymes A/S v. DuPont Nutrition Biosciences APS*, 723 F.3d 1336, 1349 (Fed. Cir. 2013)). Put another way, Patent Owner can not just invite us “to go on a hunting expedition to patch together after the fact a synthetic definition of an invention.” *Indivior UK Ltd. v. Dr. Reddy’s Labs. S.A.*, 18 F.4th 1323, 1329 (Fed. Cir. 2021) (quoting *Brenner v. Manson*, 383 U.S. 519, 536 (1966)).

B. Patent Owner’s Citations

Patent Owner cites to the Abstract, over thirty paragraphs (Paragraphs 2, 18–20, 23–29, 33, 34, 38, 39, 55, 58, 61, 63–65, 74, 75, 78, 81–83, 89, 90, 92, and 93) and seven drawings (Figures 3, 4–7, 9, and 10) in the ‘995 Application as written description support for RMTA Claims 26 and 41. *See* RMTA, 3–4, 6–7.

These citations, scattered through the ‘995 Application, pertain, individually, to the invention’s general architecture (Paragraph 19), gaming embodiments (Paragraphs 23–29, 38, 39, Figs. 2, 4–6), banking embodiments (Paragraphs 74, 75, Figs. 9, 10), registration procedures (Paragraphs 89, 90, 92), and an accessibility determination (Paragraphs 33, 34). *See* Ex. 1003, 10–16, 23–24, 27–28, 41, 43–45. Patent Owner also includes some citations pertaining to a customized second device (Paragraphs 82, 83). *See id.* at 25. And several citations appear to be there simply because they mention the word “malware” (Paragraphs 20, 55, 61, 63–65, 78, 81, 93, Fig. 7). *See id.* at 11, 19, 20–21, 24, 25, 28, 46.

Patent Owner's no-new-matter position, as best we understand it, is that POSITA could patch this amalgam of citations together to create a completed puzzle corresponding to the method/system set forth in RMTA Claims 26 and 41. Assuming this patchwork project is even plausible with respect to the storing, identifying, determining, and transmitting steps set forth in Issued Claims 1 and 25, POSITA would reach a breaking point when it comes to the heightened responsibilities imposed by the thereby clause in RMTA Claims 26 and 41.

The thereby clause injects further responsibilities into storing, identifying, determining, and/or transmitting steps, as they now must do something beyond-isolation to protect the second subset of information from potential malware on the first device. *See* RMTA, 30, 5; Tr. 36, Ex. 2009 ¶ 85. They must, for example, not allow the first device to access the second device and/or not allow broad access to the application server. *See id.*

In order for RMTA Claims 26 and 41 to satisfy the no-new-matter requirement, the listed citations for the thereby clause and the storing/identifying/determining/transmitting steps must provide written description support for beyond-isolation protection of the second subset of information. As discussed below, Patent Owner does not adequately explain why they do.

i. The Thereby Clause

The thereby clause sets forth “thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first device.” RMTA, Appx. A, 4, 8.

Most of the listed citations for the thereby clause (i.e., Paragraphs 20, 55, 61, 63–65, 78, 81, 83, 93, Figs. 7, 9, 10) seem to mention the word

“malware.” *See* RMTA, 4, 6–7; Ex. 1003, 11, 19–21, 24, 25, 28, 46, 48, 49. But even if listed citations echo exactly the language of the thereby clause, that alone would not be enough. “The more telling question” is whether these citations show possession of “how” the recited protection is achieved. *Vasudevan Software, Inc. v. MicroStrategy, Inc.*, 782 F.3d 671, 683 (Fed. Cir. 2015). Patent Owner does not adequately explain how the listed citations provide written description support for beyond-isolation protection of the second subset of information is achieved.

ii. The Storing Step

The storing step sets forth “storing a set of information at a server.” *See* RMTA, Appx. A, 3, 7.

The listed citations for the storing step (Paragraphs 25, 38, 39, 89, 90, Figs. 5, 6) describe information being sent/displayed to the two devices in gaming embodiments, and storing registration information. *See* RMTA 3, 6; Ex. 1003, 12, 16, 27, 28, 44, 45. Patent Owner does not explain how these alleged descriptions of storing information provide written description support for beyond-isolation protection of the second subset of information. Patent Owner does not explain, for example, how the listed citations protect against broad access to an application server.

iii. The Identifying Steps

The identifying steps set forth “identifying a first subset of the information and identifying a second subset of the information.” *See* RMTA, Appx. A, 3, 7.

The listed citations for the identifying steps (Paragraphs 23–27, 34) may describe how, in gaming embodiments, a first subset of information

(e.g., a virtual poker table) is displayed on the first device and a second subset of information (e.g., the hole cards) is displayed on the second device. *See* RMTA 3, 6; Ex. 1003, 11, 12, 14, 15. But they don't seem to actually discuss when, where, or how these subsets of information are identified, or even what does the identifying.⁸ *See id.* In any event, Patent Owner does not explain how the listed citations describe identifying steps that do something beyond isolation to protect the second subset of information from potential malware on the first device.

iv. The Determining Step

The determining step sets forth an accessibility determination (i.e., “determining at the server whether” both the first device and the second device “are accessible over at least one electronic communications network”). *See* RMTA, Appx. A, 3, 7–8. This accessibility determination is based on the user “being logged into the application using application specific authentication information that is not specific to a device at both the first and second devices.” *Id.* at 3, 8. And “the application specific authentication information used on the first device is different from the application specific authentication information used on the second device.” *Id.* at 3–4, 8.

The listed citations for the determining step (Paragraphs 33, 76, 83, 89, 90, 92, Figure 10) pertain to an array of topics, including an accessibility determination (Paragraph 33), different passwords (Paragraphs 75, 90,

⁸ RMTA Claims 26 and 41 do not require the identifying steps to be performed by a server (or anything else for that matter), they only require the first and second subsets of information to be “generated by the same application at the server.”

Figure 10), a custom second device (Paragraph 83), registration information (Paragraph 89), and authentication tokens (Paragraph 92). *See* RMTA 3–4, 6; Ex. 1003, 14, 23–25, 27, 28, 49. Patent Owner does not explain how any of these topics, individually or collectively, contribute to the beyond-isolation protection provided by RMTA Claims 26 and 41 thanks to the thereby clause.

v. The Transmitting Steps

The transmitting steps set forth “transmitting the first subset of the information to the first device from the server,” and “transmitting the second subset of the information to the second device from the server.” *See* RMTA, Appx. A, 4, 8. These transmissions occur “if and only if both the first and second devices are determined to be accessible by the server.” *Id.* And the “the second subset of the information includes information not transmitted to the first device.” *Id.*

The listed citations for the transmitting steps (Abstract, Paragraphs 23–29, 33, 34, 58, Figs. 4–6) may describe transmitting subsets of information to the devices, and they may describe to-be-protected information not being transmitted to the first device. *See* RMTA 4, 6; Ex. 1003, 11–14, 19, 43–45. But Patent Owner does not explain how these citations describe transmitting steps that do something beyond isolation to protect the second subset of information from potential malware on the first device. Patent does not explain, for example, how these transmitting steps additionally prevent isolation from being undermined.

vi. “*Not Specific to a Device*” Limitation

As indicated above, the determining step recites “using application specific authentication information that is **not specific to a device** at both the first and second devices.” *See* RMTA, Appx. A, 3, 7–8 (emphasis added.)

Patent Owner corrects a suggestion that this limitation is security related and makes a point of clarifying that this limitation relates to “enhanc[ing] the user experience.” RMTA, 21 n.1. In other words, Patent Owner contends that this limitation in no way contributes to the enhanced security responsibilities imposed by the thereby clause. Thus, this would seem to detract from Patent Owner’s no-new-matter position with respect to the thereby clause.

Additionally, Petitioner presents persuasive arguments and evidence that this limitation introduces new matter. *See* Opp. RMTA, 1 (citing Ex. 1029 ¶ 4); Sur-Reply 1, Tr. 6–9. Patent Owner’s citations for the determining step include Paragraph 92 which says that “authentication information (such as a password) should allow for authentication on any **second** device.” Ex. 1003, 28 (emphasis added). Patent Owner argues that the Application “sufficiently describes the negative limitation of narrowing first device authentication by excluding non-device specific authentication information.” Reply Opp., 1 (citing *Novartis Pharms. Corp. v. Accord Healthcare, Inc.*, 38 F.4th 1013, 1016 (Fed. Cir. 2022)). However, as pointed out by Petitioner, this citation relates only to the second device. *See* Opp. RMTA, 1. Thus, we agree with Petitioner that this amendment fails to meet the statutory and regulatory requirement that the amendment add no new matter.

vii. Summary

Patent Owner does not adequately explain how the listed citations for the thereby clause and the storing/identifying/determining/transmitting steps provide written description support for beyond-isolation protection of the second subset of information. Thus, Patent Owner does not demonstrate adequately that RMTA Claims 26 and 41, and the claims depending therefrom, meet the no-new-matter requirement.

VIII. CONCLUSION⁹

For the reasons discussed above, we conclude that record does not support a finding that the RMTA meets the statutory and regulatory requirements necessary for its adding proposed substitute claims 26–41. *See* 35 U.S.C. § 316(d)(3); 37 C.F.R. § 42.121(a)(2)(ii).

⁹ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner’s attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

In summary:

Claim(s)	35 U.S.C. §	Reference(s)/Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1–4, 9, 13, 14, 16, 23–25	103	Zha ¹⁰ and POSITA’s knowledge ¹¹		
1–4, 9, 13, 14, 16, 23–25	103	Zha, POSITA’s knowledge, and Tsushima ^{12,13}		
5, 15	103	Zha, POSITA’s knowledge, and Gumbula ^{14,15}		
5, 15	103	Zha, POSITA’s knowledge, Tsushima, and Gumbula ¹⁶		
10	103	Zha, POSITA’s knowledge, and Stafford ^{17,18}		
10	103	Zha, POSITA’s knowledge, Tsushima, and		

¹⁰ Ex. 1004.

¹¹ Because these claims are canceled, we do not address this ground.

¹² Ex. 1010.

¹³ Because these claims are canceled, we do not address this ground.

¹⁴ Ex. 1011.

¹⁵ Because these claims are canceled, we do not address this ground.

¹⁶ Because these claims are canceled, we do not address this ground.

¹⁷ Ex. 1012.

¹⁸ Because this claim is canceled, we do not address this ground.

Claim(s)	35 U.S.C. §	Reference(s)/Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
		Stafford ¹⁹		
1–5, 9–10, 12–14, 16, 17, 23–25	103	<i>Takahashi</i> and POSITA’s knowledge ²⁰		
1–5, 9–10, 12–14, 16, 17, 23–25	103	<i>Takahashi</i> and POSITA’s knowledge ²¹		
Overall Outcome				

Motion to Amend Outcome	Claim(s)
Original Claims Cancelled by Amendment	1–5, 9, 10, 12–17, 23–25
Substitute Claims Proposed in the Amendment	26–41
Substitute Claims: Motion to Amend Granted	
Substitute Claims: Motion to Amend Denied	26–41
Substitute Claims: Not Reached	

¹⁹ Because this claim is canceled, we do not address this ground.

²⁰ Because these claims are canceled, we do not address this ground.

²¹ Because these claims are canceled, we do not address this ground.

IX. ORDER

For the reasons given, it is

ORDERED that Patent Owner's Revised Motion to Amend is *granted-in-part* as to the noncontingent request to cancel 1–5, 9–10, 12–17, and 23–25 of the '376 Patent;

FURTHER ORDERED that Patent Owner's Revised Motion to Amend is *denied-in-part* as to the request to add proposed substitute claims 26–41 to the '376 Patent; and

FURTHER ORDERED that, because this is a Final Written Decision, any party to the proceeding seeking judicial review of this Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2023-00683
Patent 9,064,376 B1

FOR PETITIONER:

R. William Beard, Jr
Brian C. Banner
SLAYDEN GRUBERT BEARD PLLC
wbeard@sgbfirm.com
bbanner@sgbfirm.com

Rudolph Y. Kim
Naveen Modi
Chetan Bansal
PAUL HASTINGS LLP
rudymkim@paulhastings.com
naveenmodi@paulhastings.com
chetanbansal@paulhastings.com

FOR PATENT OWNER:

ROBERT MCARTHUR
VASQUEZ, BENISEK & LINDGREN LLP
mcarthur@vbllaw.com