

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORESCOUT TECHNOLOGIES, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

IPR2021-00915
Patent 9,948,662 B2

Before THOMAS L. GIANNETTI, KIMBERLY McGRAW, and
CHRISTOPHER L. OGDEN, *Administrative Patent Judges*.

McGRAW, *Administrative Patent Judge*.

DECISION

Denying Institution of *Inter Partes* Review
35 U.S.C. § 314, 37 C.F.R. § 42.4

I. INTRODUCTION

Petitioner, Forescout Technologies, Inc., filed a Petition for *inter partes* review of claims 1, 2, 5–7, 9, 10, 13–15 of U.S. Patent No. 9,948,662 B2 (Ex. 1001, “the ’662 patent”). Paper 2 (“Pet.”). Patent Owner, Fortinet, Inc., filed a Preliminary Response. Paper 10 (“Prelim. Resp.”). Applying the standard set forth in 35 U.S.C. § 314(a), which authorizes institution of an *inter partes* review when “the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition,” we *do not* institute an *inter partes* review of any of the challenged claims of the ’662 patent on the grounds asserted in the Petition.

A. *Real Parties-in-Interest*

Petitioner identifies itself (i.e., Forescout Technologies, Inc.) as the real party-in-interest for Petitioner. Pet. 47. Patent Owner identifies itself (i.e., Fortinet, Inc.) as the real parties-in-interest for Patent Owner. Paper 4 (Patent Owner Mandatory Notice), 1.

B. *Related Matters*

The parties represent that the ’662 patent is at issue in *Fortinet, Inc. v. Forescout Technologies, Inc.* Case No. 3:20-cv-03343-EMC (N.D. Cal.). Pet. 47; Paper 4, 1.

C. *The ’662 Patent*

The ’662 patent, titled “Providing Security in a Communication Network,” issued on April 17, 2018 from an application filed on July 31, 2015. Ex. 1001, codes (10), (22), (45), (54). The ’622 patent is directed to systems and methods for optimizing system resources by selectively enabling various scanning functions relating to user traffic streams based on

the level of trust associated with the destination provided. *Id.* at code (57), 1:6–7.

In one embodiment, a client device within an enterprise network generates an application protocol request to access an external network. *Id.* at 7:65–67, Fig. 3. Before client device is able to access the external network, a network security device receives the application protocol request, which may include a network parameter, such as a domain or a destination Internet Protocol address. *Id.* at 7:67–8:6, Fig. 3. Based on the application protocol request, the network security device determines whether the network parameter of the external network is associated with a set of trusted networks. *Id.* at 8:8–11, Fig. 4. “When client device accesses the external network and a result of the trust determination made by the network security device is affirmative,” then the “network security device selectively disables application of a predefined and/or configurable subset of security features of those available on the network security device.” *Id.* at 8:17–22.

D. Challenged Claims

Of the challenged claims (i.e., claims 1, 2, 5–7, 9, 10, 13–15), claims 1 and 9 are independent. Claim 1 is reproduced below with formatting and bracketing added for clarity.

1. A method comprising:

- [a] receiving, by a network security device within an enterprise network, an application protocol request directed to an external network that is originated by a client device associated with the enterprise network;
- [b] determining, by the network security device, based on the application protocol request whether a network parameter of the external network is associated with a set of trusted networks; and

[c] selectively disabling, by the network security device, application of a subset of security features of a plurality of security features to be applied to network traffic exchanged between the client device and the external network while the client device is accessing the external network when a result of said determining is affirmative, wherein the subset of security features are selected based on a trust level associated with the external network.

Ex. 1001, 14:53–15:3.

9. A network security device comprising:

- [a] at least one processor; and
- [b] a computer-readable medium storing instructions that, when executed by the at least one processor, cause the at least one processor to perform a method comprising:
 - [b1] receiving an application protocol request directed to an external network that is originated by a client device associated with an enterprise network protected by the network security device;
 - [b2] determining based on the application protocol request whether a network parameter of the external network is associated with a set of trusted networks; and
 - [b3] selectively disabling application of a subset of security features of a plurality of security features to be applied to network traffic exchanged between the client device and the external network while the client device is accessing the external network when a result of said determining is affirmative, wherein the subset of security features are selected based on a trust level associated with the external network.

Id. at 15:44–10:11.

E. Prior Art and Asserted Grounds

Petitioner asserts that challenged claims are unpatentable under 35 U.S.C. § 103(a) on the following grounds (Pet. 7–8):

Claims Challenged	35 U.S.C. §¹	Reference(s)/Basis
1, 2, 5–7, 9, 10, 13–15	103	Ramsey ²
1, 2, 5–7, 9, 10, 13–15	103	Ramsey, Harris ³

Petitioner relies on the Declaration of Eric Cole, Ph.D. (the “Cole Declaration”) in support of its unpatentability contentions. *See* Ex. 1002.

II. ANALYSIS

A. Level of Ordinary Skill in the Art

In determining whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). Petitioner contends a person of ordinary skill in the art at the time of the alleged invention (a “POSITA”) would have a bachelor’s degree in computer science, computer engineering, or electrical engineering and at least three years of experience in networking operating systems and cyber security, or would have a master’s degree in one of the foregoing and at least two years of experience in the aforementioned fields. Pet. 5 (citing Ex. 1002 ¶¶ 26–28). Petitioner also asserts that someone with less or different technical education but more relevant practical experience, or more relevant education but less practical experience, could also be considered a POSITA.

¹ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), amended 35 U.S.C. § 103. Because the challenged claims of the ’662 patent have an effective filing date after the effective date of the applicable AIA amendment, we refer to the AIA version of 35 U.S.C. § 103.

² US 7,331,061 B1, issued Feb. 12, 2008 (Ex. 1003, “Ramsey”).

³ US 9,419,989 B2, issued August 16, 2016 (Ex. 1004, “Harris”).

Id. (citing Ex. 1002 ¶¶ 26–28). Petitioner also contends that this level of skill in the art is reflected by the references cited in this petition, the state of the art, and the experience of Dr. Eric Cole, as described in his declaration. Pet. 5–6. At this stage of the proceeding, Patent Owner does not dispute Petitioner’s definition of a POSITA nor articulate another level of skill for a POSITA. *See* Prelim. Resp. 6.

Based on our review of the ’662 patent, the types of problems and solutions described in the ’662 patent and cited prior art, we adopt and apply Petitioner’s definition of a person of ordinary skill in the art at the time of the claimed invention, except that we delete the qualifier “at least” to eliminate vagueness as to the appropriate level of education. The qualifier expands the range without an upper bound, i.e., encompassing a computer scientist with 25 years of experience and beyond, and thus does not meaningfully indicate the level of ordinary skill in the art.

B. Claim Construction

For petitions filed on or after November 13, 2018, such as here, we apply the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

Petitioner proposes construction for three terms, (1) “application protocol request,” (2) “security feature,” and (3) “trust levels.” For the first two terms, (i.e., “application protocol request” and “security feature”), Petitioner proposes construing the terms using the same construction proposed by Patent Owner in the co-pending district litigation. Pet. 6. For

the third term (i.e., “trust levels”), Petitioner provides unpatentability arguments under a construction proposed by Petitioner as well as a construction proposed by Patent Owner in the co-pending district court litigation. Pet. 6–7. In its Preliminary Response, Patent Owner responds that all claim terms should “be given their plain and ordinary meaning.” Prelim. Resp. 6.

We determine that no terms require express construction in order to determine whether Petitioner has met its burden to demonstrate a reasonable likelihood that any of the challenged claims are unpatentable. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy’” (quoting *Vivid Techs., Inc. v. Am. Sci & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

C. Principles of Law

A claim is unpatentable under § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in

the art; and (4) where in evidence, so-called secondary considerations.⁴
Graham, 383 U.S. at 17–18.

D. Asserted Unpatentability of Claims 1, 2, 5–7, 9, 10, and 13–15 over Ramsey

Petitioner contends that claims 1, 2, 5–7, 9, 10, and 13–15 would have been obvious under 35 U.S.C. § 103(a) over Ramsey. Pet. 7, 9–33. Patent Owner responds that Ramsey does not teach a network security device that performs the selective disabling steps required by independent claims 1 and 9. Prelim. Resp. 1, 6–15. For the following reasons, we agree with Patent Owner and determine that Petitioner has not demonstrated a reasonable likelihood it would prevail in showing that any of the challenged claims (i.e., 1, 2, 5–7, 9, 10, and 13–15) would have been obvious over Ramsey.

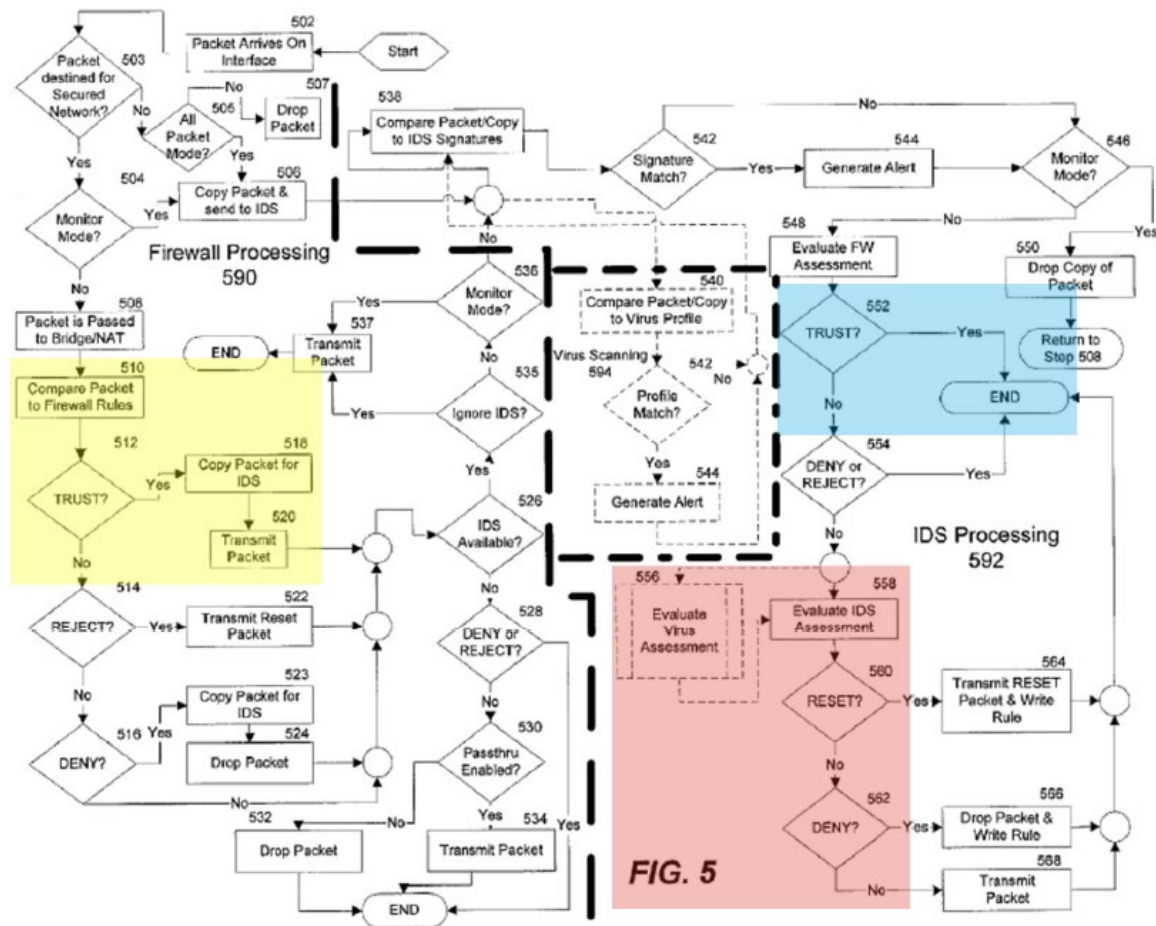
1. Overview of Ramsey

Ramsey is a US patent titled “Integrated Computer Security Management System and Method” that issued on February 12, 2008. Ex. 1003, codes (45), (54). Ramsey states that conventional secured computer networks typically include stand-alone firewalls, manufactured by a first party, that can route information to one or more stand-alone intrusion decision systems (“IDSs”) and one or more anti-virus systems (“AVSs”). *Id.* at 1:27–31. The stand-alone IDSs and AVSs are usually designed by second parties not affiliated with the first party firewall manufacturer. *See id.* at 1:31–33. Ramsey states that because the stand-alone firewalls and stand-alone IDS are manufactured by different vendors, complex interfaces are needed to pass packets entering a firewall destined for an IDS. *Id.* at 1:59–

⁴ Patent Owner does not present arguments or evidence of such secondary considerations in its Preliminary Response; as such, secondary considerations do not constitute part of our analysis.

63. Ramsey further states that a conventional system design that waits for separate processing to be completed by the stand-alone firewall, stand-alone IDS, and stand-alone AVS “consumes invaluable time that is critical” to any type of distributed computer network where speed is both a priority and a necessity. *Id.* at 1:51–55.

Figure 5 of Ramsey below, with yellow, blue, and red color highlights added by Petitioner, depicts a logic flow diagram illustrating an exemplary method for managing computer security information according to the invention. *Id.* at 6:14–17; Pet. 20.



The first section (i.e., Firewall Processing 590), which includes steps 510, 512, 516, and 520 highlighted in yellow, is on the left side of the figure and “denotes the steps that can be performed by [] firewall 225.” *Id.* at 19:36–38; Pet. 20. The second section (i.e., IDS Processing 592) is found on the right side of the figure and “denotes the steps of the process that can be performed by [] IDS 255.” *Id.* at 19:38–39. This second section (i.e., IDS processing 592) includes step 552 highlighted in blue and steps 556, 558, 560, and 562 highlighted in red. Ex. 1003, Fig. 5; Pet 20. The third section, 594, found in the center of the figure, is completely enclosed by dashed lines and denotes the steps of the process that can be performed by virus scanner 250. *Id.* at 19:42.

2. *Analysis of Claim 1*

Petitioner contends Ramsey’s firewall 225 is a “network security device” that performs the “receiving,” “determining,” and “selectively disabling” steps recited in claim elements 1[a], [b], and [c] respectively. Pet. 13–22.

For example, Petitioner asserts that Ramsey teaches receiving an application protocol request as required by claim element 1[a] because Ramsey’s firewall receives and examines all network traffic flowing to and from client devices and to and from external networks and that a POSITA would have understood that Ramsey’s firewall can receive and process application protocol requests. Pet. 13–15 (citing Ex. 1003, 4:31–37; Ex. 1002 ¶¶ 73–79).

Petitioner also contends Ramsey teaches determining whether a network parameter is associated with a set of trusted networks as required by claim element 1[b] because, *inter alia*, Ramsey’s “firewall analyzes ‘characteristics of packet headers’ to make a trust determination.” Pet. 18.

Petitioner explains that Ramsey’s firewall stores a list of trusted external networks and can immediately transmit messages from such networks without waiting on the intrusion detection system (IDS) to perform certain security functions. Pet. 16–17 (citing Ex. 1003, 10:36–53; Ex. 1002 ¶ 83). Petitioner contends this process is also depicted Ramsey’s Figure 5, “where the firewall at step 510 determines whether a packet is trusted.” Pet. 17; *see also* Pet. 20 (reproducing Ex. 1003, Fig. 5 with yellow highlights added to, *inter alia*, step 510). Petitioner asserts that step 510 involves comparing characteristics of packet headers for those packets that may be considered trusted by firewall 225. *Id.* (quoting Ex. 1003, 16:31–60 (quotations omitted)). Petitioner states that if a packet is trusted, it “can be permitted to pass immediately through [] firewall 225.” *Id.* (quoting Ex. 1003, 16:31–60). Petitioner further states that “[u]ltimately the trusted packet is transmitted at step 520.” Pet. 17; *see also* Pet. 20 (reproducing Ex. 1003, Fig. 5 with step 520, *inter alia*, highlighted in yellow).

Petitioner also asserts that Ramsey teaches “selectively disabling . . . application of a subset of security features . . . wherein the subset of security features are selected based on a trust level” as required by claim element 1[c], pointing to, *inter alia*, steps shown in Firewall Processing 590 and in IDS Processing 592 of Ramsey’s Figure 5. *See* Pet. 19–22 (citing, *inter alia*, Ex. 1002 ¶¶ 87–97; Ex. 1003, 11:66–12:1, 12:30–42, 16:31–60, 19:15–22, Fig. 5).

In particular, Petitioner contends that step 510 on the left side of Ramsey’s Figure 5 (highlighted in yellow), involves comparing packet header characteristics for those packets “that may be considered ‘trusted’ by . . . firewall 225.” Pet. 19 (citing Ex. 1003, 16:31–60). Petitioner states that if a packet “is trusted, it ‘can be permitted to pass immediately through []

firewall 225.’ . . . Ultimately the packet is transmitted at step 520.” Pet. 19–20 (quoting Ex. 1003, 16:31–60).

Petitioner also contends that the steps shown in the right side of Ramsey’s Figure 5 and highlighted in blue depict “that the IDS evaluates the firewall’s assessment in step 552 and immediately goes to ‘END’ if the packet is trusted.” Pet. 20 (reproducing Ex. 1003, Fig. 5 with highlighting added). Petitioner explains that Ramsey’s “IDS 255 can determine whether [] firewall 225 has deemed a particular packet to be trusted” and that if “IDS 255 detects any one of these firewall 225 verdicts, then processing by [] IDS 255 stops.” Pet 20 (quoting Ex. 1003, 12:30–42; citing Ex. 1002 ¶¶ 90–92). Petitioner contends that “[s]topping IDS processing disables certain security features by ending the IDS without performing those steps for a particular transmission.” *Id.* Petitioner explains that certain steps shown on the right side of Ramsey’s Figure 5 (i.e., steps 556, 558, 560, 562) are the claimed “security features” and that these security features “are disabled if Ramsey’s firewall determines that a packet is to be trusted. Pet. 20–21 (reproducing Ex. 1003 Fig. 5 with red highlights added to steps 556, 558, 560, 562 and citing Ex. 1002 ¶ 93). Petitioner concludes that “these features are disabled based on the trust level, i.e., whether Ramsey’s firewall has determined the packet to be trusted or not.” Pet. 21 (citing Ex. 1002 ¶ 95).

Patent Owner responds that Petitioner fails to demonstrate how Ramsey’s firewall performs the selectively disabling limitation of claim element 1[c]. Prelim. Resp. 7, 11–15.

We agree with Patent Owner. Claim 1 explicitly requires that the step of “selectively disabling . . . application of a subset of security features” be performed “by the network security device.” Petitioner, however, fails to sufficiently show that Ramsey’s *firewall*, the asserted “network security

device,” performs the *selectively disabling* of security features step as required by claim element 1[c].

Although Petitioner does cite to steps that are performed by Ramsey’s firewall, Petitioner does not sufficiently show that these steps perform the “selectively disabling” required by claim element 1[c]. For example, Petitioner asserts that Ramsey’s step 510 involves comparing characteristics of packet headers for those packets that may be considered trusted by firewall 225, that if the packet is trusted that it can be permitted to immediately pass through firewall 225, and that the packet is transmitted at step 520⁵. Pet. 19–20. Petitioner, however, does not sufficiently explain how any of these steps disable any security features.

Rather, Petitioner asserts that “[s]topping IDS processing disables certain security features by ending the IDS without performing those steps for a particular transmission.” Pet. 20. Significantly, however, the steps that Petitioner identifies as stopping IDS processing all occur in the IDS, not in Ramsey’s firewall, the asserted network security device. Notably, Petitioner asserts that, as shown in the right side of Figure 5, “the *IDS* evaluates the firewall’s assessment in step 552 and immediately goes to ‘END’ if the packet is trusted (highlighted in blue . . .).” *Id.* (emphasis added). Petitioner goes on to state that Ramsey’s “*IDS 255 can determine*” whether Ramsey’s firewall 225 has deemed a particular packet to be trusted and that if IDS 225 detects any of these firewall verdicts, then “*then processing by the IDS stops.*” *Id.* (citing Ex. 1003, 12:30–42; Ex 1002 ¶¶ 90–92). Thus,

⁵ Petitioner also relies on the same steps as satisfying the “determining . . . whether a network parameter . . . is associated with a set of trusted networks” required by claim element 1[b]. *See* Pet. 17–20.

the steps that Petitioner asserts disable certain security features are performed in Ramsey's IDS, not in the firewall.

As such, the steps that Petitioner identifies as selectively disabling the application of security features (i.e., stopping IDS processing) are performed in the IDS, not by the firewall (the asserted network security device), as required by claim element 1[c]. Thus, because Petitioner fails to sufficiently show that Ramsey's firewall performs the selectively disabling limitation, Petitioner fails to establish a reasonable likelihood that it would prevail in establishing claim 1 of the '662 patent is unpatentable under over Ramsey.

3. Independent Claim 9 and Dependent Claims 2, 5–7, 10, and 13–15

Independent claim 9 is directed to a network security device having, *inter alia*, a processor that performs a method comprising receiving an application protocol request (i.e., claim element 9[b1]), determining whether a network parameter is associated with a set of trusted networks (claim element 9[b2]), and selectively disabling a subset of security features (claim element 9[b3]). Ex. 1001, 15:43–16:11.

Petitioner asserts that claim elements 9[b1], [b2], and [b3] are “substantively indistinguishable” from claim elements 1[a], [b], and [c] and that a POSITA would have found the subject matter of claim 9 obvious for the same reasons as claim 1. Pet. 31. Petitioner does not provide any additional argument that Ramsey teaches or suggests the selectively disabling limitation of claim element 9[b3]. For the same reasons stated above with respect to claim 1, we determine that Petitioner fails to establish a reasonable likelihood that it would prevail in establishing claim 9 of the '662 patent is unpatentable under over Ramsey.

Dependent claims 2, 5–7, 10, and 13–15 depend, directly or indirectly, from claim 1 or claim 9. Petitioner’s analysis of these claims addresses only the added limitations of each dependent claim and does not provide further argument that would remedy the deficiency as to the independent claims. *See* Pet. 22–29, 31–33. Thus, Petitioner fails to demonstrate a reasonable likelihood that it would prevail in establishing that claims 2, 5–7, 10, and 13–15 are unpatentable as obvious over Ramsey. *See In re Fine*, 837 F.2d 1071, 1076 (Fed. Cir. 1988) (“Dependent claims are nonobvious under section 103 if the independent claims from which they depend are nonobvious.”).

4. Conclusion

For the foregoing reasons, we determine the evidence and arguments presented fail to show a reasonable likelihood Petitioner would prevail in establishing that claims 1, 2, 5–7, 9, 10, and 13–15 would have been obvious over Ramsey.

E. Asserted Unpatentability of Claims 1, 2, 5–7, 9, 10, and 13–15 over Ramsey and Harris

Petitioner also contends that claims 1, 2, 5–7, 9, 10, and 13–15 are unpatentable as obvious over Ramsey and Harris. Pet. 33–46.

Petitioner, however, does not rely upon Harris for teaching or suggesting a “network security device” that performs the selectively disabling step of claim element 1[c] or similar limitations of claim 9. As such, for the same reasons stated above in Section II.D, Petitioner has not sufficiently shown that the combination of Ramsey and Harris teaches or suggests all of the limitations of independent claims 1 and 9 or the claims that depend therefrom. Accordingly, Petitioner has not shown a reasonable

likelihood that it would prevail in showing that any of the challenged claims would have been obvious over the combination of Ramsey and Harris.

III. CONCLUSION

After considering the evidence and arguments presented by the parties, we determine the information presented does not establish a reasonable likelihood that Petitioner would prevail in showing that claims 1, 2, 5–7, 9, 10, and 13–15 of the '662 patent are unpatentable. Accordingly, we do not institute *inter partes* review of any of the challenged claims on any ground asserted in the Petition.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1, 2, 5–7, 9, 10, and 13–15 of the '662 patent is *not* instituted.

IPR2021-00915
Patent 9,948,662 B2

FOR PETITIONER:

Katherine Vidal
Louis Campbell
kvidal@winston.com
llcampbell@winston.com

FOR PATENT OWNER:

Patrick D. McPherson
Christopher Tyson
D. Joseph English
Patrick C. Muldoon
Tairan Wang
Paul H. Belnap
DUANE MORRIS LLP
PDMcPherson@duanemorris.com
CJTyson@duanemorris.com
DJEnglish@duanemorris.com
PCMuldoon@duanemorris.com
TWang@duanemorris.com
PHBelnap@duanemorris.com